Informationsrechte und –pflichten bei Sicherheitslücken im Internet

Zum Beitrag des Rechts zur Steuerung der IT-Sicherheit im Internet

Vom Fachbereich Rechts- und Wirtschaftswissenschaften der

Technischen Universität Darmstadt genehmigte

Dissertation

zur Erlangung des akademischen Grades eines Doctor iuris (Dr. iur.)

Vorgelegt von

Ruth Schadel

Geburtsdatum: 23.12.1974

Geburtsort: Würzburg

Erstgutachterin: Prof. Dr. Viola Schmid, LL.M. (Harvard)

Zweitgutachter: Prof. Dr. Jochen Marly

Eingereicht am: 13.06.2006

Mündliche Prüfung am: 13.11.2006

Darmstadt 2007

D 17

Meiner Familie

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

Abl.	Amtsblatt
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AktG	Aktiengesetz
AMG	Arzneimittelgesetz
AO	Abgabenordnung
ArbSchG	Arbeitsschutzgesetz
AtG	Atomgesetz
b2b	Business to Business
b2c	Business to Customer
b2g	Business to Government
BAG	Bundesarbeitsgericht
BayObLG	Bayerisches Oberstes Landesgericht
BB	Betriebs-Berater (Zeitschrift)
BCP	Best Current Practices
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BfD	Bundesdatenschutzbeauftragten
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	(Amtliche Sammlung der) Entscheidungen des Bundesgerichtshofs in Strafsachen
BImSchG	Bundesimmissionsschutzgesetz
BPersVG	Bundespersonalvertretungsgesetz
BR-Drs.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über die Errichtung des Bundesamtes für die Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	(Amtliche Sammlung der) Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
c´t	Magazin für Computertechnik (Zeitschrift)
CCC	Convention on Cybercrime
ccTLD	country code Top Level Domain
CEN/CENELEC	European Committee for Standardization/ European Committee for Electrotechnical Standardization
CERT	Computer Emergency Response Team

CR	Computer und Recht (Zeitschrift)
DB	Der Betrieb (Zeitschrift)
DeNIC	de Network Information Center
DFN	Deutsches Forschungsnetz
DIN	Deutsches Institut für Normung e.V
DNS	Domain Name System
DoS	Denial of Service
DSL	Digital Subscriber Line
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBl.	Deutsches Verwaltungsblatt (Zeitschrift)
EGMR	Europäischer Gerichtshof für Menschenrechte
ENISA	Europäische Agentur für Netz und Informationssicherheit
EuGH	Europäischer Gerichtshof
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (Zeitschrift)
FCC	Federal Communication Commission
ftp	File Transfer Protocol
FYI	For Your Information
g2b	Government to Business
g2g	Government to Government
GAN	Global Area Network
GG	Grundgesetz
g2c	Government to Citizen
GPSG	Geräte- und Produktsicherheitsgesetz
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GRUR Int	Gewerblicher Rechtsschutz und Urheberrecht International (Zeitschrift)
gTLD	generic Top Level Domain
GVG	Gerichtsverfassungsgesetz
HbdStR	Handbuch des Staatsrechts
HGB	Handelgesetzbuch
HSOG	Hessisches Sicherheits- und Ordnungsgesetz
html	Hypertext Markup Language
http	Hypertext Transfer Protocol
https	Hypertext Transfer Protocol Secure
IAB	Internet Architecture Board
ICANN	Internet Cooperation for Assigned Names and Numbers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IP	Internet Protocol
IRTF	Internet Research Task Force
ISDN	Integrated Services Digital Network
ISO	International Standardization Organization
ISOC	Internet Society
IT	Informationstechnik

ITRB	IT-Rechtsberater (Zeitschrift)
ITSec	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
IuK	Informations- und Kommunikationstechnologie
IVBB	Informationsverbund Berlin-Bonn
JurPC	Internet-Zeitschrift für Rechtsinformatik (Zeitschrift)
JuS	Juristische Schulung (Zeitschrift)
JZ	Juristenzeitung (Zeitschrift)
K&R	Kommunikation & Recht (Zeitschrift)
KG	Kammergericht
Krw-/AbfG	Kreislaufwirtschafts- und Abfallgesetz
KWG	Kreditwesengesetz
LAG	Landesarbeitsgericht
LAN	Local Area Network
LG	Landgericht
LIR	Local Internet Registries
MAN	Metropolitan Area Network
MB	Megabyte
MMR	Multimedia und Recht (Zeitschrift)
MPG	Medizinproduktegesetz
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NuR	Natur und Recht (Zeitschrift)
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
NZA	Neue Zeitschrift für Arbeitsrecht (Zeitschrift)
NZA-RR	Neue Zeitschrift für Arbeitsrecht Rechtsprechungs-Report (Zeitschrift)
NZG	Neue Zeitschrift für Gesellschaftsrecht (Zeitschrift)
NZV	Neue Zeitschrift für Verkehrsrecht (Zeitschrift)
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OIS	Organization for Internet Safety
OLG	Oberlandesgericht
OPN	Open Network Provision
OSI	Open System Interconnection
PAN	Personal Area Network
PC	Personal Computer
PDA	Personal Digital Assistant
ProdHaftG	Produkthaftungsgesetz
PTSG	Post- und Telekommunikationssicherstellungsgesetz
QoS	Quality of Service
RdA	Recht der Arbeit (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RFC	Request for Comments
RIR	Regionalen Internet Registries

RStV	Rundfunkstaatsvertrag
SGB	Sozialgesetzbuch
SLD	Second Level Domains
smtp	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordung
TCP	Transmission Control Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
TLD	Top Level Domain
UBAG	Gesetz über die Errichtung eines Umweltbundesamtes
UIG	Umweltinformationsgesetz
ULD	Unabhängiges Landeszentrum für Datenschutz
UrhG	Urheberrechtsgesetz
URL	Uniform Resource Locator
UWG	Gesetz gegen den unlauteren Wettbewerb
VersR	Versicherungsrecht (Zeitschrift)
VG	Verwaltungsgericht
VPN	Virtual Private Network
VuR	Verbraucher und Recht (Zeitschrift)
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
VVG	Versicherungsvertragsgesetz
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
WAN	Wide Area Network
WiVerw	Wirtschaft und Verwaltung (Zeitschrift)
wLAN	Wireless Local Area Network
WM	Wertpapier-Mitteilungen (Zeitschrift)
WPg	Die Wirtschaftsprüfung (Zeitschrift)
WpHG	Wertpapierhandelsgesetz
WRP	Wettbewerb in Recht und Praxis (Zeitschrift)
WTO	World Trade Organization
ZEuP	Zeitschrift für Europäisches Privatrecht
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik (Zeitschrift)
ZZP	Zeitschrift für Zivilprozeß (Zeitschrift)

EINLEITUNG

Die Bedeutung des Internets ist unbestreitbar. Es prägt die Lebenswirklichkeit weit mehr als bisherige Medien. Dies liegt daran, dass es Optionen für die Arbeitswelt und den privaten Bereich bietet, gesellschaftlichen Interaktionen dient und tendenziell den gesamten menschlichen Kommunikationsbereich umfasst. Die Reichweite des Internets und Abhängigkeit von ihm wird insbesondere dann deutlich, wenn es ausfällt und nicht mehr zur Verfügung steht. Der Sicherheit des Internets kommt, anders gesagt, eine Schlüsselposition zu.

Einem Strategiepapier der Europäischen Kommission vom 31.05.2006 liegt die Prämisse zu Grunde, dass Informationen über Bedrohungen, Risiken und Warnungen einen Beitrag zur Sicherheit von IT-Systemen zu leisten vermögen.[1] Nicht nur vor dem Hintergrund der ökonomischen Relevanz von IT-Systemen sei IT-Sicherheit eine condito sine qua non. Wie kritischen Infrastrukturen von IT-Systemen abhängig seien, so seien auch diese von deren Sicherheit abhängig. Die Nutzer von IT-Systemen trügen zur IT-Sicherheit entscheidend bei; ihrem Anteil könne eine eigene Qualität zugesprochen werden. Bei der Etablierung von IT-Sicherheit komme den Behörden eine beispielgebende Rolle zu. Darüber hinaus wird im genannten Papier die Qualität der IT-Sicherheit als Wettbewerbsvoraussetzung und -vorteil von Unternehmen hervorgehoben und auf die Rolle des individuellen Nutzers als Glied einer Sicherheitskette hingewiesen. Diesen Herausforderungen, heißt es dann, könnten die Akteure nur gerecht werden, wenn sie zuverlässig über Bedrohungen und Sicherheitsvorfälle informiert würden. Die Strategie der Europäischen Kommission zielt daher auf den Aufbau eines

> *„European information sharing and alert system to facilitate effective response to existing and emerging threats to electronic networks. A requirement of such a system will be a multilingual EU portal to provide tailored information on threats, risks and alerts."*[2]

Das Strategiepapier betont einen organisatorischen Aspekt der Veröffentlichung von Information. Ob und inwieweit ein solches Informationsportal zu realisieren ist, bleibt abzuwarten. Denn die Europäische Kommission befindet sich derzeit erst im Status der Planung der Entwicklung.

---

1 Mitteilung über eine Strategie für eine sichere Informationsgesellschaft – „Dialog, Partnerschaft und Delegation der Verantwortung", KOM(2006)251 vom 31.05.2006.

2 A.a.O., (Fn. 1), Punkt 3.2., S. 8.

Die Beantwortung der Frage, ob und inwieweit das Recht die Veröffentlichung von Information regeln kann, sich also ein Informationsmodell in Form von Informationsrechten und –pflichten aus dem Recht entwickeln lässt, ist Gegenstand dieser Arbeit. Ihre grundlegende These ist, dass Informationen über Sicherheitslücken und Schwachstellen im Internet einen Beitrag zur Sicherheit des Internets leisten kann.

Es gilt daher zu prüfen, ob und inwieweit Information tatsächlich einen Beitrag zur Erhöhung der Sicherheit des Internets leisten kann. Beispielhaft kann der Einfluss von Information auf die IT-Sicherheit anhand der Verbreitung von Sasser erörtert werden.

Sasser[3] ist ein Computerwurm, der 2004 weltweit unzählige Computer befiel. Er suchte und nutzte selbstständig eine ausnutzbare Sicherheitslücke im Betriebssystem und brachte infizierte Rechner zum Absturz. Dieser Absturz führte nicht nur zu Nutzungsbeeinträchtigungen, so etwa bei den PCs der Europäischen Kommission, sondern hatte im Falle einer Fluggesellschaft die Streichung mehrerer Flüge zur Folge.[4] Das gesamte Ausmaß der Schäden ist wohl nicht bekannt. Für die Sicherheitslücke, die Sasser ausnutze, hatte der Hersteller einige Wochen zuvor Programme, die die Lücke schließen (Patches), veröffentlicht und verbreitet. Die Angriffstechnik von Sasser zielte auf die Sicherheitslücke. Der Autor von Sasser nutzte hierbei Informationen aus dem Patch und die Tatsache aus, dass nicht jeder Nutzer das Patch installierte. Die Entstehung von Sasser kann als Präzedenzfall für das Verhältnis von Information und IT-Sicherheit dienen. Hierbei sind folgende Gesichtspunkte ausschlaggebend:

Sasser wurde erst geschrieben, nachdem Informationen über die Sicherheitslücke öffentlich bekannt geworden waren, d. h. erst die Information über die Sicherheitslücke und das Patch als Schutztechnik ermöglichte das Ausnutzen. Dabei bleibt fraglich, ob ohne die Information über die Sicherheitslücke und den Patch Sasser überhaupt geschrieben und die Sicherheitslücke damit ausgenutzt worden wäre.

---

[3] Vgl. die Kurzbeschreibung dieses Wurms und seiner Funktionsweise unter http://www.bsi.de/av/vb/sasser.htm (30.05.2006). Der Autor des Wurms wurde vom LG Verden, Urteil v. 08.07.2005 – 3-5/05 zu einer Jugendstrafe von einem Jahr und neun Monaten, ausgesetzt auf Bewährung, verurteilt.

[4] Vgl. verschiedene Pressemitteilungen: heise news vom 06.07.2005, http://www.heise.de/security/news/meldung/61458 (30.05.2006); teltarif.de vom 04.01.2005, http://www.teltarif.de/arch/2005/kw01/s15821.html (30.05.2006); heise news vom 21.05.2004, http://www.heise.de/security/news/meldung/47546 (30.05.2006).

Sasser war deswegen so erfolgreich, weil das notwendige Patch von vielen Nutzern nicht installiert wurde, d. h. die Information darüber nicht beachtet wurde.

Dies macht deutlich, dass Information nicht notwendigerweise ein Schritt zur Erhöhung der Sicherheit darstellt, sondern als ambivalent eingeschätzt werden kann. Ob mit der Information ein tatsächlicher Beitrag zur Sicherheit im Internet geleistet werden kann, entscheiden damit letztendlich die Nutzer, welche Maßnahmen zur Beseitigung der Sicherheitslücken und Erhöhung der Sicherheit ergreifen müssen. Information kann grundsätzlich Einfluss auf die Nutzer und ihr Bewusstsein um Gefahren haben. In jedem Fall wird bei der rechtlichen Diskussion die Ambivalenz von Information zu berücksichtigen sein.

Bei Sasser hat sich gezeigt, dass selbst nach Ausnutzen der Sicherheitslücke und dem Eintreten von Schäden Informationen über Sicherheitslücken nicht in jedem Fall veröffentlicht, sondern geheim gehalten werden. Unternehmen fürchten nicht zuletzt einen Imageverlust, der beim Bekanntwerden eines nicht hinreichenden Einsatzes von IT-Sicherheitstechnik entstehen könnte.

Informationsrechte und –pflichten stehen nicht nur im Kontext von Sicherheit. Bei der Bestimmung ihres Umfangs muss unterschiedlichen Interessen Rechnung getragen werden. Welche Interessen präferiert werden, kann etwa dem Urheberrecht oder dem Strafrecht entnommen werden. Dies aber kann bisweilen zu Asymmetrien in der Verteilung von Information über Sicherheitslücken führen.

Nach dieser Vorstellung des Anliegens der vorliegenden Arbeit soll im Folgenden der Gang der Untersuchung entwickelt werden.

In Kapitel 1 werden zunächst Szenarien skizziert, die beispielhafte Konstellationen mit Bezug zu Sicherheitslücken im Internet aufzeigen: So wird einerseits der Umgang mit Sicherheitslücken bestimmter Akteure – wie dem Staat – akzentuiert. Andererseits werden Bereiche aufgezeigt, in denen der Umgang mit Sicherheitslücken offenbar anderen Interessen unterworfen ist. Dies wird exemplarisch am Arbeitsverhältnis erläutert. Schließlich werden anhand eines Beispiels aus dem E-Commerce die Folgen der Sicherheitslücken für Rechtsgüter hervorgehoben.

In Kapitel 2 und Kapitel 3 werden Sicherheit, Internet und Information als zentrale Begriffe der Arbeit in ihrem Bedeutungsgehalt umrissen und in ihrer wechselseitigen Bezogenheit eingeführt.

Besagter Bedeutungsgehalt lässt sich durch Definitionen oder Kontexteinbettungen allerdings nur annäherungsweise ausdrücken. Im Falle des Internets, der Sicherheit

bzw. der Sicherheitslücke scheint eine definitorische Annäherung nicht sonderlich ergiebig zu sein. Denn Definitionen besitzen nur im begrenzen Maße eine disziplinübergreifend Gültigkeit. Die Untersuchung der Informationsrechte und –pflichten erfordert vielmehr eine Synthese des rechtlichen und technischen Kontexts. Diese Verknüpfung soll durch die Herausarbeitung von Bezügen erfolgen. Das heißt: Eine inhaltliche Bestimmung von Sicherheit wird hinsichtlich des Gegenstandes der Arbeit in einer technischen und rechtlichen Kategorienbildung vorgenommen.

Mit der Relation von Sicherheit und Internet sollen im Kapitel 2 zunächst technische, rechtliche und ökonomische Kategorien von Sicherheit erörtert werden. Was Sicherheitslücken im Internet sind, wird anhand der Elemente und Funktionsweise des Internets bestimmt. Sicherheitslücken können hierbei durch fehlerhaft funktionierende Einzelkomponenten oder Wechselwirkung der Einzelkomponenten (systembedingt) oder durch fehlerhafte Bedienung bei Implementierung oder Anwendung (nutzungsbedingt) den Zustand der Gefahr herbeiführen. In der systembedingten Betrachtung konzentriert sich Sicherheit auf zwei Hauptaspekte: erstens, auf die zu Grunde liegende Infrastruktur (in der Arbeit als Schwachstellen in IT-Systemen bezeichnet), und zweitens, auf die ausgeführte Anwendung (als Sicherheitslücke vorwiegend die genutzte Software betreffend). Unter rechtlichen Aspekten ist eine Sicherheitslücke im Internet, verkürzt formuliert, durch den Zustand einer Gefahr für Rechtsgüter oder Interessen gekennzeichnet.

Mit der Relation von Sicherheit und Information soll in Kapitel 3 der Beitrag von Information zur Erhöhung der Sicherheit und die Erwartungen und Reaktionen der Nutzer aufgezeigt werden. Hier wird zunächst exemplarisch, mit der Offenlegung von Sicherheitsinformation bei ec-Karten, das oben angedeutete Spannungsverhältnis zwischen dem Interesse an der Geheimhaltung und dem Interesse an Information beim Ausgleich von Informationsasymmetrien dargestellt. Des Weiteren wird die bereits beschriebene ambivalente Wirkung von Information aus Sicht der Technik angegangen. Darüber hinaus soll der Nutzer als Rezipient der Information über die Sicherheitslücke in einem Nutzerleitbild charakterisiert werden.

In Kapitel 4 wird der Beitrag von Recht und Information im Allgemeinen vorbereitet, bevor im Kapitel 5 der Beitrag von Informationsrechte und –pflichten zur Sicherheit im Besonderen dargestellt wird. Der Beitrag von Recht und Information im Allgemeinen wird dabei auch durch die Frage nach Steuerungsmöglichkeiten problematisiert. Dieser Rekurs dient zum einen der Darstellung der (intendierten) Wirkung von Recht und Information. Zum anderen werden am Beispiel der staatli-

chen Steuerung des Informationsvorgangs mittels Warnung, Aufklärung und Empfehlung wichtige Steuerungsinstrumente vorgestellt, sowie mit der Beschreibung der Funktion von Informationszentren die Ausgleichs- und Selektionsfunktion der Steuerung des Informationsvorgangs unterstrichen.

In Kapitel 5 wird erläutert, welchen Beitrag die Informationsrechte und –pflichten zur Sicherheit im Internet als IT-Informationsrecht zu leisten vermögen. Die Untersuchung orientiert sich hierbei an einem strukturellen und einem personellen Gliederungsstrang.

Das IT-Informationsrecht lässt sich strukturell aufteilen in das Recht sich zu informieren und das Recht zu informieren sowie der Pflicht sich zu informieren und der Pflicht zu informieren.

In personeller Hinsicht wird die strukturelle Gliederung der Rechte und Pflichten des IT-Informationsrechts durch eine Untergliederung und Zuordnung nach Akteuren – Herstellern, Anbietern und Nutzern des Internets – ergänzt. Hierbei wurde davon abgesehen, Informationspflichten des Staates in einem getrennten Kapitel zu behandeln. Damit soll deutlich gemacht werden, dass der Staat im Internet – unabhängig von seiner sonstigen dichotomischen Abgrenzung zum Bürger – mit den Anbietern und Herstellern hinsichtlich des Umgangs mit den Informationen über Sicherheitslücken im Grundsatz gleichgestellt werden kann.

Da die unterschiedlichen Ausprägungen und Auswirkungen von Sicherheitslücken grundsätzlich eine Bestimmung der Rechte und Pflichten als Einzelfallentscheidungen indizieren, sollen diese – soweit möglich – unter Rückgriff auf die Szenarien in Kapitel 1 bestimmt werden. Hierbei kommt es weniger auf eine umfangreiche und ausführliche Lösung der Szenarien an; durch diese soll vielmehr die anschauliche Untersuchung eines IT-Informationsrechts ermöglicht werden.

In Kapitel 6 werden schließlich die in den vorangehenden Kapiteln gewonnenen Ergebnisse zu abschließenden Thesen zusammengeführt.

KAPITEL 1 SZENARIEN

Um an den Gegenstand der Untersuchung heranzuführen, werden im Folgenden ausgewählte Fälle aus der Praxis vorangestellt. Die skizzierten Szenarien werfen grundlegende Fragen im Umgang mit Sicherheitslücken auf, die im Laufe der Arbeit beantwortet werden sollen. Technische Details und Abkürzungen werden wegen der hier gebotenen Knappheit nicht in den Szenarien, sondern im nächsten Kapitel erläutert.

Die Szenarien dienen als plastische Ergänzung der Diskussion bestimmter Bereiche. Deshalb liegt der Schwerpunkt der Untersuchung auch nicht in der Ausarbeitung einer umfangreichen und erschöpfenden Lösung der Szenarien.

A Szenario 1: Staatliche Verbraucherwarnung vor Software

Das Betriebssystem eines führenden Softwareunternehmens enthält einige Sicherheitslücken. Soweit es einschlägigen Mailinglisten[1] und Newsgroups entnommen werden kann, kommen ständig neue Lücken hinzu, respektive werden gefunden.

Neben den Sicherheitslücken der Betriebssysteme[2] wird die Sicherheit des Browsers kritisiert, der vom Hersteller standardmäßig beigegeben wird. Hierbei werden die standardmäßigen (vom Nutzer veränderbaren) Werkseinstellungen sowie nicht hinnehmbare Sicherheitslücken der Software, die zum Systemabsturz führen können, an sich festgestellt. Konkret wird etwa kritisiert, dass Java-Script mittels Werkeinstellung zugelassen ist und nicht durch bewusste Einstellungen des Nutzers aktiviert werden muss.

Unter Ausnutzen dieser Sicherheitslücken kann teilweise auf gespeicherte Information zugegriffenen und diese verändert werden. Teilweise werden andere Angriffsformen – etwa durch Java-Script das Phishing – ermöglicht.

Die Sicherheitslücken werden zum einen vom Softwareentwickler selbst aufgedeckt, zum anderen wird er von Dritten über Sicherheitslücken informiert. Der Softwarehersteller, der grundsätzlich – aufgrund der Reputation und der hier unter-

---

1 Zu nennen ist hier etwa bugtraq, http://www.securityfocus.com/archive (30.05.2006).

2 Dies betrifft sowohl das Betriebssystem für Server, als auch das vorwiegend für Clients verwendete.

stellten eigenen Nutzung der Produkte – an der Schließung der Lücken interessiert ist, kann in einigen Fällen, wenn auch teilweise mit extremer zeitlicher Verzögerung, ein Angebot zur Abhilfe schaffen. Teilweise bleibt das Sicherheitsproblem aus technischen Gründen ungelöst. Als Zeichen des guten Willens kündigt er an, an einem regelmäßigen Patchday Angebote zur Schließung der Lücke bereitzuhalten.

Unabhängig voneinander raten die Bundesregierung (der Bundeswirtschaftsminister anlässlich eines Interviews), das Bundesamt für Sicherheit in der Informationstechnik (im Internet) und der Landesdatenschutzbeauftragte von Schleswig-Holstein (in seinem Tätigkeitsbericht) explizit von dem Browser ab und stellen alternative Konkurrenzprodukte vor.

Ist dieses Verhalten rechtmäßig?

B Szenario 2: Sicherheitslücken am Arbeitsplatz[3]

Der Arbeitgeber eines IT-Sicherheitsexperten bietet neben anderen Online-Dienstleistungen unter anderem einen „unified messaging service" an, womit Online-Nachrichten auf Fax, Anrufbeantworter, E-Mail, SMS umgeleitet werden können. Empfänger von Nachrichten können so je nach Situation entscheiden, auf welchem Endgerät sie ihre Nachricht entgegennehmen und/oder ob sie die Nachrichten mit einem Nutzerzugang auf dem Online-Portal einsehen wollen.

Jeder Nutzer erhält für eine Session, für die er eingeloggt ist, einen „numerical code" (NID). Wenn der Nutzer durch einen Link in einer E-Mail die eingeloggte Seite verlässt, wird der NID mitübermittelt, damit der Nutzer zu der Seite mit dem Abruf der E-Mails zurückkehren kann. Ein technisch versierter Hacker kann durch die

[3] Diesem Szenario liegt ein Fall vor amerikanischen Gerichten zu Grunde. In erster Instanz wurde der ehemalige Mitarbeiter zu einer Haftstrafe von 16 Monaten vom United States District Court for the Central District of California verurteilt (D.C.No 03-50135 Cal). Die Verurteilung basierte auf 18 U.S.C. § 1030 (a) (5) (A) (Computer Fraud and Abuse Act (CFAA)).Vertreten wurde der Angeklagte von Angehörigen der Stanford Law School, namentlich von der Direktorin des Stanford Law School Center for Internet and Society. Der United States Court of Appeals for the Ninth Circuit hob das Urteil wieder auf. Die entsprechenden Entscheidungen der Gerichte sind unter http://cyberlaw.stanford.edu-/about/cases/united_states_v_mcdanel.shtml (30.05.2006) abrufbar. Weitere Artikel zu diesem Fall: Krause, Jason, The case of the ethical hacker, 7. Nov. 2003, 2 No 44 A.B.A. J.E-Report, S. 2; Springmann, Chris, The federal Government´s strange cyber-defamation case against Bret McDanel, Modern Practice October 2003, http://practice.findlaw-.com/scripts/printer_friendly.pl?page=/feature-1003.html (30.05.2006); Rasch, Mark, The Sad Tale of a Security Whistleblower, SecutityFocus 18.08.2003, http://www.securityfocus.-com/columnists/179 (30.05.2006).

NID des Nutzers theoretisch zu dessen Nutzerzugang und damit zu dessen Nachrichten gelangen.

Noch als Mitarbeiter und Administrator entdeckte der Sicherheitsexperte diese Sicherheitslücke. Er schlug seinem damaligen Arbeitgeber vor, diese theoretische Sicherheitslücke zu schließen. Dieser lehnte jedoch ab. Er vertraue darauf, dass weiterhin kein Hacker die Übertragung der NID und damit die Sicherheitslücke aufdeckt. Er war der Ansicht, dass das Risiko der Aufdeckung der Sicherheitslücke doch sehr gering wäre.

Kurze Zeit danach verließ der Sicherheitsexperte das Unternehmen. Ein halbes Jahr später stellte er fest, dass die NID weiterhin mitübertragen wird.

Die Systemkapazitäten kennend verschickte der Ex-Arbeitnehmer über den Server seines ehemaligen Arbeitgebers simultan an alle Kunden eine E-Mail mit dem Hinweis auf die Sicherheitslücke. Dieses führte zu einem Crash des Servers. Zugleich postete er die Information in Internetforen.

Durfte der Sicherheitsexperte (als Ex-Arbeitnehmer) die Kunden über die Sicherheitslücke informieren?

C Szenario 3: Unberechtigter Zugang zu Kundendaten[4]

Ein junger aufstrebender Architekt sucht in Zeiten der Bauflaute einen Nebenverdienst. Da es ihn schon lange ärgert, dass geschmackvolle Architektenlampen aus dem hochpreisigen Segment bisher nicht an Endkunden direkt abgegeben werden, offeriert er diese über einen Online-Versandshop. Den Webauftritt hat er als krea-

[4] Dieses Szenario wurde in Anlehnung an die Sicherheitslücken bei T-Com entwickelt. Diese und weitere Sicherheitslücken wurden von einem Mitglied des ccc (Chaos Computer Club) aufgedeckt. Als Mitarbeiter administrierte er ein entsprechendes WebPaket eines Kunden der T-Com. Neben der beschriebenen Sicherheitslücke entdeckte der Mitarbeiter noch weitere Varianten des Zugangs und der Möglichkeit des Zukaufs von weiteren Produkten. Durch die Identität des vorgeschlagenen Benutzernamens mit dem realen Nachnamen konnte so der Zugang zu weitern Kundenkonten erlangt werden. Darüber hinaus konnte durch das Erraten von Benutzername (etwa Telekom1) und Passwort (Telekom1) der Zugang einiger Telekommitarbeiter erlangt werden. Weiterführende und ausführliche Informationen sind zu finden unter: heise news vom 31.07.2004, http://www.heise.de/newsticker/meldung/49630 (30.05.2006), heise news vom 27.07.2004 http://www.heise.de/newsticker/meldung/49495 (30.05.2006) und heise news vom 26.07.2004 http://www.heise.de/newsticker/-meldung/49424 (30.05.2006) und Heringhaus, Dirk, No more secrets?, Datenschleuder Nr. 83, http://ds.ccc.de/083/obsoc/ (30.05.2006).

tiver Architekt selbst gestaltet und lediglich die Speicherung der Daten auf einem Server eines Providers ausgelagert.

Um dem bürokratischen Aufwand der größer werdenden Kundschaft Herr zu werden, bietet er Stammkunden und solchen, die es werden wollen, eine Registrierung an. Bei dieser werden alle für den Vertragsschluss erforderlichen Kundendaten (Name, Anschrift, Kontoverbindung/Kreditkartennummer) in einer Online-Vertragsverwaltungsdatenbank gespeichert und verarbeitet. Der Kunde kann sich online registrieren und erhält bei Registrierung ein Passwort und eine Kundennummer. Passwort und Kundennummer sind standardmäßig jeweils der Nachname des Kunden. Mit diesen eingeloggt, erhält der Kunde Zugang zu seinen Kundendaten und kann im Versandshop einkaufen, ohne jedes Mal seine Daten eingeben zu müssen. Eingeloggt erscheint folgende URL:

http://www.web-service.d-com.de/contrctview/frameset.asp?ConPK=1456

Eine Kundin, Frau Anonym, die technisch einigermaßen, aber nicht allzu versiert ist, wundert sich über den Aufbau der URL, vor allem, da die letzten Ziffern der URL ihrer Kundennummer entsprechen. Als neugierige Zeitgenossin ersetzt sie ihre Kundennummer durch eine zufällig ausgewählte weitere Nummer und tippt

http://www.web-service.d-com.de/contrctview/frameset.asp?ConPK=1457

in ihren Browser ein.

Das Fenster zeigt daraufhin die Kundendaten eines weiteren Kunden. Entsprechende Ergebnisse erzielt Frau Anonym mit weiteren, willkürlich gewählten Nummern.

Frau Anonym macht darauf hin den Betreiber des Versandshops auf die Lücke aufmerksam und übermittelt zum Beweis Kundendaten Dritter, die sie auf ihrem Rechner gespeichert hat.

Muss der Betreiber seine Kunden über diese Lücke informieren, sie insbesondere darauf aufmerksam machen, dass ihre Daten möglicherweise von einer unbestimmten Anzahl Personen eingesehen wurden?

D Szenario 4: Manipulation des virtuellen Rathauses

Stadt F plant in einer Großoffensive die niedrige kommunale Geburtenrate zu erhöhen. Unter anderem garantiert sie jedem Kind bei rechtzeitiger Anmeldung einen

Kindergartenplatz. Für diese hat die Stadt F ein Verfahren der Online-Anmeldung eingerichtet. Bewerber geben ihre Daten online ein und erhalten eine elektronische Bestätigung der Anmeldung. Die Stadt F informiert daher auf ihrer Webpräsenz im Internet:

> *„Die Plätze sind sicher. Wir bitten allerdings aus Gründen der Kalkulation und Organisation der Plätze eine Anmeldung bis spätestens zum zweiten Geburtstag des Kindes vorzunehmen.*
>
> *Eine rechtzeitige Anmeldung ist erforderlich, da die Stadt selbst vorerst keine neuen Stätten errichten, sondern, je nach Bedarf, zusätzlich zu den kommunalen auf private Betreuungseinrichtungen zurückgreifen will. Nur bei rechtzeitiger Anmeldung kann die Stadt die notwendige Kalkulation und Organisation der ausstehenden Plätze leisten. Andernfalls verschiebt sich die Zuteilung des Platzes."*

Da er den Zusagen der Stadt nicht traut, schließlich hatte der verzweifelte Vater den Slogan – „Die Plätze sind sicher" – im anderen Kontext schon mal gehört, hat V um einen Platz in einem Kindergarten näher zu kommen, die Informationsseite – respektive den unzulänglich gesicherten ftp-Server – gehackt. Er modifizierte die Informationen der Stadt F dahingehend:

> *„Die Plätze sind sicher. Wir bitten daher aus Gründen des Verwaltungsaufwandes und der Übersicht ihr Kind frühestens einen Monat vor seinem dritten Geburtstag anzumelden."*

Um engagierte Eltern tatsächlich abzuhalten, leitet er zusätzlich die Online-Anmeldung anderer Eltern auf einen eigenen Server weiter, so dass die Stadt F keine Anmeldung der Eltern erhält. Den Eltern wurde allerdings nach Abschicken der Daten eine ordnungsgemäße Anmeldung online bestätigt.

Nach einiger Zeit wurde die Stadt auf die Fehlinformation aufmerksam. Sie kann nicht feststellen, wer bereits eine Anmeldung abgeschickt hat. Da die zuständige Dezernentin aus eigener Erfahrung weiß, dass nur ein sicherer Platz die Rückkehr und Planung des erziehenden Elternteils in den Beruf ermöglicht, fragt sie sich, ob sie über die Sicherheitslücke und ihre Ausnutzung informieren muss?

KAPITEL 2 SICHERHEIT UND INTERNET

Das „Internet der Anfangszeit", das ARPANET[1], wurde entwickelt, um ein ausfallsicheres Netzwerk gewährleisten zu können. Daher wurde das ARPANET so konstruiert, dass der Datenfluss nicht über feste Wege, sondern flexibel über einen jeweils funktionierenden Weg geroutet wird. Demgemäss konzentrierte sich die Sicherheit auf den Aspekt des Funktionsausfalls. In diesem Sinne ist auch die Aussage zu verstehen, die Protokolle des ARPANET seien für *„openess and flexibility, not for security"*[2] entwickelt worden. Mit der Aufgabe des Regierungsprojekts begann die Öffnung des Netzes (operational network)[3] und aus dem ARPANET wurde 1989 offiziell das Internet[4] und andere Aspekte der Sicherheit traten in den Vordergrund.

Den Anforderungen an die Sicherheit des Internets in der Gegenwart im Teil B dieses Kapitels sollen zunächst mit Teil A abstrakte Überlegungen zum Verhältnis von Sicherheit, Technik und Recht vorangestellt werden. Zu Beginn soll mit der Erörterung der Idee von Sicherheit diese an die Kontexte Technik und Recht angenähert werden, bevor Kategorisierungen von Sicherheit aus technischer und rechtlicher Sicht dargelegt werden, die den Begriff der Sicherheit ausfüllen.

A Sicherheit

I. Idee von Sicherheit

1. Sicherheit – Idee der Technik

Der Techniker/Ingenieur, der ein Produkt entwickelt, begegnet nicht selten der Vorgabe: „So viel Sicherheit wie nötig, so wenig wie möglich." D. h. er begegnet

---

1 Advanced Research Projects Agency Network des Departments of Defense, vgl. http://de.wikipedia.org/wiki/ARPANET (30.05.2006).

2 Longstaff, Thomas/Ellis, James/Hernan, Shawn/Lipson, Howard, Security of the Internet, veröffentlicht unter, http://www.cert.org/encyc_article/tocencyc.html (30.05.2006).

3 Longstaff, Thomas/Ellis, James/Hernan, Shawn/Lipson, Howard, a.a.O., (Fn. 2).

4 Der Begriff Internet setzt sich aus „INTER-connected group of NETworks" zusammen, vgl. RFC 2664, "FYI on Questions and Answers to Commonly Asked "New Internet User" Questions"1999, S. 1. Mit RFC (Request for Comments) werden nummeriert Informationen und Standards zum Internet veröffentlicht, vgl. http://www.rfc-editor.org/ (30.05.2006).

der Sicherheit mit dem technisch Machbaren, der Praktikabilität – ist das Produkt mit Sicherheit überladen, oder kann es zum erdachten Zweck noch eingesetzt werden – und wird hier mit Sicherheit an die Grenze des finanziell Möglichen stoßen.[5] Mit dem Stichwort Praktikabilität ist auch die Benutzerfreundlichkeit der Sicherheitstechnologie angesprochen. Mit dem Stichwort der Nachfrage wird der Einfluss des Nutzers angesprochen. Zugespitzt formuliert: Nur wenn dieser konsequent Sicherheit fordert – eventuell bereit ist, dafür einen höheren Preis zu zahlen – oder das Recht Vorgaben setzt, werden Hersteller und Entwickler entsprechende Angebote machen.

Sicherheit kann durch Technik oder durch den Menschen (Nutzer) hergestellt werden. Während der Nutzer durch sein Wissen um die Technik und den vernünftigen Umgang mit der Technik einen Beitrag zur Minimierung von Gefahren leisten kann, kann die Technik zur Optimierung der Sicherheit beitragen. Sicherheit durch Technik kann infrastrukturell durch Produktsicherheit[6] oder (techno)logisch durch die Optimierung von Protokollen und der Konfiguration des Systems gewährleistet werden. Letzteres kann durch Kriterien der Quality of Service (QoS) evaluiert und so Sicherheit implementiert werden. Solche Kriterien sind etwa Laufzeit von Daten im Netz, Stabilität des Netzes, Grad der Auslastung von Netzwerkelementen und eben die Sicherheit.[7]

Die Optimierung der QoS konfligiert mit widerstreitenden Interessen. So setzt etwa der Betreiber eines Netzes die QoS unter den Prämissen der Kundenwünsche, Kostenminimierung und Wettbewerb nach dem Prinzip „nur so hoch wie nötig" an. Dagegen wünscht sich der Kunde – unter der Prämisse eines entsprechenden Verbraucherbewusstseins und einer Verbrauchererwartung hinsichtlich Sicherheit - die QoS grundsätzlich „so hoch wie möglich". Entsprechend den Wünschen (Anforderungsprofil) wird die technische Sicherheit definiert und entwickelt.[8]

---

5 Vieweg, A Safety Code as an Instrument to Tighten Technical Law?, Vortrag am World Congress Safety of Modern Technical Systems 2001, http://www.irut.de/saarbrueckene.html (30.05.2006).

6 Ob mit der Produktsicherheit auch rechtliche Anforderungen an die Software gestellt werden können, ist umstritten. So ist etwa fraglich ob das Geräte und Produktsicherheitsgesetz vom 06.01.2004 (in Kraft seit 01.05.2004) auch Software erfasst, zur Diskussion wird im weiteren Verlauf der Arbeit Stellung genommen.

7 Eberspächer, Intelligenz in Netzen, in: Tinnefeld/Phillipps/Weis (Hrsg.), Sicherheit in der Informationstechnik Institutionen und Einzelne im Zeitalter der Informationstechnik, 1994, S. 165 (167).

8 So für den Begriff der Qualität, der auch den Aspekt der Sicherheit umfassen kann, dargelegt in: Hess, /Werk, Qualitätsmanagement, Risk Management, Produkthaftung, 1995, S. 120, die

Sicherheit kann in der technischen Umsetzung ambivalent sein. Sicherheitswerkzeuge können sowohl zur Effektivierung der Sicherheit eingesetzt werden, als auch gleichzeitig dieselbe reduzieren.

Als solches ambivalentes Werkzeug seien etwa mobile Agenten genannt. Mobile Agenten sind *„kleine Software-Einheiten, die von Server zu Server durch das Internet wandern und für ihre Nutzer Aufträge erledigen“*[9]. Sicher implementiert können mobile Agenten bei der Realisierung und Verbesserung vorhandener Sicherheitsanwendungen eine wichtige Rolle spielen.[10] So können mobile Agenten als Analysten und Garanten der Sicherheit eingesetzt werden.[11]

Mittels mobiler Agenten können E-Mails verschickt werden, Flüge online gebucht oder sonstige Rechtsgeschäfte abgeschlossen werden. Bei solch sensiblen Operationen muss bei der Implementierung das Hauptaugenmerk auf die Kommunikationssicherheit gelegt werden, andernfalls reduziert der Agent als selbstständiges Angriffsziel die Sicherheit.

Je nach Kontext ist die Benutzerfreundlichkeit von Sicherheitswerkzeugen eine technische Herausforderung. Soweit sie nur mit Expertenwissen zu bedienen sind oder durch die Bedienung weitere Schwachstellen auslösen, sind diese disqualifizierende Aspekte für Sicherheitswerkzeuge in einem verbreiteten System wie dem Internet.

Festzuhalten ist, die technische Realisierung der Sicherheit ist in der Implementierung von widerstreitenden Interessen geprägt und in der Wirkung ambivalent.

2. Sicherheit – Idee des Rechts

Die Grenzen des technisch Machbaren, der Praktikabilität und des finanziell Möglichen gelten für das Recht nur bedingt. In einer pragmatischen Betrachtung kann Recht jedoch nicht Unmögliches fordern. Diese Erkenntnis ist so simpel, wie in der

---

den relativen Qualitätsbegriff abgrenzen von der „Methode“ des Abgleichs eines Ist- mit einem Soll-Zustand.

9 Fraunhofer-Institut für Graphische Datenverarbeitung IGD, Sichere Mobile Agenten, 2003, unter http://www.uni-protokolle.de/nachrichten/id/13340/ (30.05.2006).

10 Leitner, Architektur eines sicheren Mobile-Agenten-Systems, 2003, S. 111.

11 Im Einzelnen können mobile Agenten die Sicherheit des Host beurteilen und erhöhen, indem sie *„die Version und Konfiguration der installierten Software überprüfen oder Einträge in Log-Dateien überwachen.“,* Leitner, Architektur eines sicheren Mobile-Agenten-Systems, 2003, S. 112. Bei erkannter Gefahr können die mobilen Agenten die Gefahr durch Patches oder eine Anpassung der Zugriffsrechte auf Dateien bannen, a.a.O.,

Wirkung auf die Sicherheit verheerend. Die Schwierigkeiten zeigen sich etwa in der Forderung, keine bekanntermaßen unsichere Software einzusetzen. Diese Forderung ist so notwendig, wie illusionär, angesichts der täglichen Meldungen von Sicherheitslücken in Software.

Die Grenze des technisch Machbaren gilt für das Recht ebenso wie für die Technik. Allerdings mit der Erwägung, dass das Recht bereits dort Einschränkungen treffen sollte, wo eine Abwägung der technischen Machbarkeit mit dem Risiko des Schadenseintritts und der Höhe des Gefahrenpotenzials zu dem Ergebnis kommt, dass das technisch Machbare noch nicht ausreicht, um ein akzeptables Sicherheitsniveau garantieren zu können. Diese mit dem Recht zu treffende Abwägung findet sich in – wiederum von der Technik ausfüllungsbedürftigen – Rechtsbegriffen wieder. In diesem Sinne greift das Recht im Bezug auf die Sicherheit auf Formeln wie den *„Stand der Technik“*[12] zurück, um einen bestimmten Sicherheitsstandard vorzugeben.

Die Grenze der Praktikabilität und das finanziell Mögliche interessieren das Recht zunächst nicht. Das Recht greift grundsätzlich erst für Produkte, für die die Technik die beiden Aspekte zufrieden stellend berücksichtigt hat und somit eine entsprechende Marktreife erreicht ist. Unter dem Aspekt der Verhältnismäßigkeit können das technisch und finanziell Machbare im Recht Berücksichtigung finden. So macht etwa § 9 S. 2 BDSG deutlich, dass der Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen muss.

So wie die Technik keinen hundertprozentigen Schutz herstellen kann, kann das Recht keinen hundertprozentigen Schutz garantieren. Wie sicher „sicher genug“ im Sinne des Rechts ist, lässt sich nicht allgemein beantworten, sondern erfordert eine Orientierung an und Bestimmung durch die jeweils gefährdeten Rechtsgüter, was sich idealiter als rechtlich gebotenes Maß der Sicherheit in Normen widerspiegelt.[13]

Zur Gewährleistung einer tatsächlichen Sicherheit ex ante, und nicht bloß zur Wiederherstellung des Status quo ex post, sollte das Recht eher vom *„Prinzip der Vorsorge“*[14] denn dem „Prinzip der Nachsorge“ durch Haftungs- oder Strafrecht geleitet sein.

---

12 Vgl. § 3 Abs. 6 BImSchG; höherer Standard: „Stand der Wissenschaft und Technik“, § 7 Abs. 2 Nr. 3 AtG; niedrigerer Standard: „allgemein anerkannte Regeln der Technik“, § 55 Abs. 1 Nr. 3 Bundesberggesetz.

13 Murswiek, Die staatliche Verantwortung für die Risiken der Technik, 1985, S. 87.

14 Ausführlich zum Prinzip der Vorsorge: Stoll, Sicherheit als Aufgabe von Staat und Gesellschaft, 2003, S. 319 ff. Das Prinzip der Vorsorge spielt im Umweltrecht eine große Rolle,

In jedem Fall setzt die rechtliche Umsetzung von Sicherheit die Überwindung der technischen Ambivalenz voraus und löst die widerstreitenden Interessen durch ausfüllungsbedürftige Vorgaben.

II. Kategorien der Sicherheit

„Sicherheit (…) gilt es zu optimieren – und nicht „nur" zu definieren."[15] Weitergehend für die Sicherheit im Internet kann formuliert werden, dass Sicherheit nicht befriedigend pointiert definiert, dafür aber kategorisiert werden kann. Die Kategorien sollen ausgehend von den zu den Bedrohungen komplementären Schutzzielen gebildet werden. Nur wenn ein bestimmtes Schutzziel formuliert werden kann, können Bedrohungen auch als Gefahren für die Sicherheit betrachtet werden.[16] Dementsprechend kann Sicherheit als Gewährleistung des Schutzes von Personen, Sachen, Werten und Interessen gedacht werden. Grob können Bedrohungen der Sicherheit in interne und externe Sicherheitsrisiken eingeteilt werden. Interne Sicherheitsrisiken sind etwa schlecht geschulte oder desinteressierte Mitarbeiter in einem Unternehmen und dessen interne Infrastruktur. Externe Sicherheitsrisiken sind technische Angriffe durch Dritte – etwa durch Malware (Viren, Würmern, Trojanern, etc.) – auf die (Informations-)Infrastruktur.

Als Leitidee der Sicherheit kann gelten: Sicherheit ist *„die Minimierung der Verwundbarkeit von Werten und Ressourcen"*[17].

IT-Sicherheit kann als Schutz von personenbezogenen Daten und Ressourcen des Nutzers, Werten der Gesellschaft und nicht zuletzt der Reputation von Herstellern und Anbietern vor Gefahren, die mit dem Einsatz der Informationstechnik zu-

---

rechtlich verbindlich als Grundsatz der Vorsorge im Europarecht in Art. 174 Abs. 2 EG geregelt. Neben den unterschiedlichen Ausprägungen des Prinzips in weiteren Rechtsbereichen ist der alltägliche Umgang mit Gefahren von einem „Prinzip der Vorsorge" geprägt.

15 Schmid, IT-Sicherheit durch Cyberlaw?, in: thema Forschung IT-Sicherheit, 1/2004, S. 82.

16 Schumacher, Security Patterns, in: Informatik Spektrum, Band 25 Nr. 3 2002, 220 (220).

17 Gerd tom Markotten, Benutzbare Sicherheit, 2003, S. 10 mit Hinweis auf die Definition in der ISO-Norm 17799. Darüber hinaus weist Gerd tom Markotten auf vielfältige Definitionen abhängig vom disziplinären Kontext hin.

sammenhängen, bezeichnet werden.[18] IT-Sicherheit bildet deshalb keine eigene Kategorie, sondern dient vielmehr für diese Arbeit als Oberbegriff.[19]

Nach der Annäherung durch die Idee der Technik und des Rechts von Sicherheit soll Sicherheit in den Kontexten Technik und Recht konkretisiert werden. Die Kategorisierungen erfolgen vor dem Hintergrund der gemeinsamen Schutzziele.

1. Schutzziele

Schutzziele werden sowohl von Technik als auch von Recht begründet und gewährleistet. Die Technik implementiert die Schutzziele.[20] Das Recht formuliert Interessen, die durch die Implementierung von (technischen) Schutzzielen gewährleistet werden können.[21]

Den folgenden unterschiedlichen Kategorien der Sicherheit soll ein Kanon von Grundwerten der Information vorangestellt werden.[22]:

- Authentizität: Die Information stammt wirklich vom angegebenen Absender.
- Integrität: Die Information erreicht den Empfänger unverändert.
- Vertraulichkeit: Die Information kann nur der vorgesehene Empfänger lesen.
- Verfügbarkeit: Der Informationsvorgang ist unbeeinträchtigt.
- Zurechenbarkeit: Der Informationsvorgang kann unabstreitbar nachgewiesen werden.

Diese kennzeichnen das Ausmaß und die Dimension der Sicherheitsanforderungen an die technischen und rechtlichen Kategorien und stellen die zu verwirklichenden Schutzziele dar.

---

18 Droste, Konzept eines komponentenbasierten, verteilten Sicherheitsverbundes, 2002, S. 1. Als Legaldefinition der IT-Sicherheit wird immer wieder § 2 Abs. 1 BSIG zitiert, zuletzt: Heckmann, Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen, in: MMR 2006, 280 (281).

19 In einer anderen Zuordnung der Begriffe um die Sicherheit wird die Informationssicherheit als umfassender Begriff verstanden, Kersten, Sicherheit in der Informationstechnik, 2. Aufl. 1995, S. 12.

20 *Federrath/Pfitzmann*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, S. 64, Rd. 13.

21 Rechtliche Schutzinteressen können etwa die Zurechenbarkeit von Nachrichten zu Absender/Empfänger oder die rechtlich gewünschte Anonymität (vgl. § 4 Abs. 6 TDDSG) sein. Vgl. auch *Federrath/Pfitzmann*, a.a.O., S. 64, Rd. 11.

22 Vgl. etwa die vom BSI aufgeführten Ziele, IT-Grundschutzhandbuch 2005, S. 11 und 41, http://www.bsi.bund.de/gshb/deutsch/download/itgshb_2005.pdf (30.05.2006).

2. Technische Kategorien

In einem komplexen System, wie dem Internet, in dem Personen interagieren, Sachen eingebracht und verwendet sowie Interessen verfolgt werden sollen, gibt es nicht nur ein Schutzziel und somit eröffnen sich vielfältige Kategorien von Sicherheit. Ausgehend von den Ausführungen zur IT-Sicherheit und den Schutzzielen sollen jedoch folgende technische Kategorien[23] zur weiteren Spezifizierung dieser Begriffe gebildet werden.

a) Kategorie 0: Produktsicherheit

Die allgemeine Frage der Produktsicherheit einzelner Komponenten (etwa Clients) ist dem System Internet vorgeschaltet, da sie ohne Integration und Nutzung der Produkte im Internet für die Sicherheit des Internets irrelevant ist. So kann der PC auch als bloße Schreibmaschine fungieren. Die Produktsicherheit könnte allerdings bei der Realisierung von „Trusted Computing“[24] als Kategorie eine Antwort auf die Sicherheitsfrage des gesamten Systems Internet bieten. Die Produktsicherheit ist bei der Frage der strukturellen Lücken wohl eine notwendige, aber keine hinreichende Voraussetzung. Die Sicherheit oder Unsicherheit des Systems wird häufig erst durch die Kombination und Konfiguration der einzelnen Elemente – etwa beim Zusammenwirken von Programmen[25] – beurteilt werden können.

---

[23] Die Kategorien werden in Anlehnung an Eckert, IT-Sicherheit Konzept, Verfahren, Protokolle, 2005, S. 4 f. gebildet, die von Funktionssicherheit, Informationssicherheit und Datensicherheit und Datenschutz spricht.

[24] Diese anfängliche Bezeichnung hat eine Vielzahl von Synonymen: Microsoft: 'trustworthy computing', Free Software Foundation: 'treacherous computing' oder etwa Intel: 'safer computing'. Trusted Computing setzt am „größten Feind“ der Sicherheit an, dem Menschen. Die Trusted Computing Group will einen Standard für sichere PCs fördern, vgl. Anderson, Ross, Trusted Computing FAQ 1.1 – deutsch, 2004, http://moon.hipjoint.de/tcpa-palladium-faq-de.html (30.05.2006). Grundidee ist, durch die Aufdeckung von Manipulationen durch Trojaner, Viren, etc. und Datensicherheit in beide Richtungen, die Sicherheit der eigenen und fremder Daten, zu gewährleisten, vgl. Himmelein, Gerald, Trusted Computing 2004: Was vom Schlagwort übrig blieb, Vortrag am 24.06.2004 beim LinuxTag 2004, http://www.heise.de/ct/Redaktion/ghi/tc/linuxtagTC04.html (30.05.2006). Diese Gefahren haben PC-Produzenten und Softwareentwickler erkannt, vgl. eine Stellungnahme des BSI: Welche Meinung hat das BSI zu Palladium/NGSCB und TCPA/TCG?, http://www.bsi.bund.de/sichere_plattformen/trustcomp/stellung/StellungnahmeTCG1_2a.pdf (30.05.2006). Gegner behaupten, Trusted Computing bietet lediglich Sicherheit für Computerhersteller, Softwareentwickler und die Contentindustrie, Anderson, Ross, Trusted Computing FAQ 1.1 – deutsch, 2004, http://moon.hipjoint.de/tcpa-palladium-faq-de.html (30.05.2006).

[25] Vgl. Browser und Betriebssystem.

Zunächst ist zu gewährleisten, dass die einzelnen Komponenten an sich sicher sind.[26] Dieses Schutzziel kann im IT-Sektor durch die Zertifizierung von Produkten der Hard- und Software nach außen hin sichtbar gemacht werden.[27] Die Produktsicherheit ist demnach ein Teilbereich, der aber nicht die Frage nach der Sicherheit „des Ganzen", somit nach der Sicherheit des Internets, zu beantworten vermag. Zumal die Produktsicherheit bei der Nutzung eines PC ohne Internetanbindung keinen Beitrag zur Sicherheit im Internet zu leisten vermag (daher Kategorie „0"). Das Internet entsteht erst aus der Nutzung der weiteren Komponenten und ist von ihrer Konfiguration abhängig.

b) Kategorie 1: Netzsicherheit

Zunächst ist zu gewährleisten, dass das System Internet überhaupt funktioniert. Das heißt, dass die Ist-Funktionalität mit der spezifizierten Soll-Funktionalität übereinstimmt.[28] Beschrieben werden soll diese Funktionssicherheit als Netzsicherheit[29]. Primär sind damit die Verfügbarkeit und der Schutz vor dem Ausfall der physikalischen Infrastruktur verbunden. Die Erreichung dieses Schutzzieles liegt in der Verantwortung der Hersteller und Anbieter der physikalischen Infrastruktur[30], der Softwareentwickler der (techno)logischen Infrastruktur und der Netzarchitekten, die diese Komponenten zusammensetzen. Konkret betrifft die Netzsicherheit die Komponenten der Übertragungstechnik, die eingesetzten Übertragungswege, Energiezufuhr, etc.[31]

---

26 Sicherheit reicht hier von der Gewährleistung von Kurzschlüssen (Brandgefahr) bis zum produktspezifischen Beitrag zur IT-Sicherheit.

27 Eine solche Zertifizierung kann allerdings nicht immer die Grundlage von Sicherheit im Internet sein. So testet die TÜV Rheinland Group die „elektrische und mechanische Sicherheit (EN 60950)" von Hardware. Dies deckt allerdings nicht die typischen Gefahrenquellen von Angriffen im Internet ab. Software wird auf Gebrauchstauglichkeit getestet, da „*sich die Erzeugnisse immer weniger durch Preis, Funktionalität oder Leistungsfähigkeit unterscheiden, spielt die Gebrauchstauglichkeit hierbei die entscheidende Rolle.*", http://www.de.tuv.com/de/produkte_und_leistungen/produktsicherheit_und_qualitaet/ergonomie_und_gebrauchstauglichkeit/software/index.php (30.05.2006).

28 Eckert, IT-Sicherheit Konzept, Verfahren, Protokolle, 2005, S.4.

29 Der Begriff der Netzsicherheit verführt zu einer Gleichstellung mit der Sicherheit im Internet an sich. Es bedarf jedoch weiterer Kategorien der Sicherheit, da die vielfältigen Schutzziele nicht mit der Netzsicherheit alleine zu fassen sind.

30 Vgl. Kapitel 2 B II. 1. a).

31 Wie ein Fall aus der Praxis zeigt, sind bei der Netzsicherheit auch herkömmliche Alltagsdelikte nicht zu vernachlässigen. Wie einer heise Meldung zu entnehmen ist, soll ein Provider seinem ehemaligen Vertragspartner einen Server gestohlen haben. Dies hatte zur Folge, dass für die Kunden dieses Providers ein Internetzugang per DSL zeitweilig nicht mehr möglich

c) Kategorie 2: Kommunikationssicherheit

Weiterhin – ein grundsätzlich funktionsfähiges System unterstellt – ist zu gewährleisten, dass die Ist-Funktionalität mit der spezifizierten Soll-Funktionalität dieses Systems auch im Gebrauch erhalten bleibt und es zu keiner unautorisierten Veränderung des Kommunikationsvorgangs kommt. Diese soll hier als Kommunikationssicherheit bezeichnet werden.[32]

Die Kommunikationssicherheit kann etwa durch die Authentifizierung des Nutzers oder durch Verschlüsselung des Kommunikationsvorgangs gewährleistet werden. Eine technische Möglichkeit sich über Sicherheitslücken in der Kommunikationssicherheit zu informieren bieten Intrusion Detection Systeme. Durch die Analyse des Netzwerkverkehrs mittels Intrusion Detection Systemen (diese können sowohl in der physikalischen als auch (techno)logischen Infrastruktur[33] implementiert sein) werden Anomalien oder Missbrauch dem Administrator mitgeteilt, welcher entsprechende Gegenmaßnahmen treffen kann.[34]

Die Kommunikationssicherheit ist von gewerblichen, staatlichen und privaten Anbietern und Nutzern, mithin von jedem Interaktionspartner, zu gewährleisten.

d) Kategorie 3: Datensicherheit

Geht man von einem grundsätzlich funktionsfähigen System aus, ist zu gewährleisten, dass auf das System oder auf Systemressourcen nicht unautorisiert zugegriffen oder diese verändert werden können und die Systemressourcen erhalten bleiben. Diese Kategorie soll als Datensicherheit beschrieben werden.[35] Sie beinhaltet den Schutz vor Dritten („zugegriffen“) und vor dem Nutzer selbst („erhalten bleiben“). Die Adressaten dieser Kategorie sind bei den gewerblichen, staatlichen und privaten Anbietern und Nutzern zu finden.

---

war, heise news vom 31.08.2004, http://www.heise.de/newsticker/meldung/50555 (30.05.2006).

32 Der verwandte Begriff Informationssicherheit wird nicht verwendet, da betont werden soll, dass es nicht nur um die bloße Übertragung von Daten geht (Information), sondern um den persönlichen oder zweckbestimmten Austausch von Daten (Kommunikation).

33 Vgl. Kapitel 2 B II. 1. b).

34 Droste, Konzept eines komponentenbasierten, verteilten Sicherheitsverbundes, 2002, S. 8. Über eine Überwachung hinaus können Intrusion Response Systeme (automatisch) reagieren

35 Die Datensicherheit entspricht dem technisch-organisatorischen Schutz im Sinne des § 9 BDSG und Anlage zu § 9 BDSG.

e) (Kategorie 4: Interessensicherung)

Darüber hinaus – ein grundsätzlich funktionsfähiges und sicheres System unterstellt – ist zu gewährleisten, dass systemexterne Werte und Ressourcen geschützt werden. Diese sind etwa der Jugendschutz oder der Schutz von Urheberrechten. Im Gegensatz zu den Kategorien 1-3 wird diese Kategorie nicht durch die Technik indiziert. Vielmehr bedarf es zunächst einer Konkretisierung der Schutzziele durch die Gesellschaft. Erst im nächsten Schritt kann die Technik den Schutz der Interessen realisieren.[36] Diese Kategorie soll als Schutz von Werten und Ressourcen mithin als Interessensicherung beschrieben werden. Inhaltlich vom Recht vorgegeben ist die Interessensicherung keine originär technische, sondern eine derivative Kategorie.[37] Sie ist aber eine Kategorie der Sicherheit im Internet zu dem die Technik ihren Beitrag leisten kann. Die Adressaten dieser Kategorie sind etwa beim Jugendschutz im Nutzerkreis (etwa Eltern) oder mit der Implementierung technischer Schutzmechanismen bei den Anbietern zu finden.

Bestimmte Schutzziele – etwa der Jugendschutz – werden durch eine rein technische Kategorisierung der Schutzziele nicht erfasst. Eine Gefahr für den Jugendschutz kann im Internet etwa durch spezielle Inhalte (nationalsozialistische Äußerungen, Pornographie) bzw. durch ungeeignete Rezipienten (Kinder) bestehen. Die sichere Nutzung des Internets kann dann auch Sicherheit bei Inhalten fordern. Die

---

36 Soweit rechtlich formulierte Werte nur durch die Technik gewährleistet werden können, liegen der Interessensicherung technische Überlegungen zu Grunde und rechtfertigt damit eine Bewertung als technische Kategorie.

37 Zwischen der Netzsicherheit und Interessensicherung kann das Problem des Spamming (Spam) verortet werden. Spam ist eine Ausreizung des E-Mail-Dienstes zugunsten einiger weniger und zulasten „aller". Spam kann unter drei Aspekten betrachtet werden. Zum einen ist Spam technisch eine Ressourcenbelastung und kann damit bis hin zu einer Überlastung von Servern führen (Netzsicherheit). Zum anderen kann Spam als vom Verbraucher unverlangte Werbekommunikation Wettbewerbsvorteile sichern und wird somit in rechtlicher Hinsicht vom Wettbewerbsrecht be- bzw. in § 7 Abs. 2 Nr. 3 UWG „verurteilt" (Interessensicherung). So wurde Spam mit Art. 13 der Elektronischen Datenschutzrichtlinie (2002/58/EG) europaweit durch Umsetzungszwang der vorherigen Einwilligung unterstellt. In Deutschland wurde dies mit § 7 Abs. 2 Nr. 3 UWG umgesetzt. In den USA wurde mit dem "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003", oder kurz der "CAN-SPAM Act of 2003", in Kraft seit 01.01.2004, die Verbreitung von Spam normativ geregelt. Schließlich besitzt Spam unangenehmer Qualität oder Quantität einen gesellschaftlichen Aspekt (etwa Einladungen zu sexuell anzüglichen Seiten).

Sicherheit erfasst in diesem Fall eine bestimmte Nutzergruppe – Kinder und Jugendliche.[38]

Ein weiteres Schutzziel, das mit einer technischen Kategorisierung im engeren Sinn nicht erfasst – und somit in Kategorie 4 fällt, sondern durch die Anwendung von Technik ausgehöhlt werden kann, ist die Gewährleistung von Urheberrechten im Internet.[39] Hier wird die Sicherheit erst durch eine rechtliche Regelung erreicht. So sind etwa technische Kopierschutzmaßnahmen für Software ohne ein rechtliches Verbot der Umgehung kein wirksamer Schutz, sondern lediglich eine technische Herausforderung.

f) Modifikation der Kategorien durch Recht

Die technischen Kategorien können durch rechtliche Regelungen verschoben werden und damit bei Missachtung rechtlich bestimmte und somit steuerbare Konsequenzen zeitigen. Dies kann durch folgendes Beispiel ausgeführt werden.

Bei dem Nutzer, der keine Firewall installiert, funktioniert das Betriebssystem – seine sonstige Fehlerfreiheit vorausgesetzt – sicher im Sinne der Kategorie 0. Mangels Firewall können Trojaner unautorisiert Daten des Nutzers übertragen. Diese Schutzlücke betrifft die Kommunikationssicherheit in Kategorie 2, da das grundsätzlich zuverlässig funktionierende System verändert wird.

Durch Normen oder die Rechtsprechung könnte diese Sicherheitslücke der Kategorie 2 in die Kategorie 0 verschoben werden – etwa durch eine Auslegung der notwendigen Beschaffenheit eines Produkts durch die Rechtsprechung. Zudem sind rechtliche Normen[40] denkbar, die eine Firewall als Komponente eines sicher funktionierenden Betriebssystems begreifen und deren Einsatz vorschreiben. Damit wäre eine fehlende Firewall ein Defizit der Kategorie 0. Vorteile wäre zum einen, dass in der Kategorie 0 meist professioneller Sachverstand befasst ist (etwa Softwareentwickler und Netzwerkadministratoren), zum anderen, dass die Sicher-

---

38 Einen rechtlichen Rahmen schafft etwa die Entscheidung Nr. 1151/2003/EG des Europäischen Parlaments und des Rates (...) über die Annahme eines mehrjährigen Aktionsplans der Gemeinschaft zur Förderung der sichern Nutzung des Internets durch die Bekämpfung illegaler und schädlicher Inhalte in globalen Netzen, ABl. Nr. L 162, vom 01.07.2003, S. 1. Zurzeit durch den Vorschlag für eine weitere Entscheidung, KOM(2004)91 endg. vom 12.03.2004, in Überarbeitung.

39 Dieses Schutzziel findet sich etwa in § 95a UrhG geregelt, der das geistige Eigentum durch technische Maßnahmen (Verbot der Umgehung des Kopierschutzes) schützt.

40 Etwa in Rechtsverordnungen nach §§ 4 Abs. 1 i.V.m. 3 Abs. 1 GPSG.

heit nicht von der individuellen Implementierung der Firewall durch den Nutzer abhängig ist. Nicht zuletzt könnten diese Konsequenzen durch haftungsrechtliche Regelungen (Produkthaftung) durchgesetzt werden. Regelungen, die für die Kommunikationssicherheit in dieser Klarheit bisher nicht zur Verfügung stehen.

3. Rechtliche Kategorien

Eine rechtliche Kategorisierung könnte über die klassische Einteilung in Öffentliches, Zivil- und Strafrecht versucht werden. Dem steht entgegen, dass das „Internetrecht“[41] oder das „Cyberlaw“[42] eine Querschnittsmaterie ist. Gleiches gilt für das IT-Sicherheitsrecht als einem Ausschnitt des Internetrechts oder Cyberlaw.

Eine eigene Kategorienbildung entsprechend der technischen ist für das Recht zunächst nicht indiziert. Ein Netzsicherheitsrecht ist ebenso wenig weiterführend wie die Kategorie Kommunikationssicherheitsrecht. Klassische „Schutzziele“ in der juristischen Terminologie als zu schützende Rechtsgüter bezeichnet, sind im Recht als „Leben“, „körperliche Unversehrtheit“, „Freiheit“ und „Eigentum“[43] oder allgemein als „Öffentliche Sicherheit“ formuliert. Der Schutz eines PC vor Viren (Netz- oder Kommunikationssicherheit) wird im Recht als Schutz des Eigentums subsumiert.[44] Der Detailliertheit der technischen Kategorisierung steht eine abstrakt vorzunehmende rechtliche Annäherung an die technischen Schutzziele gegenüber.

Eine rechtliche Kategorienbildung soll vielmehr unter dem Aspekt, wie Sicherheit unter den Akteuren aufgeteilt werden kann, versucht werden. Die Frage und Suche nach Akteuren ist ein Ansatzpunkt, der Recht und Technik eint, unabhängig von abstrakt oder konkret formulierten Schutzzielen oder Rechtsgütern. Bei Sicherheit

---

41 Vgl. Hoeren, Internetrecht, 2004, der jedoch nicht definitorisch klärt was, Internetrecht ist, vielmehr in den ersten Seiten zum Begriff des Informationsrechts Stellung nimmt, a.a.O., S. 1 ff.

42 Zum Begriff Cyberlaw: Schmid, Cyberlaw – eine neue Disziplin im Recht?, in: Hendler/Marburger/Reinhardt/Schröder (Hrsg.), Jahrbuch UTR 2003, S. 449 (468); unter Cyberlaw können demnach alle Regelungsbereiche zusammengefasst und verstanden werden, die sich mit dem Internet beschäftigen, etwa das Telekommunikationsrecht, Datenschutzrecht, EDV- und Computervertragsrecht, Domainrecht, Urheberrecht oder das Strafrecht etwa in einer völkerrechtlichen Ausprägung als Convention on Cybercrime. Vgl. auch den Inhalt bei Boehme-Neßler, Cyberlaw, 2001.

43 Vgl. etwa die zwar nicht abschließende, aber dennoch exemplarische Aufzählung in § 823 Abs. 1 BGB. Diese sind als Schutzobjekte liberaler Tradition bezeichnend, Isensee, Das Grundrecht auf Sicherheit, 1983, S. 23.

44 Dies hat insbesondere Folgen für das deliktische Haftungsrecht, welches eine Verletzung an einem Rechtsgut und einen daraus kausal folgenden Schaden voraussetzt.

im rechtlichen Kontext kann jedoch pointiert gefragt werden, wer für den Schutz vor Schäden von Rechtsgütern verantwortlich ist. Klassisch ist dies im Zivilrecht eine Frage nach der Pflicht zur Schadensvermeidung und dem Anspruch auf Schadensvermeidung bzw. -ersatz.

Je nach rechtlichem Kontext können zu schützende Rechtsgüter festgelegt bzw. die technischen Kategorien der Schutzziele rechtlich berücksichtigt werden. Mit dem Recht kann festgelegt werden, wer wie die Rechtsgüter (technisch) zu schützen hat (Handlungsanweisung). Mit dieser Verpflichtung zum Schutz korreliert ein Anspruch auf Schutz, wenn durch entsprechende Haftungsnormen oder vertraglich ein subjektives Recht eines Einzelnen normiert ist.

Die Handlungen der Akteure können entsprechend den Verhaltensanforderungen als rechtswidrig oder rechtsmäßig angesehen werden. Im Regelfall greifen diese Bewertungen jedoch nicht, wenn das Gesetz keine konkrete Handlungsanweisung gibt. In diesem Fall ist das Recht durch (Eigen)Verantwortung geprägt.

Betrachtet man die Kategorie – die im Weiteren als (Eigen)Verantwortung bezeichnet werden soll – so wird klar, dass das System der Sicherheit nicht zwangsläufig auf einem austauschenden und einklagbaren Korrelat Anspruch-Verpflichtung basieren muss und kann. Der Verantwortung wohnt die Freiheit – bei Tragung der entsprechenden Konsequenzen – inne, die Verantwortung gerade nicht wahrzunehmen, diese zu delegieren oder etwa durch Versicherungen zu realisieren.

Im Folgenden sollen der Anspruch auf Sicherheit, die Pflicht zur Sicherheit und die (Eigen)Verantwortung als Kategorien des Rechts dargestellt werden.

a) Anspruch auf Sicherheit

Ein Anspruch auf Sicherheit im engen Sinne, d. h. im Sinne des § 194 Abs. 1 BGB als Recht, von einem anderen ein Tun oder Unterlassen verlangen zu können, ist in zweifacher Hinsicht zu denken. Zum einen kann er als ein mit der Pflicht zur Sicherheit korrelierender Anspruch bestehen, so etwa die werkvertragliche Pflicht eines Hosting Provider[45] zur Verfügbarkeit der Server (Netzsicherheit).

---

[45] Exemplarisch können die AGB von Strato, einem großen Anbieter von „Webpräsenzen", herangezogen werden, unter „2.3. Leistung" heißt es: *„Die Verfügbarkeit der STRATO Server und der Datenwege bis zum Übergabepunkt in das Internet (Backbone) beträgt mindestens 99 % im Jahresmittel. STRATO weist den Kunden darauf hin, dass Einschränkungen oder Beeinträchtigungen der von ihr erbrachten Dienste entstehen können, die außerhalb des Einflussbereiches von STRATO liegen. Hierunter fallen insbesondere Handlungen Dritter, die nicht im Auftrag von STRATO handeln, von STRATO*

Ein Anspruch auf Sicherheit realisiert sich meist erst ex post im Haftungsrecht.[46] Der Anspruch setzt einen Anspruchssteller und einen Anspruchgegner voraus. Diese interagieren im Bereich der IT-Sicherheit regelmäßig erst dann, wenn „das Kind in den Brunnen gefallen ist". Diese Interaktion betrifft letztendlich die Frage, wer den Schaden zu tragen hat.[47] Das Erfordernis, einen Schaden beziffern zu können, ist eine große Hürde der Realisierung der ex post-Sicherheit. So ist strittig, ob ein Schaden im rechtlichen Sinne vorliegt, wenn etwa aufgrund von der Verbreitung von Viren Daten auf dem PC gelöscht werden – dies hängt auch von der Beurteilung der Sacheigenschaften von Daten ab. Regelmäßig wird diesen eine Sacheigenschaft zugesprochen, soweit sie auf einem Datenträger verkörpert sind.[48] Neben dem „Ob" ist auch die Frage nach der Höhe des Schadens zu klären. Wie ist etwa der Ausfall eines Servers von einem Tag in einem Unternehmen zu beziffern, welches dadurch nicht mittels E-Mail kommunizieren kann?

Zum anderen kann der Anspruch auf Sicherheit als Anspruch gegen den Staat, eine bestimmte Lebenswirklichkeit und einen Rechtsgüterschutz zu gewährleisten, gedacht werden. Typischerweise realisiert sich der „Anspruch" gegen den Staat in den Grundrechten des Grundgesetzes. Die Frage nach einem konkreten „Grundrecht auf IT-Sicherheit" in der Verfassung kann schnell beantwortet werden. In einer grammatischen Auslegung trifft die Verfassung keine Regelung zur IT-Sicherheit. In grammatikalischer Auslegung ist jedoch auch ein abstraktes und generelles „Grundrecht auf Sicherheit" im Grundgesetz nicht enthalten. Sicherheit wird an mehreren Stellen des Grundgesetzes erwähnt, die im Kontext dieser Arbeit nicht

---

nicht beeinflussbare technische Bedingungen des Internet sowie höhere Gewalt. Gleichermaßen kann auch die vom Kunden genutzte Hard- und Software oder technische Infrastruktur (z.B. DSL-Anschluss eines anderen Anbieters) Einfluss auf die Leistungen von STRATO haben. (…)", http://www.strato.de-/full/details/agbbestell.html (30.05.2006). Eine grundsätzliche Verfügbarkeit von 99% bedeutet immerhin, dass die Server an 3,65 Tagen im Jahr vom Netz sein können.

46 Denkbar sind, wenn die (IT-)Sicherheit Bestandteil einer fehlerfreien oder vollständigen Erfüllung eines Vertrages ist, auch Ansprüche auf Gewährleistung oder Erfüllung. Diese vertraglichen Ansprüche sollen jedoch nicht im Vordergrund der Betrachtung stehen.

47 Im Bereich der vertraglichen Haftung (Gewährleistung) für fehlerhafte Software werden die unpassenden Regelungen (in manchen Ländern soll keine Haftung für fehlerhafte Software existieren) für die Softwaregewährleistung als eine rechtliche Ursache für unsichere Software herangezogen (weiter rechtliche Ursachen sollen in den „Intellectual Property Laws" und „Trade secret laws" liegen), Gehring, Software Development, Intellectual Property, and IT Security, in: Journal of Information Law & Technology 2003, Issue 1, http://-elj.warwick.ac.uk/jilt/03-1/gehring.htm (30.05.2006).

48 Statt vieler: Libertus, Zivilrechtliche Haftung bei Computerviren, in: MMR 2005, 507 (508). Nachweis des Meinungstandes bei Spindler/Klöhn, Neue Qualifikationsprobleme im E-Commerce, in: CR 2003, 81 (82 Fn. 12); mit weiteren Hinweisen zur Sacheeigenschaft der Software: Hilty, Der Softwarevertrag, MMR 2003, 3 (3 insb. Fn. 3 und 4).

weiterführend sind.[49] In einer verfassungshistorischen Interpretation führt Isensee jedoch aus, dass die Gewährleistung von Sicherheit die Grundannahme und Legitimation für die Existenz des Staates überhaupt sei.[50] Wie Isensee weiter ausführt, könne diese Grundlage des Staates mit dem Verständnis der vom Bundesverfassungsgericht entwickelten grundrechtlichen Schutzpflichten im Sinne eines Grundrechts auf Sicherheit angenommen werden.[51] Dieses Verständnis wird auch in der weiteren Literatur rezipiert:

> *„Der Gewinn, den man aus der Argumentationsfigur des „Grundrechts auf Sicherheit" ziehen kann, liegt darin, dass deutlich wird, dass die effektive Gewährleistung von Grundgütern ein aktives Tun, eine Schutzbemühung des Staates voraussetzt, die in der Wirklichkeit wirksam ist."*[52]

In Zusammenhang mit den Konzeptionen des Grundrechts als Freiheitsrecht und dem Grundrecht als Abwehrrecht kann das „Grundrecht auf Sicherheit" um einen weiteren Aspekt beleuchtet werden. Dem Grundgesetz ist mit dem Verständnis Isensees und dem Bundesverfassungsgericht[53] so eher eine „Pflicht" des Staates zum Schutz denn ein Anspruch des Bürgers auf Schutz zu entnehmen – allgemein formuliert und anerkannt als *„Lehre von den grundrechtlichen Schutzpflichten"*.[54] Diese Schutzfunktion der Grundrechte ist in erster Linie vom Gesetzgeber zu er- und auszufüllen, der in der Umsetzung eine Einschätzungsprärogative besitzt.[55] Ein Anspruch auf Schutz und damit Sicherheit bei legislativer Untätigkeit ist in der engen Bedeutung des Anspruchs damit nicht verbunden. So wird konstatiert:

> *„Ein „Grundrecht auf Sicherheit" kann über die allgemeinen grundrechtlichen Schutzpflichten hinaus allenfalls eine appellative Wirkung haben."*[56]

Der Staat kann seine Schutzbemühungen nicht in jedem Bereich voll entfalten. So steht etwa die allgemeine Handlungsfreiheit aus Art. 2 Abs. 1 GG einem aufdrängenden Schutz des Staates grundsätzlich entgegen. Sicherheit ist in verfassungsrechtlicher Hinsicht ein auszubalancierendes Verhältnis von Schutz und Freiheit.[57]

---

49 Etwa Art. 24 Abs. 2 GG kollektive Sicherheit.

50 Isensee, Das Grundrecht auf Sicherheit, 1983, S. 4 mit Bezug auf Hobbes.

51 Isensee, a.a.O., S. 33. Im Weiteren geht Isensee auf die Qualität und die Struktur dieses „Grundrechts" ein. Insbesondere betont er den Vorbehalt des Gesetzes: *„Die grundrechtliche Legitimität ersetzt nicht die Legalität."*, a.a.O., S. 43.

52 Stoll, Sicherheit als Aufgabe von Staat und Gesellschaft, 2003, S. 5.

53 Vgl. Serie der Urteile des BVerfG zu den Schutzpflichten, bei *Dreier*, in: Dreier (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 2. Aufl. 2004, Vorb. Rd. 102, Fn. 427.

54 Ausführlich zu den Grundrechten als Schutzpflichten, *Dreier*, in: Dreier (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 2. Aufl. 2004, Vorb. Rd. 101 ff.

55 *Dreier*, in: Dreier (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 2. Aufl. 2004, Vorb. Rd. 102 f.

56 Gusy, Gewährleistung von Freiheit und Sicherheit, in: VVDStRL 63 (2004), S. 151 (170).

57 Stoll, Sicherheit als Aufgabe von Staat und Gesellschaft, 2003, S. 11.

Bezogen auf die aus technischer Sicht formulierten Schutzziele bedeutet dies, dass der Staat verfassungsrechtlich verpflichtet ist, sich um diese Schutzziele zu bemühen. Bemühen soll andeuten, dass Art und Ausmaß der Gewährleistung des Staates für die Sicherheit und der Beitrag des Einzelnen und der Gesellschaft mit jeder Aufgabe neu bestimmt werden müssen. An dieser Stelle soll auf die Debatte um die sinkende Leistungsfähigkeit und die Steuerungsunfähigkeit des Staates nur verwiesen werden.[58]

b) Pflicht zur Sicherheit

Die Rechtsordnung postuliert keine allgemeine Pflicht andere vor Schäden zu bewahren.[59] Eine Pflicht zur Sicherheit soll daher in ein einer ex ante- und einer ex post-Perspektive entwickelt und dargestellt werden.

aa) Pflicht zur Sicherheit aus einer ex ante-Perspektive

Soweit die Pflicht durch Anforderungen an ein Produkt oder einen Prozess ex ante konturiert werden kann, ist die Pflicht zur Sicherheit eine ex ante-Betrachtung. Die Pflicht zur Sicherheit ist (normativ nicht faktisch) zwingend zu realisieren, wo das Recht explizit Sicherheit vorschreibt, etwa die Anlagensicherheit im Atomrecht. Ohne die Einhaltung bestimmter sicherheitsrealisierender Vorschriften darf eine Anlage nicht in Betrieb genommen werden.[60]

Die Pflicht zur Sicherheit kann sich in personellen, produkt- oder prozessorientierten Regelungen wieder finden. So schreibt etwa § 109 Abs. 3 S. 1 TKG vor, dass ein Sicherheitsbeauftragter oder eine Sicherheitsbeauftragte zu benennen ist (personelle Regelung), nach § 9 BDSG sind technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten zu treffen (produktorientierte Regelung) und § 109 Abs. 3 S. 1 TKG schreibt zusätzlich die Erstellung eines Sicherheitskonzepts vor (prozessorientierte Regelung).

Diese drei Beispiele machen deutlich, dass das Recht zwar zur Sicherheit durch unterschiedliche Regelungen verpflichtet, Sicherheit aber nicht garantieren kann. Allerdings kann sich das Gesetz an eine „Garantie der Sicherheit“ nur annähern. So ist etwa die Benennung eines Sicherheitsbeauftragten zwar Pflicht, aber ohne nor-

---

58 Mit Beiträgen und weiteren Nachweisen: Grimm (Hrsg.), Wachsende Staatsaufgaben – sinkende Steuerungsfähigkeit des Rechts, 1990.

59 Koch, Haftung für die Weiterverbreitung von Viren, in: NJW 2004, 801 (803).

60 Vgl. § 7 Abs. 2 AtG.

mierte Regelungskompetenzen, Unabhängigkeit oder Sanktionsmechanismen nicht unbedingt effizient und weit von einer „Garantie“ entfernt.

Das Bedürfnis und Erfordernis einer „Garantie“ ist entsprechend unterschiedlicher Gefahrenpotenziale in unterschiedlichen Bereichen unterschiedlich ausgeprägt. So sollte sich etwa die Handhabung der operationellen Risiken eines Kreditinstituts beim Online-Banking durch entsprechende Vorschriften eher einer „Garantie“ annähern, wohingegen die Risiken eines Unternehmens bei einer bloßen werbenden Webpräsenz lediglich zu minimieren sein dürften.

Im Bereich der IT-Sicherheit im Internet steht die gesetzliche Entscheidung (noch) aus, ob eine so verstandene Pflicht zur Sicherheit Ausnahmeregelungen für besonders prekäre Konstellationen schafft – etwa zu treffende Sicherheitsanforderungen bei einer Gesundheitskarte[61] – oder ob im Regelfall Sicherheitsvorkehrungen für jede Infrastruktur und Anwendungen zu treffen sind.

bb) Pflicht zur Sicherheit aus einer ex post-Perspektive

Ebenso lässt sich eine Pflicht zur Sicherheit in einer ex post-Betrachtung entwickeln. Verstanden etwa als Verkehrssicherungspflicht kann Sicherheit nicht im obigen Sinne „garantiert“ werden, weil Mechanismen zur Überprüfung der Umsetzung regelmäßig nicht installiert sind, sondern die Umsetzung und Realisierung der Sicherheit einem Abwägungsprozess ausgesetzt wird. Der Abwägungsprozess betrifft die Entscheidung des Einzelnen, die Sicherheit ex ante tatsächlich zu realisieren oder ex post im Falle der Realisierung des Risikos die Folgen zu tragen, d. h. zu

---

61 Etwa erfordert die „Server-Lösung“ der Gesundheitskarte, vgl. heise news vom 16.07.2004, http://www.heise.de/newsticker/meldung/49157 (30.05.2006), oder die geplante „Server-Lösung“ der französischen Gesundheitskarte, heise news vom 21.07.2004, http://-www.heise.de/newsticker/meldung/49266 (30.05.2006), Regelungen zur Sicherheit hinsichtlich Authentifizierung und Verschlüsselung (die Gesundheitskarte kann im Wege der zentralen Datenspeicherung („Server-Lösung“) oder durch die Speicherung der Daten auf der Karte realisiert werden („Karten-Lösung“)). Eine weitere „prekäre Konstellation“ findet sich im Bereich des E-Government: vgl. etwa die Vorschriften zur elektronischen Übermittlung von Dokumenten an die Gerichte, vgl. (Artikel)Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz, BGBl. 2005 I Nr. 18, 29.03.2005, S. 837; im Bereich der Online-Wahlen ist etwa das Pilotprojekt des Landesbetriebs für Datenverarbeitung und Statistik aus Brandenburg zu nennen. Im Rahmen dieses Projektes wurde temporär für die Durchführung der Personalratswahlen die Erste Verordnung zur Änderung der Wahlordnung zum Landespersonalvertretungsgesetz vom 29.01.2002 erlassen. In dieser Erprobungsregelung wurden explizite Anforderungen an die Sicherheit der Server und die Übertragung der Stimmabgabe gestellt, vgl. http://www.brandenburg.de/evoting/pr_wahl2002_-recht.htm (30.05.2006).

haften. Zudem ist die tatsächliche Möglichkeit des Geschädigten, Schadensersatz[62] für einen Schaden aufgrund fehlender Sicherheit, abzuwägen.

Die im Deliktsrecht begründete Verkehrssicherungspflicht scheint für eine Diskussion der Informationspflichten für die IT-Sicherheit deshalb interessant, weil auch diese erfordert, die Schäden

> *„in Bereichen, in denen menschliches Zusammenleben stattfindet und der Einzelne potenziell einer Gefährdung durch seine Mitmenschen ausgesetzt ist, bestimmte Pflichten zur Rücksichtnahme auf die Rechtsgüter festzulegen."*[63]

Welches Verhalten – respektive Information – vom Einzelnen zu fordern ist, damit er seiner Verkehrssicherungspflicht genügt, mithin für sein Verhalten nicht deliktisch verantwortlich gemacht werden kann, soll im Kapitel 5 diskutiert werden. Da in diesem deliktsrechtlichen Umfeld die Erreichung von Sicherheit nicht rechtlich zu garantieren ist, soll im Folgenden die Chancen durch eine ex ante zu realisierende Eigenverantwortung betrachtet werden.

c) (Eigen)Verantwortung

Im Kontext des Internets wird teilweise entsprechend dem *„Internet als rechtsfreien Raum"*[64] vom Internet als *„verantwortungsfreien Raum"*[65] gesprochen. Dies ist eine Sicht nur auf die Risiken des „grenzenlosen" Internets, die die Chancen für die Erhöhung der Sicherheit durch die Übernahme von Verantwortung unberücksichtigt lässt. Die Risiken des „verantwortungsfreien Raums" sind die mangelnde Greifbarkeit und Individualisierbarkeit, mithin die Durchsetzung der Verantwortung für Angriffe. Teilweise resultieren diese in der fehlenden Reichweite ordnungs- und vollzugsrechtlicher Instrumente. Verantwortung wird so in einer ex post-Betrachtung der (zivil- oder strafrechtlichen) Haftung gleichgestellt. Verantwortung in diesem Sinne ist somit dem Bereich der Pflicht zur Sicherheit zuzuordnen.

---

62 Der Schadensersatz hängt etwa im Rahmen von § 823 Abs. 1 BGB nicht alleine von der Verletzung der Verkehrssicherungspflicht ab, sondern erfordert zudem den Nachweis einer Rechtsgutverletzung und eines Verschuldens.

63 Raab, Die Bedeutung der Verkehrssicherungspflichten, in: JuS 2002, 1041 (1043).

64 Wenning, Das Internet - ein rechtsfreier Raum?, in: JurPC Web-Dok. 16/1997.

65 Vgl. Fiedler, Rechtssicherheit im Internet – kein verantwortungsfreier Raum?, in Reinemann (Hrsg.), Regieren und Verwalten im Informationszeitalter, 2000, S. 326 (326 ff.), der das Vermögen und die Verantwortlichkeit des Staates für die Rechtsdurchsetzung im Internet in Frage stellt, da das Internet eine Realisierung gemeinschaftsbezogener Verantwortung kaum mehr möglich mache. Das Ergebnis sei ein verantwortungsfreier Raum in dem Sinn, dass der Einzelne Verantwortung nur nach seinem Gutdünken zu übernehmen braucht, da Zwang und Sanktionen für die Übernahme von Verantwortung fehlen würden.

Die Chancen für die Realisierung von Sicherheit liegen allerdings in einer Eigenverantwortung[66] im Sinne eines ex post „rechtsfreien“[67] – d. h. keinem Haftungsanspruch ausgesetzten – Verantwortungsbewusstseins für die Sicherheit. Im Unterschied zur Selbstverantwortung, die ein ethisches Prinzip gegenüber sich selbst sein soll, kann Eigenverantwortung als Appell zur Verantwortung für sich und andere rechtlich verankert werden.[68] Als rechtliches Pendant zur Selbstverantwortung ist die Eigenverantwortung zudem ein wesentlicher Grundsatz der Privatautonomie.[69]

Eigenverantwortung findet sich zum einen als staatliche im Grundgesetz (1) und einfachgesetzlich als gesellschaftliche Verhaltensprämisse wieder (2) und besitzt zum anderen eine hier interessierende Rolle im Bereich der Haftung (3). Abschließend soll die Eigenverantwortung als Infrastrukturverantwortung des Staates dargestellt werden (4).

(1) Staatliche Eigenverantwortung kann dem Verantwortungsträger einen Bereich zuweisen, innerhalb dessen er weisungsunabhängig berechtigt und verpflichtet ist, seine Aufgaben zu erfüllen.[70] Die so verstandene Eigenverantwortung beschreibt eine *„Kontrollgrenze, also gewissermaßen einen Steuerungsverzicht.“*[71] Insoweit bedeutet Eigenverantwortung (rechtliche) Verantwortungsfreiheit für den Verantwortungsträger – etwa die Kommune – und markiert eine Grenze der bundesverfassungsrechtlichen Kontrolle der Regierung, des Gesetzgebers und der Selbstverwaltung.[72]

---

66 So auch im Rahmen des Umweltrechts Breuer, Zunehmende Vielgestaltigkeit der Instrumente im deutschen und europäischen Umweltrecht, in: NVwZ, 1997, 833 (837): *„In Ermangelung ordnungsrechtlicher und vollzugsbehördlicher Instrumente ist (…) auf marktorientierte Instrumente und die Eigenverantwortung der wirtschaftlichen Unternehmen zu setzen.“*

67 Rechtsfrei ist nicht gleichzusetzen ohne rechtliche Relevanz. Eine rechtliche Relevanz hat die Eigenverantwortung dort, wo sie in Kriterien der rechtlichen Argumentation und Beurteilung eines Sachverhalts eingestellt wird; etwa im Rahmen der deliktischen Verkehrssicherungspflichten sind die berechtigten Sicherheitserwartungen der betroffenen Verkehrskreise oder im Rahmen des Mitverschuldens ist die Eigenverantwortung als Obliegenheit zu berücksichtigen. Diese Erwartungen reduzieren sich in dem Maße, wie eigenverantwortliche Vorsorge vor Schäden eine Sicherheitslücke minimiert, vgl. Koch, Haftung für die Weiterverbreitung von Viren, in: NJW 2004, 801 (804). Als Selbstschutz kann die Eigenverantwortung auch im Rahmen eines Mitverschuldens nach § 254 Abs. 1 BGB zu berücksichtigen sein, Libertus, Zivilrechtliche Haftung bei Computerviren, in: MMR 2005, 507 (511).

68 Murswiek, Die staatliche Verantwortung für die Risiken der Technik, 1985, 51.

69 Loritz, Aufklärungs- und Informationsbeschaffungspflichten, in: NZG 2002, 889 (890).

70 Murswiek, Die staatliche Verantwortung für die Risiken der Technik, 1985, 51. Im Gesetz findet sich dies etwa in Art. 28 Abs. 2 und 65 S. 2 GG wieder.

71 Röhl, Verwaltungsverantwortung, in: Die Verwaltung, Beiheft 2, 1999, S. 33 (39).

72 Röhl, a.a.O., S. 33 (40), mit Hinweisen zur Erfüllung grundrechtlicher Schutzpflichten; BVerfG, Beschluss v. 14.01.1981 – 1 BvR 612/72, BVerfGE 56, 54 (80 f.); BVerfG, Beschluss v. 06.05.1997 – 1 BvR 409/90 BVerfG, 96, 56 (64) und BVerfG, Urteil v. 12.07.1994

(2) Eigenverantwortung findet sich einfachgesetzlich in Bereichen des „sozialen Netzes“[73]. Etwa: § 6 SGB XI Soziale Pflegeversicherung [Eigenverantwortung]

> *„Die Versicherten sollen durch gesundheitsbewußte Lebensführung, durch frühzeitige Beteiligung an Vorsorgemaßnahmen und durch aktive Mitwirkung an Krankenbehandlung und Leistungen zur medizinischen Rehabilitation dazu beitragen, Pflegebedürftigkeit zu vermeiden*

Das „soziale Netz“ ist ein Bereich, in dem ein verantwortungsbewusstes und damit ein gemeinschaftsverantwortliches (das Netz und Ressourcen nicht überstrapazierendes) Verhalten zur Prämisse und Notwendigkeit gemacht ist. Der Einzelne soll durch das Konzept der Eigenverantwortung für die Verwirklichung des Gemeininteresses herangezogenen werden.[74] Die Notwendigkeit von Information für die Wahrnehmung von Eigenverantwortung wird deutlich, wenn es in § 7 Abs. 1 SGB XI Soziale Pflegeversicherung heißt:

> *„Die Pflegekassen haben die Eigenverantwortung der Versicherten durch Aufklärung und Beratung (…) zu unterstützen (…).“*

Diese Gedanken lassen sich für die Sicherheit im Netz Internet übertragen.

(3) Verantwortung kann in Eigen- und (Fremd-)Verantwortung unterschieden werden. Unter dem angesprochenen Haftungsaspekt ist Verantwortung ein Zurechnungsbegriff, während Eigenverantwortung – nicht lediglich ein Pleonasmus der Verantwortung[75] – eine eigene Qualität durch die Sicherung einer „rechtlichen Sicherheitslücke“ erhalten kann. Diese Unterscheidung wird in der Praxis nicht immer trennscharf sein. So kann die Zugänglichkeit von Daten eines Unternehmens – grundsätzlich eine in Eigenverantwortung zu treffende Entscheidung – eine Frage von Verantwortung werden, wenn personenbezogene Daten Dritter im Unternehmen gespeichert und so für Dritte zugänglich werden. Letzteres indiziert eine Eigenverantwortlichkeit, die – im Unterschied zur Verantwortung für eigene Daten – eigene Sicherungsmaßnahmen fordert.[76]

-2 BvE 3/92, 5/93, 7/93, 8/93, BVerfGE 90, 286 (389 f.); BVerfG, Beschluss v. 17.07.1996 - 2 BvF 2/93, BVerfGE 95, 1 (16), zum Kernbereich exekutiver Eigenverantwortung.

73 Ebenso: § 1 S. 2 SGB V Gesetzliche Krankenversicherung [Solidarität und Eigenverantwortung]:
„Die Versicherten sind für ihre Gesundheit mit verantwortlich; sie sollen durch eine gesundheitsbewusste Lebensführung (…) dazu beitragen (…) Krankheit (…) zu vermeiden (…).“

74 Röhl, Verwaltungsverantwortung, in: Die Verwaltung, Beiheft 2, 1999, S. 33 (42).

75 So aber Di Fabio, Das Kooperationsprinzip, in: NVwZ 1999, 1153 (1154) zum Verhältnis von Verantwortung und Eigenverantwortlichkeit.

76 Zum Unterschied von Eigenverantwortung und Eigenverantwortlichkeit auf staatlicher Ebene: Ruge, Die Gewährleistungsverantwortung des Staates, 2004, S. 165. Während Eigenverantwortung mit Verantwortungsfreiheit gleichzusetzen sei, indiziere die Eigenverantwortlichkeit eine selbstständige Aufgabenerfüllung ohne Unterstützung Dritter.

Eigenverantwortung kann darüber hinaus auch dort relevant werden, wo keine konkrete rechtliche Regelung des Verhaltens vorhanden oder möglich ist oder greift. Über § 254 BGB ist die Eigenverantwortung als Obliegenheit rechtlich zu berücksichtigen.[77] Auch können durch die Betonung der Eigenverantwortung Entscheidungsspielräume jenseits vom Recht erst erwachsen.[78] Insoweit kann Eigenverantwortung eine bewusste und unbewusste rechtsersetzende Funktion haben, die gerade im gesellschaftlichen Netz Internet eine Relevanz besitzen kann, etwa beim Auseinanderfallen von Schadensrisiko und Systemsicherheit. So realisiert sich der überwiegende Schaden bei einem gehackten Server, der als Viren- oder Spamverteiler genutzt wird, nicht bei dem Betreiber des „unsicheren" Servers, sondern bei Dritten. Der Serverbetreiber sollte an exponierter Stelle nicht nur in Eigenverantwortung, sondern auch für Dritte in Sicherheit investieren.[79]

Die Verantwortung wird durch den Prozess der Verantwortungsteilung von Hersteller und Entwickler von Hard- und Software, Administratoren der Netze- und Systeme und Nutzern portioniert, so dass letztendlich die Verantwortung und die Zurechenbarkeit der Haftung des Einzelnen auf ein niedrigeres Niveau reduziert werden.[80] Eine wirksam wahrgenommene Eigenverantwortung kann jedoch über den so verstandenen Teil an der Gesamtverantwortung, bis hin zu einer Gemeinschaftsverantwortung für die Interaktionspartner im Internet (etwa bei selbsttätiger Weiterverbreitung von Viren über E-Mails ohne Wissen und Wollen des Nutzers[81]), hinausgehen. Nicht zuletzt ist eine Normierung oder Annahme einer bloß appellie-

---

77 Zivilrechtlich kann die Eigenverantwortung dann als Obliegenheit bezeichnet werden. Vgl. etwa Bartl, „Jahr-2000-Problem", in: NJW 1999, 2144 (2145).

78 Kloepfer, Staatliche Informationen, 1998, S. 10. In diesem Sinne auch Murswiek, der betont, dass Eigenverantwortung die Selbstbestimmung der Aufgaben und Ziele impliziert, für deren Erfüllung der Staat rechtlich nicht verantwortlich sei, Murswiek, Die staatliche Verantwortung für die Risiken der Technik, 1985, 52.

79 Vgl. Gehring, Sicherheit mit Open Source, in: Gehring/Lutterbeck (Hrsg.), Open Source Jahrbuch 2004, S. 209 (214 f.).

80 Vossbein, Eigenverantwortung und Marktwirtschaft als Steuerungsimpulse der IT-Sicherheit, in: Pohl/Weck (Hrsg.), Beiträge zur Informationssicherheit, 1995, S. 43 (46); ebenso Pipkin, der eine Verantwortungsteilung entsprechend der „Rolle" im System vorsieht, so solle etwa der „information owner" die Einstufung der „Sicherheitsstufe" vornehmen, während der „information user" die Verantwortung für den angemessenen Gebrauch trage, Pipkin, Information Security, 2000, S. 103.

81 Ebenso die Weiterleitung von E-Mail durch Trojaner. Die Eigenverantwortung bestünde in diesem Fall in der Installation eines entsprechenden Programms zu Schutz vor Trojaner. Zur Haftung bei unbeabsichtigten Verbreitung: Libertus, Zivilrechtliche Haftung bei Computerviren, in: MMR 2005, 507 ff.

renden Eigenverantwortung anderen Zumutbarkeitserwägungen ausgesetzt als die Auferlegung einer haftungsrelevanten Verantwortung.

Soweit eine Eigenverantwortung für das Funktionieren eines „Systems" vorausgesetzt wird[82], ist der Einzelne vor einem fließenden Übergang zur Verantwortung durch den Vorbehalt des Gesetzes[83] vor den Folgen der Verantwortung geschützt. D. h. das Recht muss klarstellen, wo Eigenverantwortung eine bloße Appellfunktion besitzt und wo haftungsrelevante Verantwortung beginnt.

(4) Die Eigenverantwortung des Einzelnen korrespondiert mit einer Infrastrukturverantwortung des Staates.[84] Soweit der Staat es dem Einzelnen im Rahmen seiner Infrastrukturgewährleistung ermöglicht, sich selbst zu schützen, trägt der Einzelne im gewissen Maße auch die Konsequenzen aus der Freiheit und der Möglichkeit zum Schutz. Allerdings soll das Recht auch für *„nachlässige und uninteressierte Personen ein Mindestmaß an Schutz bieten."*[85] Soweit der Staat hier zu normativen Lösungen greift, sind diese den Beschränkungen der rechtlichen Steuerung des Internets unterworfen.[86]

Soweit der Staat zur Sicherheit „verpflichtet" werden kann, zielt diese Idee regelmäßig auf die Verantwortung des Staates. Auf staatlicher Ebene kann die Verantwortung abgeschichtet sein. Das Spektrum reicht von der Erfüllungsverantwortung mit der *„größten Leistungstiefe"*[87] über die Gewährleistungsverantwortung, die sich in einem Rahmen der Überwachung und Kontrolle realisiert, bis zur Auffangverantwortung, um Fehlentwicklungen entgegenzusteuern.[88] Mit welchem Grad der Staat „verpflichtet" ist Sicherheit zu gewährleisten, hängt von dem Bereich ab, in dem Sicherheitsaspekte virulent werden.

---

82 Neben dem angesprochenen Sozialversicherungssystem wird die Eigenverantwortung auch im Straßenverkehr vorausgesetzt, Burmann, Die Verkehrssicherungspflicht für den Straßenverkehr, in: NZV 2003, 20 (20).

83 Zu den Voraussetzungen der (rechtlichen) Verantwortung: Masing, Politische Verantwortlichkeit und rechtliche Verantwortung, in: ZRP 2001, 36, (36): „*Rechtliche Verantwortung ist gesetzlich bemessene Verantwortung. Ihre Prinzipien sind Äußerlichkeit, Formalität und Begrenztheit.*"

84 *Rossnagel,* in: Rossnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, S. 333, Rd. 20.

85 *Rossnagel,* a.a.O., (Fn. 84), S. 333, Rd. 20.

86 Vgl. Kapitel 4 B.

87 Ruge, Die Gewährleistungsverantwortung des Staates, 2004, S. 166.

88 Ruge, a.a.O., (Fn. 87), S. 166: Die Abschichtung der Verantwortung sei eine Frage der Kooperation von staatlichen und privaten Akteuren. Zum „Regulierungsverwaltungsrecht" im Gewährleistungsstaat: Masing, Grundstrukturen eines Regulierungsverwaltungsrechts, in: Die Verwaltung, 36. Band 2003, S. 1.

Soweit es um Sicherheit durch polizeiliche Gefahrenabwehr geht, trifft den Staat die Erfüllungsverantwortung.[89] Diese Erfüllungsverantwortung zeichnet sich dadurch aus, dass sie nicht grundsätzlich einklagbar ist, sondern nur die Maßnahme an sich beanstandet werden kann, dass sie ein Ergebnis der Abwägung von Freiheit und Sicherheit sein kann[90] und die Sicherheit ex ante konturiert. Aufgrund der territorialen Gebundenheit des nationalstaatlichen Einflusses und der Vollzugsprobleme wegen Unkörperlichkeit kann der Staat einer Erfüllungsverantwortung im Internet nicht gerecht werden.[91] Seiner Schutzpflicht genüge der Staat deshalb, wenn der Staat die Bürger in die Lage versetze und es sicherstelle, sich selbst zu schützen.[92]

Soweit die Sicherheit durch ex post-Bestimmungen etwa im zivilrechtlichen Deliktsrecht realisiert wird, kann die Zivilrechtsordnung als Teil der Gewährleistungsverantwortung des Staates verstanden werden.

Soweit es um IT-Sicherheit im eigentlichen Sinn geht, kann der von Hermes entwickelte Begriff der Infrastrukturgewährleistungsverantwortung herangezogen werden.[93] Grundlage dieser Infrastrukturgewährleistungsverantwortung ist die Erkenntnis, dass funktionierende Netzinfrastrukturen zwar keine hinreichende, doch aber notwendige Existenzbedingungen für Staat und Gesellschaft sind.[94] Zweifelsohne gehört zu diesen das Internet.[95] Die Infrastrukturverantwortung ist in der

---

89 Ruge, a.a.O., (Fn. 87), S. 173.

90 Die Verfassung konstituiert in den Grundrechten die Freiheit des Bürgers und ist auf die Abwehr des staatlichen Eingriffs angelegt. Die Sicherheit, die ein Staat gewährleisten kann, resultiert meist in einem staatlichen Eingriff. Insofern wirkt die Sicherheit auf staatlicher Ebene grundsätzlich freiheitsmindernd, vgl. Isensee, Das Grundrecht auf Sicherheit, 1983, S. 2.

91 *Rossnagel,* a.a.O.,(Fn. 84), S. 333, Rd. 18.

92 *Rossnagel*, a.a.O., (Fn. 84), S. 333, Rd. 19. Nicht zuletzt gebiete es die Infrastrukturverantwortung für eine ausreichende Aufklärung über die Selbstschutzmöglichkeiten zu sorgen, a.a.O., (Fn. 84), S. 334, Rd. 21.

93 *Rossnagel*, a.a.O., (Fn. 84), S. 333, Rd. 19, der den Datenschutz im Internet als Infrastrukturverantwortung versteht.

94 Hermes, Infrastrukturverantwortung, 1998, S. 324.

95 Hermes will die Verantwortung für die Infrastruktur nach Netz und Dienst unterschiedlich bewerten, Hermes, a.a.O., (Fn. 94), S. 333. Für das Internet lässt dies unter Umständen einen unterschiedlichen Grad der Verantwortung für die (techno)logische bzw. physikalische Infrastruktur und Anwendung zu. Bei Hermes wirkt sich die Verantwortung für die Sicherheit der Netze nur bei der Interoperabilität (Netzsicherheit im hier beschriebenen Sinn), den offenen Netzzugang und die Verteilung knapper Kapazitäten aus. Für die Dienste sei zentraler Punkt der Verantwortung die Sicherung der allgemeinen Zugangsmöglichkeiten, Hermes, a.a.O., (Fn. 94), S. 348. Allerdings impliziert eine Grundversorgung, wie sie in Art. 87f Abs. 1 GG genannt ist, ein gewisses Maß an Qualität, welche auch Sicherheit umfasst. In histori-

oben beschriebenen „Abschichtungsphase“ der Gewährleistungsverantwortung in Kooperation mit Privaten wahrzunehmen.[96] Diese Verantwortung kann der Staat nicht mit klassischen ordnungsrechtlichen Instrumenten, sondern in einem *„policy mix“*[97] wahrnehmen. Diese Überlegungen finden sich im Grundgesetz für die Telekommunikation in Art. 87f GG wieder.

Aufbauend auf die Infrastrukturverantwortung des Staates wird teilweise *„die Organisation von Systemschutz und die Ermöglichung von privaten Selbstschutz“*[98] als Bestandteil der Umsetzung von staatlichen Schutzpflichten und als *„Privatisierungsfolgenrecht“*[99] verstanden. Teilweise werden diese Überlegungen, wie der Staat seine Schutzpflichten für Informationsvorgänge nachkommen kann, konkretisiert. Zum einen wird allgemein eine *„proaktive Prävention“*[100] gefordert. Diese sei eine Folge des gewandelten Schutzkonzepts. Mit der *„Dynamisierung des Sicherheitsdenkens“*[101] gehe es nicht darum repressive Mittel ex post einzusetzen, sondern um die Sicherung von Rechten und Ansprüchen ex ante.[102]

Zum anderen werden konkrete Handlungspflichten für Private angedacht und § 85 Abs. 2 TKG a. F. (entspricht § 88 Abs. 2 TKG) beispielhaft genannt.[103] Weitere Schutzelemente sind Transparenzanforderungen, die – fokussiert auf die informationelle Selbstbestimmung als Datenschutz – als Informations- und Auskunftsrechte benannt werden.[104]

---

scher Auslegung umfasst die flächendeckend „angemessene“ Dienstleistung auch die Qualität der Dienstleistung, Gesetzentwurf zur Änderung des Grundgesetzes vom 14.04.1994, BT-Drs. 17/7269, S. 10. Roßnagel benennt dies bezogen auf das Netz: *„In seiner Verantwortung für die Funktionsfähigkeit staatlicher Aufgabenerfüllung trifft ihn* [der Staat, d. Verf.] *die Verpflichtung, die Verfügbarkeit der verwendeten Techniksysteme und Informationen, deren Unversehrtheit und Vertraulichkeit sicherzustellen.“* Nicht zuletzt trügen alle staatliche Organe Verantwortung für ein freies und demokratisches Zusammenleben. Roßnagel, Notwendige und mögliche Regulierungen der IT-Sicherheit, in: Pohl/Weck (Hrsg.), Beiträge zur Informationssicherheit, 1995, S. 51 (56).

96 Hermes, a.a.O., (Fn. 94), S. 338 f.

97 Grimm, Staatsaufgaben - eine Bilanz, in: Grimm (Hrsg.), Staatsaufgaben, 1994, S. 771 (778).

98 Schoch, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, in: VVDStRL 57 (1998), S. 158 (208).

99 Schoch, a.a.O., (Fn. 98), S. 158 (207).

100 Gusy, Gewährleistung von Freiheit und Sicherheit, in: VVDStRL 63 (2004), S. 151 (158).

101 Gusy, a.a.O., (Fn. 100), S. 151 (157).

102 Gusy, a.a.O., (Fn. 100), S. 151 (157).

103 Trute, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, in: VVDStRL 57 (1998), S. 216 (259).

104 Trute, a.a.O., (Fn. 103), S. 216 (261).

Soweit die Eigenverantwortung organisiert bzw. auf der Ebene von Wirtschaft und Gesellschaft wahrgenommen wird, wird auch von Selbstregulierung gesprochen, ohne hierbei den Grad der Abschichtung, d. h. der Kooperation, näher zu bezeichnen.

> *„Selbstregulierung entsteht nicht von selbst und benötigt manchmal auch eine Art rechtlicher Untermauerung: Vielleicht muss aktiver vorgegangen werden, um die Vereinbarung einer geeigneten Menge an Regeln und ihre Umsetzung zu fördern."*[105]

Soweit eine Eigenverantwortung anzunehmen ist, sollte das Recht oder die Technik dem Nutzer die Chance geben, diese auch sinn- und verantwortungsvoll zu nutzen. So kann die Frage nach den rechtlichen Rahmenbedingungen der (Selbst)Information über Sicherheitslücken eine mögliche Chance und Grenze durch Recht für die Sicherheit durch Eigenverantwortung beleuchten (Chance durch Recht und Grenze durch Rechtsfolgen).[106] Wenn es etwa in oder für Unternehmen bereits an verbindlichen (rechtlichen) Regelungen fehlt, wie über Sicherheitslücken zu informieren ist, und somit auch an einer notwendigen Voraussetzung für eine Sicherheitskultur,[107] dann wird die Chance auf Eigenverantwortung in diesem Bereich von vornherein verringert.

d) Zusammenfassung

Eine Erfassung der Sicherheit entsprechend der technischen Kategorienbildung ist dem Recht nicht zu entnehmen. Das Recht muss notwendigerweise grundsätzlich abstrakt bleiben. Der Vorteil der Technik, konkret sein zu dürfen und zu müssen, lässt sich in konkreten Kategorien der Sicherheit abbilden.[108]

Sicherheit ist mit den Mitteln des Rechts (Normen, Rechtsprechung) eigentlich nicht ausreichend zu begegnen, da in der Umsetzung der Pflichten zur Sicherheit

---

105 Vorschlag für eine Entscheidung des Europäischen Parlaments und des Rates über ein mehrjähriges Gemeinschaftsprogramm zur Förderung der sichereren Nutzung des Internets und neuer Online-Technologien vom 12.03.2004, KOM(2004)91 endg., S. 9.

106 So wird die Chance auf Eigenverantwortung durch einen rechtlich normierten Informationsfluss erhöht. Vgl. etwa in § 7 Abs. 1 SGB XI Soziale Pflegeversicherung [Aufklärung und Beratung]:
„Die Pflegekassen haben die Eigenverantwortung der Versicherten durch Aufklärung und Beratung (…) zu unterstützen (…)."

107 Pipkin, Information Security, 2000, S. 103: *"Many incidents go unreported because the individuals who have knowledge of the incident are not aware of how to report the problems."*

108 Die Genauigkeit bezieht sich allerdings nur auf die technischen Anforderungen. Hinsichtlich der Erwartungen und Rollen der Kommunikationspartner abstrahiere die Technik gerade: Kilian, Datensicherheit in Computernetzen, in: CR 1990, 73 (75).

oder in der Geltendmachung eines Anspruchs auf Sicherheit dem Schutz der Rechtsgüter nicht tatsächlich hinreichend Rechnung getragen werden kann. Recht bleibt im Detail von der Umsetzung (d. h. Kontroll- und Durchsetzungsmöglichkeiten) und von der Geltendmachung (etwa Beweisschwierigkeiten) abhängig. Insoweit ist auch die hier propagierte Eigenverantwortung eine „Krücke", die jedoch weitere Regelungen zur Sicherheit, wenn auch nur ungenügend, ergänzen könnte. Soweit sie als Obliegenheit rechtlich zu berücksichtigen ist, ist der Beitrag der Eigenverantwortung im Hinblick auf mögliche Informationspflichten im weiteren Verlauf der Arbeit zu prüfen.

Als Annäherung an die Sicherheit und Denkmodel für den Umgang mit Sicherheit eignen sich die rechtlichen „Kategorien" dennoch. Insbesondere können sie Basis für die Entscheidung sein, ob Sicherheit in einem Regel-Ausnahmeverhältnis (dann ist auf eine ex ante verpflichtende Sicherheit zu setzen) oder als Ausnahme (dann steigt die Relevanz der Eigenverantwortung) geregelt werden sollte.

4. Ökonomische Kategorie – Risikomanagement

In ökonomischer Hinsicht kann Sicherheit aus Sicht des Herstellers (Produktsicherheit) und aus Sicht des Unternehmens und Marktteilnehmers bei Nutzung des Internets (Netz- und Kommunikationssicherheit) betrachtet werden. Für alle gilt die Betrachtung unter dem Aspekt der Wirtschaftlichkeit und Wirksamkeit der Sicherheitskomponente.

Überlegungen zur Produktsicherheit schließen Absatzchancen, „Preis-Leistungsverhältnis" und Haftungsrisiken ein und sind nicht daher zuletzt vom Markt beeinflusst. Die Beurteilung der Netz- und Kommunikationssicherheit ist mehr eine interne Betrachtung und zunächst weniger am Markt orientiert, sondern primär von anderen Interessen (Daten- und Rechtsgüterschutz) geprägt.[109] Die Marktrelevanz kann sich bei Veröffentlichung von Sicherheitsrisiken zunächst in einem Reputationsverlust zeigen, der jedoch nicht zwingend Einfluss auf den Absatz des eigentlichen Produkts des Unternehmens hat.

---

[109] In diesem Sinne können Sicherheitsmaßnahmen nicht nur als wirtschaftliches Eigeninteresse angesehen werden. Dies hat zur Folge, dass gesetzliche Regelungen zur Sicherheit etwa vor unerlaubten Zugriffen oder zur Vorbeugung von Schwachstellen erforderlich sind. Vgl. etwa Überlegungen zu gesetzlichen Sicherheitsmaßnahmen in § 87 TKG a. F., Scheuerle/Mayen-*Zerres,* TKG Kommentar § 87 Rd. 2.

Mögliche Einwirkungen auf den Gewinn lassen sich mit einer Softwareversicherung abfangen. So bezieht sich die „Erweiterte Softwareversicherung“ eines Versicherungsanbieters auf Schäden durch Störungen oder Ausfall des Systems, durch externe Angriffe und durch Malware (Viren, Trojaner, Würmer, etc).[110]

Der Internetschutzbrief ist die Idee einer Internetversicherung, die Nutzer vor dem finanziellen Risiko (Schäden) bei der Internetnutzung absichern soll. Dieser Internetschutzbrief wurde für Anfang 2005 in Aussicht gestellt,[111] und bisher noch nicht realisiert.

Im Folgenden sollen ökonomisch relevante Erwägungen unter dem Aspekt der Wirtschaftlichkeit der Sicherheit und unter dem Aspekt des Risikomanagements dargestellt werden.

a) Wirksamkeit und Wirtschaftlichkeit der Sicherheit

Ein Faktor, der sich wohl nicht unwesentlich auf die Sicherheit auswirkt, ist die Verfügbarkeit von Sicherheit zu betriebswirtschaftlich sinnvollen Maßstäben, d. h. sichere, aber „unbezahlbare“ Software wird selten zum Einsatz kommen.[112] Da Sicherheit Geld kostet, sollte sich der Kompromiss zwischen dem technisch Machbaren und ökonomisch Vernünftigen in den rechtlichen Anforderungen wieder finden.[113] Hierbei kann zugespitzt formuliert werden, das technisch Machbare ist die Obergrenze der Sicherheit und das ökonomisch Vernünftige muss die Untergrenze der Sicherheit beachten, die vom Gesetz vorgegeben wird. Im Recht findet sich diese Abwägung etwa in § 9 S. 2 BDSG:

---

110 Die „Erweiterte Softwareversicherung“ der VHV, http://www.vhv.de:80/web/Ihre_VHV/-PresseService/Pressemitteilungen/2005/20050315/index.jsp (30.05.2006).

111 Nach dem Aktionsprogramm der Bundesregierung, Informationsgesellschaft Deutschland 2006, 2003 sollte dieser Internetschutzbrief Anfang 2005 verfügbar sein, http://www.bmbf.de/pub/aktionsprogramm_informationsgesellschaft_2006.pdf, S. 11 (30.05.2006).

112 Bartsch, Computerviren und Produkthaftung, in: CR 2000, 721 (724). Ein weiterer Faktor wird vom Nutzer bestimmt, dessen Kaufentscheidung nicht von Sicherheitsfeatures, sondern von anderen Features der Software motiviert wird. Wo keine Nachfrage, da keine Investition in Sicherheit, vgl. Gehring, Software Development, Intellectual Property, and IT Security, in: Journal of Information Law & Technology 2003, Issue 1, http://elj.warwick.ac.uk/jilt/03-1/gehring.htm (30.05.2006).

113 Die rechtlichen Anforderungen können allerdings den Kompromiss zugunsten der einen oder anderen Komponente verschieben. So müssen explizite Sicherheitsprodukte oder Produkte mit sicherheitsrelevantem Einsatzgebiet mehr (teure) Sicherheit gewährleisten können als Produkte, bei denen eine bestimmte Nutzungsfunktion in der Freizeit im Vordergrund steht.

„Erforderlich sind diese Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

Oder in § 109 Abs. 2 S. 4 TKG:

„Technische Vorkehrungen (…) sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtung für die Allgemeinheit steht."

In § 109 Abs. 2 S. 4 TKG und § 9 S. 2 BDSG wird letztlich der Kompromiss zwischen dem technisch Machbaren und ökonomisch Vernünftigen (Aufwand), also unternehmensinterne ökonomische Überlegungen, um eine extern bedingte Verhältnismäßigkeitabwägung zwischen Aufwand und Schutzzweck bzw. den gefährdeten Rechtsgütern ergänzt.[114]

Der Maßstab der Verhältnismäßigkeit ist Chance und Risiko für die tatsächlich gewährleistete Sicherheit. Ist ein angemessener Aufwand zur Erreichung des Schutzzweckes nicht möglich, so ist nach dem Gesetz entweder ein höherer Aufwand in Kauf zu nehmen, oder etwa auf die Verarbeitung der Daten zu verzichten.[115] Letztlich besteht dennoch ein faktisches Risiko, da es realitätsfern erscheint, dass ein Unternehmen etwa auf eine elektronische Datenorganisation verzichtet, wenn es das in § 9 BDSG gebotene Schutzniveau nicht leisten kann.

b) Risikomanagement

Im Kontext der IT-Sicherheit ist Risiko die Wahrscheinlichkeit, dass Schwachstellen im System die Authentizität, Integrität, Vertraulichkeit oder Verfügbarkeit der Daten beeinflussen.[116] Ökonomisch ist jedes Risiko auch gleichzeitig eine Chance:

„Risiken sind natürlicher Bestandteil der Geschäftstätigkeit eines jeden Unternehmens und bedeuten gleichzeitig Gefahr, aber auch notwendige Voraussetzung für unternehmerischen Erfolg.-Gerade durch den bewussten, kontrollierten Umgang mit Risiken können Kosten reduziert und Wettbewerbsvorteile realisiert werden."[117]

Soweit Risiko zugleich als Chance begriffen wird, kann der Umgang mit dem Risiko (Risikomanagement) nicht zwangsläufig mit einem Sicherheitsmanagement gleich-

---

114 Simitis u. a., BDSG/*Ernestus/Geiger*, § 9 Rd. 23.

115 Simitis u. a., BDSG/*Ernestus/Geiger*, § 9 Rd. 44 der darüber hinaus betont, dass auch der Abschluss einer Haftpflichtversicherung die gebotenen Maßnahmen nicht ersetzen kann.

116 Vgl. Art. 4 lit h) der Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10.März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit, ABl. Nr. L 077, vom 13.03.2004, S. 1

117 Thiel, IT-Sicherheitsmanagement, 2004, http://www.competence-site.de/itsecurity.nsf/F75C331F3CD6FDEEC1256E450037A1F7/$File/it_sicherheitsmanagement.pdf (30.05.2006).

gesetzt werden. Eine Sicherheitsarchitektur kann risikofreudig, -neutral oder –scheu ausgestaltet werden. Das Risiko nimmt zudem proportional zur Abhängigkeit vom Internet und Intranetzen zu. Diese Kategorisierung, die sich auch auf das Risikomanagement in Unternehmen übertragen lässt, sollte gleichzeitig eine Antwort auf die Frage, wer das Risiko trägt, ermöglichen. Bei einer Realisierung von Sicherheit (im Fall eines risikoscheuen Unternehmens) kann demnach das Recht unterstützend und steuernd eingesetzt werden. Die Verteilung des Risikos darf rechtlich nicht obskur bleiben, sondern bedarf klarer Richtungsweisungen.

Risikomanagement entspricht grundsätzlich der rechtlichen Kategorie der (Eigen)Verantwortung.[118] Solange und soweit keine rechtlich konkretisierten Pflichten ex ante zur Absicherung der Gefahren (Risiken) bestehen, liegt in einem Risikomanagement die eigenverantwortliche Entscheidung, das Risiko zu vermeiden, wenn dies nicht möglich ist, zu beseitigen (oder zumindest zu verringern), soweit dies nicht möglich, ist das Risiko zu akzeptieren oder das Risiko ökonomisch zu tragen (Akzeptanz) und auf Dritte zu verschieben (Versicherung).

Im Folgenden sollen konkrete Regelungen für die Handhabung des Risikos der IT-Sicherheit mit „Basel II", das über eine Richtlinie im Europarecht verankert wird,[119] und mit § 91 Abs. 2 AktG, eine bestehende Regelung im deutschen Recht dargestellt werden.

aa) „Basel II"

„Basel II" soll aufgrund der besonderen Relevanz der IT-Sicherheit für sensible Finanz- und Kreditgeschäfte dargestellt werden. „Basel II"[120] ist eigentlich eine inter-

---

118 Damit ist in die Verteilung des Risikos in jedem Fall an der allgemeinen strafrechtlichen oder deliktischen Haftung zu orientieren.

119 Vorab ist eine Umsetzung ins deutsche KWG bis zum 01.01.2007 geplant, vgl. Kabinettsentwurf vom 15.02.2006, http://www.bundesfinanzministerium.de/cln_03/nn_1928/DE/-Geld und Kredit/Aktuelle Gesetze/Entwurf eines Gesetzes zur Umsetzung Bankenrichtlinie.html (30.05.2006).

120 Basel II ist der populäre Name für die „Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderungen – Überarbeitete Rahmenvereinbarung", vom Juni 2004 des Baseler Ausschuss für Bankenaufsicht, http://www.bis.org/publ/bcbsca.htm (30.05.2006). In rechtlicher Hinsicht sollen die Inhalte mit denen sich „Basel II" beschäftigt auf europäischer Ebene in einer Richtlinie umgesetzt werden. Gegenwärtig im Gesetzgebungsprozess soll damit die bisherige Richtlinie über angemessene Eigenkapitalisierung novelliert werden, vgl. Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates zur Neufassung der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates vom 20. März 2000 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute und der Richtlinie 93/6/EWG des Rates vom 15. März 1993 über die angemessene Eigenkapitalausstattung

nationale Übereinkunft des „Basel Committee on Banking Supervision“[121] für die Eigenkapitalvorsorge der Kreditinstitute, die in der EU durch eine Richtlinie aufgegriffen und umgesetzt werden soll. Unter dem Teilaspekt operationelles Risiko lässt sich jedoch auch die IT-Sicherheit als relevante Komponente ausmachen.

Unter „operationellen Risiken“ sind

> *„die direkten oder indirekten Verluste zu verstehen, die durch inadäquate interne Arbeitsabläufe, Versagen der Mitarbeiter und Systeme oder durch externe Ereignisse entstehen“.*[122]

Als Komponente des operationellen Risikos fließt die Qualität der IT-Sicherheit in die Einschätzung und Bewertung von Banken- und Versicherungsrisiken und damit in die Bemessung der Eigenkapitalvorsorge ein.

Inwieweit die banken-sektorspezifischen Regelungen von „Basel II“ (unter der Prämisse des Erlasses der Richtlinie) verallgemeinerungsfähig sind und Auswirkungen auf ein branchenübergreifendes proaktives Risikomanagement von IT-Systemen und –Prozessen haben, bleibt abzuwarten.[123]

Entsprechend „Basel II“ und inhaltlich ähnlich bestehen auf nationaler Ebene bereits weitere Mindestanforderungen an das Risikomanagement von Kredit- und Finanzdienstleistungsinstitute etwa als Teil der ordnungemäßen Geschäftsführung nach § 25a Abs. 1 S. 2 KWG.

In § 25a Abs. 1 S. 2 Nr. 4 KWG werden angemessene Sicherheitsvorkehrungen für den Einsatz elektronischer Datenverarbeitung gefordert. Aktuell wurde zur Konkretisierung von § 25a KWG und im Hinblick auf die Mindestanforderungen von „Basel II“ am 20.12.2005 ein Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) veröffentlicht (MaRisk).[124] Hinsichtlich der angemessenen

---

von Wertpapierfirmen und Kreditinstituten, vom 14.7.2004 KOM(2004)486 endg. (im Folgenden Eigenkapitalvorsorgerichtlinie-Entwurf, KOM(2004)486 abgekürzt).

121 Vgl. http://www.bis.org/bcbs/aboutbcbs.htm (30.05.2006).

122 Bergles, Baseler Committee in: BKR 2002 379 (380); ähnlich Art. 4 Nr. 22 der Eigenkapitalvorsorgerichtlinie-Entwurf, KOM(2004)486.

123 Diesbezüglich positiv, Romeike, IT-Riskmanagement, in: DuD 2004, 335 (336).

124 Vgl. Mindestanforderungen an das Risikomanagement, Rundschreiben 18/2005 vom 02.02.2005, http://www.bafin.de/rundschreiben/89_2005/051220.htm (30.05.2006). Als Rundschreiben der BaFin hat die MaRisk für die Adressaten keine Regelungsqualität (schlichtes Verwaltungshandeln). Sie ist dennoch aber nicht rechtsunerheblich, da dem Rundschreiben als Mitteilung der Rechtsauffassung zu zukünftigen Aufsichtsmaßnahmen ein „vorauseilender Gehorsam“ folgen könnte, vgl. Fett, Rechtsschutz gegen schlichthoheitliches Verwaltungshandeln, in: WM 1999, 613 (613).

Sicherheitsvorkehrungen werden Ausführungen zu Umfang und Qualität der technisch-organisatorischen Ausstattung gemacht.[125]

bb) § 91 Abs. 2 AktG

§ 91 Abs. 2 AktG entspricht – weniger konkretisiert, aber in der Tendenz – weitgehend der Verpflichtung zur ordnungsgemäßen Geschäftsführung nach § 25a Abs. 1 S. 2 KWG. Danach hat der Vorstand ein Überwachungssystem einzurichten, damit bestandsgefährdende Entwicklungen frühzeitig erkannt werden können. § 91 Abs. 2 AktG betrifft somit die Gesamtsteuerung eines Unternehmens.[126] *„Zu dem von dieser Vorschrift geforderten Risiko-Management zählt zweifellos auch die sog. IT-Sicherheit".*[127] Ob die Risiken einer Internetnutzung im Einzelfall bestandsgefährdend sind, mag dahinstehen, ein Aspekt, dem Beachtung geschenkt werden sollte, kann IT-Sicherheit aber in jedem Fall darstellen.

Die tatsächliche Relevanz und Förderungschance für die IT-Sicherheit durch § 91 Abs. 2 AktG ist hier angesichts der zusätzlichen Abwägungsfaktoren in einer ökonomischen Betrachtung kaum zu beurteilen. Soweit das unternehmerische Know-how sich in dem Datenbestand eines Unternehmens widerspiegelt, sind die Maßnahmen zur Sicherung dieser Daten vor Verlust und Manipulation jedoch mit weiteren bestandsgefährdenden Risiken systematisch zu erfassen.[128] Hinsichtlich der

---

125 In AT 7.2 Rundschreiben 18/2005 werden Umfang und Qualität der technisch-organisatorischen Ausstattung konkretisiert:
„2.Die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Ihre Eignung ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.
3. Die IT-Systeme sind vor ihrem erstmaligen Einsatz und nach wesentlichen Veränderungen zu testen und von den fachlich sowie auch von den technisch zuständigen Mitarbeitern abzunehmen. Produktions- und Testumgebung sind dabei grundsätzlich voneinander zu trennen.
4. Die Entwicklung und Änderung programmtechnischer Vorgaben (z. B. Parameteranpassungen) sind unter Beteiligung der fachlich und technisch zuständigen Mitarbeiter durchzuführen. Die programmtechnische Freigabe hat grundsätzlich unabhängig vom Anwender zu erfolgen."

126 Neben den Aktiengesellschaften soll § 91 Abs. 2 Akt auch für die GmbH entsprechend gelten und nach dem Willen des Gesetzgebers Ausstrahlungswirkung auf den Pflichtenrahmen anderer Gesellschaftsformen haben, Begründung zum Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich vom 07.11.1997, BR-Drs. 872/97, S. 37.

127 Barton, Risiko-Management und IT-Sicherheit, in: K&R 2004, 305 (305).

128 Welche Risiken als bestandsgefährdende zu erfassen sind, ergibt sich zudem aus dem Prüfungsstandard für Wirtschaftsprüfer (vgl. § 317 Abs. 4 HGB): IDW Prüfungsstandard 340, WPg 1999, 658. Zur Abschlussprüfung bei Einsatz von Informationstechnologie IDW Prüfungsstandard 330: WPg 2002, 1167.

Überwachung des unternehmerischen Risikos ist darüber hinaus nach § 91 Abs. 2 AktG eine Überwachung des IT-Systems vor allem in der IT-Sicherheitsbranche oder für Kreditinstitute, deren Reputation unmittelbar von der Sicherheit des operativen Geschäftes abhängig ist, von tatsächlicher Relevanz.

c) Zusammenfassung

Ökonomische Überlegungen zur (IT-)Sicherheit sind nicht zwangsläufig nur an der Optimierung dieser ausgerichtet. (IT-)Sicherheit ist vielmehr ein Faktor von vielen, den es in der Geschäftsführung abzuwägen und zu bewerten gilt. Welches Gewicht ihr dabei zugemessen wird, hängt von der Ausrichtung des Unternehmens und den Auswirkungen auf dieses ab. Konkrete gesetzliche Regelungen können allerdings der IT-Sicherheit zusätzliches Gewicht verleihen.

5. Verbindung der technischen, rechtlichen und ökonomischen Kategorien

Auf europäischer Ebene wird in der Rechtsgestaltung und –sprache die technische Vorstellung von IT-Sicherheit als Netz- und Informationssicherheit[129] als Voraussetzung des funktionierenden Binnenmarktes[130] aufgegriffen.

Die Interessensicherung wird der Technik durch Regelungen auf europäischer Ebene vorgeben. So etwa mit den Aktionsplänen *„Sichere Nutzung des Internet"*[131]. In die-

---

129 Art. 4 lit. c) der Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit, ABl. Nr. L 077, vom 13.03.2004, S. 1:
„(…) „Netz- und Informationssicherheit" die Fähigkeit eines Netzes oder Informationssystems, bei einem bestimmten Vertrauensniveau Störungen und rechtswidrige oder böswillige Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit (…) beeinträchtigen (…)".

130 Erwägungsgrund (3) der Verordnung (EG) Nr. 460/2004, a.a.O., (Fn. 129).

131 „Aktionsplan I": Entscheidung Nr. 276/1999/EG des Europäischen Parlaments und des Rates vom 25. Januar 1999 über die Annahme eines mehrjährigen Aktionsplans der Gemeinschaft zur Förderung der sicheren Nutzung des Internet durch die Bekämpfung illegaler und schädlicher Inhalte in globalen Netzen, ABl. Nr. L 33, vom 06.02.1999, S. 1. Die Laufzeit dieses Programms war vier Jahre vom 1. Januar 1999 bis zum 31. Dezember 2002, vgl. Art.1 Abs. 2. „Aktionsplan II": Entscheidung Nr. 1151/2003/EG des Europäischen Parlaments und des Rates vom 16. Juni 2003, zur Änderung der Entscheidung Nr. 276/1999/EG über die Annahme eines mehrjährigen Aktionsplans der Gemeinschaft zur Förderung der sicheren Nutzung des Internet durch die Bekämpfung illegaler und schädlicher Inhalte in globalen Netzen, ABl. Nr. L 162, vom 01.07.2003, S. 1. Diese ändert die Entscheidung Nr. 276/1999/EG und verlängert das Programm um zwei Jahre bis zum 31.12.2004, Art. 1 Abs. 2. „Aktionsplan III": Vorschlag für eine Entscheidung des Europäischen Parlaments und

sen finden sich etwa *„Ermutigungen der Branche, Filter und Bewertungssysteme anzubieten“*[132] oder Steuerungsoptionen durch die Bezuschussung von Forschungsarbeiten zu innovativen Technologien[133]. Mehr als „Nebenschauplatz“ wird die Sensibilisierung der Nutzer für Fragen der Informations- und Netzsicherheit angesprochen.[134]

Darüber hinaus finden sich (im europäischen Recht und in der nationalen Umsetzung) Regelungen zur Interessensicherung im Urheberrecht, etwa der Schutz technischer Maßnahmen zum Schutz des Werkes in § 95a UrhG.

In der deutschen Rechtsgestaltung finden sich die technischen Kategorien der Sicherheit nur selten konkret in den Regelungen wieder. Im Gesetz zur Errichtung des Bundesamtes für die Sicherheit in der Informationstechnik (BSIG)[135] etwa rekurriert die entsprechende Regelung in § 2 Abs. 2 (inhaltlich, nicht terminologisch) auf die IT-Sicherheit. Ebenfalls mit inhaltlichen Vorgaben („technische und organisatorische Maßnahmen“) und nicht terminologisch bezieht sich § 9 BDSG auf die Datensicherheit.

Bereits diese selektive Zusammenstellung von Normen macht deutlich, dass es wenig spezifiziertes IT-Sicherheitsrecht gibt. Normiert sind vielmehr lediglich ausfüllungsbedürftige Anforderungen (etwa die bestandsgefährdenden Entwicklungen in § 91 Abs. 2 AktG), ohne dem Recht eine wirkliche Anleitungsfunktion und Durchsetzungskraft zu verleihen.[136]

In einem rechtlichen Kontext soll das ökonomische Risiko keine dogmatisch greifbare Kontur besitzen und im rechtlichen System letztendlich unspezifisch blei-

---

des Rates über ein mehrjähriges Gemeinschaftsprogramm zur Förderung der sicheren Nutzung des Internet und neuer Online-Technologien, KOM(2004)91 endg. vom 12.03.2004. Inhaltlich konzentrieren sich alle Programme auf den Kampf gegen illegale und die Bekämpfung unerwünschter und schädlicher Inhalte sowie die Förderung eines sicheren Umfeldes (funktionierendes System der Selbstregulierung) und die Sensibilisierung der Nutzer, vgl. Art. 1 Nr. 2 des „Aktionsplan III“.

132 Art. 3 des „Aktionsplan I“, Entscheidung Nr. 276/1999/EG, a.a.O., (Fn. 129).

133 Anhang I, 2. Aktionsbereich des „Aktionsplan III“, KOM(2004)91 endg., a.a.O., (Fn. 129).

134 Anhang I, 4. Aktionsbereich des „Aktionsplan III“, KOM(2004)91 endg., a.a.O., (Fn. 129).

135 § 2 Abs. 2 BSIG
„Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen (…).“

136 So fehlen spezifische Haftungsvorschriften. Selten sind etwa Normen wie § 7 und § 8 BDSG, die auf Schäden an personenbezogenen Daten zugeschnitten sind. Die Nicht-Bestellung eines Sicherheitsbeauftragten nach § 109 Abs. 3 S. 1 TKG hat etwa keine Konsequenzen nach § 149 TKG. Als Sanktionen bleiben höchstens Maßnahmen nach der aufsichtsrechtlichen Generalbefugnis des § 126 TKG.

ben.[137] Dies ist dann nicht vertretbar, wenn Sicherheit und Risiko zwei Seiten einer Medaille bilden. Soweit Sicherheit im rechtlichen System spezifiziert werden kann, trifft dies auch auf das Risiko zu.

Das Verhältnis von Technik, Recht und Ökonomie zu Sicherheit wurde wie folgt auf den Punkt gebracht.

> *„Insecurity of software is due to interaction of technological and legal shortcomings, fostered by economic rationality."*[138]

Exemplarisch für Software kann diese Aussage auch auf andere Gebiete der IT-Sicherheit bezogen werden. Im Weiteren führt Gehring die Gründe der negativen Auswirkung auf die Sicherheit aus: Technisch seien es unvollständige Spezifikationen und Tests sowie die fehlende Kenntnis von Messung von Sicherheit. Rechtlich seien es vor allem fehlende Haftung und die Zuordnung zu Geschäftsgeheimnissen. Schließlich seien die Anbieter ökonomisch dem Profit verpflichtet (Kosten zu senken und Einnahmen zu generieren) und die Anwender besäßen „asymmetrische Informationen", was eine *„adverse selection"*[139] fördere.

Beim letzten Punkt („asymmetrische Informationen") wird der Einfluss von Information für die Produktauswahl betont und damit eine Zuordnung zur Ökonomie vorgenommen. Nicht zuletzt führen aber durch ein Risikomanagement empfohlene und den rechtlichen Rahmen vorgegebene technische Überwachungen zum Auffinden von Sicherheitslücken und damit zu der Frage, wie das Unternehmen mit der Information über diese umzugehen hat. Hierbei ist der rechtliche Rahmen ausfüllungsbedürftig.

B Sicherheitslücken und Schwachstellen im Internet

Zunächst soll der ubiquitäre Charakter, d. h. die geographische, wie auch inhaltliche und funktionale Durchdringung des Alltags durch das Internet im Folgenden am

---

137 Di Fabio, Risikosteuerung im öffentlichen Recht, in: Hoffmann-Riehm/Schmidt-Aßmann (Hrsg.), Öffentliches Recht und Privatrecht, 1996, S. 143 (144).

138 Gehring, Open Source Software - Sicherheit im Spannungsfeld von Ökonomie und Politik, Vortrag zum Workshop "Sicherheit mit Open Source?", CAST Forum Darmstadt, 20. März 2003, http://ig.cs.tu-berlin.de/ma/rg/ap/2003-03/Gehring-OpenSourceSicherheit-032003.pdf (30.05.2006).

139 Gehring, Ökonomie und IT-Sicherheit Ein Denkanstoß, Workshop Grenzflächen der Informatik und Methoden von Informatik und Gesellschaft, Dagstuhl, 8. bis 12.2004, http://ig.cs.tu-berlin.de/ma/rg/ap/Gehring-OekonomieUndIT-Sicherheit-2004-11-08.pdf (30.05.2006).

Beispiel der Konvergenz verdeutlicht werden. Dem ubiquitären Charakter des Systems folgen entsprechende ubiquitäre Sicherheitslücken.

Aus der Perspektive des „Systems Internet“ und seiner Nutzung sollen die Sicherheitslücken system- und nutzungsbedingt herausgearbeitet werden. Hierbei zeichnen sich systembedingte Sicherheitslücken durch fehlerhaft funktionierende Einzelkomponenten oder einer unerwünschten Wechselwirkung der Einzelkomponenten aus. Nutzungsbedingte Sicherheitslücken sind dagegen auf eine fehlerhafte Implementierung, Bedienung oder Anwendung durch den Nutzer zurückzuführen.

Neben der Bestimmung der Infrastruktur aus physikalischen und (techno)logischen Elementen wird das „System“ Internet durch die Anwendungen und Dienste definiert. Systembedingt kann die Sicherheit auf zwei Hauptaspekte konzentriert werden:

Erstens, auf die Sicherheit der zu Grunde liegenden Infrastruktur (in der Arbeit als Schwachstellen in IT-Systemen bezeichnet), und zweitens, auf die Sicherheit der ausgeführten Anwendung (als Sicherheitslücke vorwiegend Software betreffend). Pointiert formuliert berühren Sicherheitslücken so Aspekte der Produktsicherheit und Schwachstellen die Netz-, Kommunikations- und Datensicherheit.

Die Darstellung wird vorwiegend technisch orientiert sein. Mit der technischen „Orientierung“ soll bereits hier darauf hingewiesen werden, dass diese Darstellung nicht aus Sicht und mit Mitteln eines „Technikers“ erfolgen kann und soll. Ausgangspunkt ist vielmehr, so wenig Technik wie möglich, soviel Technik wie nötig. Dies gilt für die Tiefe, wie auch die Breite der Darstellung.[140]

I. Internet

Eine Betrachtung des ubiquitären Internets als *„Netz der Netze“*[141] ist nicht nur eine infrastrukturelle Überlegung, sondern zollt auch dem Verhältnis zwischen dem In-

---

[140] Sollte trotz aller Bemühungen und Absicherungen hinsichtlich der Darstellung der Technik eine - etwa für einen Informatiker - Begriffsunklarheit bestehen, so reihe ich mich, wenn auch nicht gerne, in eine Liste von Stilblüten juristischer Vorgänger ein, vgl. unter „Juristen erklären das Internet“ http://www.daufaq.de (30.05.2006).

[141] Vgl. etwa unter: http://www.gmd.de/People/Klaus.Birkenbihl/publications/NetzDer-Netze.htm und http://pmueller.de/tele/internet/in14.htm (30.05.2006).

ternet und den klassischen Kommunikationsmedien[142] Tribut. Dies erfordert eine Betrachtung der Konvergenz.

Die Konvergenz betrifft in einer kommunikationsorientierten[143] Interpretation technologische, inhaltlich-funktionale und wirtschaftliche Aspekte des Zusammenwachsens der Medien.[144] Die technologische Konvergenz ist die Nutzung der gleichen Übertragungstechnik und der Endgeräte. Zugespitzt formuliert resultiert die technologische Konvergenz aus der Digitalisierung der Übertragungstechniken und der Übertragung mittels Breitbandtechnologie[145]. Die technologische Konvergenz ermöglicht eine Interaktivität bei der Programmauswahl (etwa Video-on-Demand[146]).

Die inhaltlich-funktionale Konvergenz ist die Chance zur Diversifikation der Inhalte und Funktionen.[147] Diese Vielfalt kann das Verständnis von dem, was die Medien

---

142 Der hier vertretene weite Medienbegriff will Medien lediglich als Plural von Medium im Sinne eines (hinsichtlich des Rezipientenkreises neutralen) Vermittlers verstanden wissen und nimmt Abstand von der Trennung der Medien in Massen- und Individualkommunikation.

143 Konvergenz kann auch naturwissenschaftlich oder wirtschaftswissenschaftlich interpretiert werden.

144 Diese drei Ausprägungen zeichnen sich bereits in der Einleitung zum „Grünbuch der Konvergenz der Branchen Telekommunikation, Medien und Informationstechnologie und ihren ordnungspolitischen Auswirkungen", KOM(97)623, ab (im Folgenden mit „Grünbuch zur Konvergenz" abgekürzt bezeichnet). Eine eingehende Beschäftigung mit diesen Ausprägungen findet sich bei: Weiss, Das Internet und die klassischen Medien Konvergenz – Konkurrenz oder Komplementierung?, 2002, S. 74 ff.; Dörr/Gersdorf, Der Zugang zum digitalen Kabel, 2002, S. 61 nennen noch die Konvergenz des Rechts und des Nutzerverhaltens.

145 Die Unterscheidung einer breitbandigen oder schmalbandigen Übertragung ist eine Unterscheidung der Durchflusskapazität einer Datenleitung. Diese Übertragungstechnologie ist nicht abhängig von einer bestimmten physischen Netzinfrastruktur. Breitbandige Anschlüsse mit Übertragungsraten über 128 kbit/s werden über Digitale Anschlussleitungen (DSL), Kabelfernsehanschlüsse (Kabel-TV), Stromkabel (Powerline) und Satellit angeboten (vgl. Jahresbericht 2003 der Regulierungsbehörde für Telekommunikation und Post (RegTP), S. 21, http://www.bundesnetzagentur.de/media/archive/215.pdf (30.05.2006). Nach dem Jahresbericht 2003 der RegTP wurden 60.000 der 4,6 Mio. breitbandigen Internetanschlüsse über bidirektionale Kabel gewährleistet. Die 60.000 sind bisher nur ein geringer Bruchteil der 21 Mio. Kabelanschlüsse die für einen Internetzugang verwendet werden. Im internationalen Vergleich wird der Internetzugang hauptsächlich über das Kabel gewährleistet, vgl. Jahresbericht 2003 der RegTP, S. 23.

146 Auf der CeBIT 2004 stellte T-Online Vision Video-on-Demand für den Fernseher vor. Bis dato waren On-Demand-Dienste ausschließlich über PC oder mobile Endgeräte abrufbar, vgl. http://www.heise.de/newsticker/meldung/45797 (30.05.2006).

147 Vgl. Schlussbericht der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft", BT-Drs. 13/11004 S. 11. Die Kommission lehnte allerdings eine rechtliche Folge (Gleichbehandlung der Medien bei gleicher Plattform) bei inhaltlicher Konvergenz ab. Lediglich in einem Sondervotum (S. 24 f.) wurde ein Einfluss der inhaltlich-funktionalen Konvergenz auf die rechtliche Einordnung der Medien erwogen.

trennt und verbindet, erweitern. Funktionen, die bisher gedanklich mit dem Endgerät PC/Laptop verbunden waren, sind mit anderen Endgeräten möglich.[148]

Die wirtschaftliche Konvergenz ist als weitere Folge der technologischen Konvergenz zu sehen. In der „Konvergenz der Unternehmen" können ökonomische Vorteile aus der technischen Entwicklung gezogen werden.[149]

Durch einen steigenden Vernetzungsgrad, umfassende Verbreitung und steigende Leistungsfähigkeit wird die Alltagswelt von der Informationstechnik – und damit dem Internet – unterstützt und abhängig.[150] Die Chancen und Risiken dieses konvergenten Internets sind in erhöhtem Maße mit einer entsprechenden Sicherheitstechnik verbunden.

Im weiteren Verlauf der Arbeit werden die rechtlichen Rahmenbedingungen der Konvergenz nicht vertieft dargestellt werden können. Zur Einleitung sei hier nur auf die europarechtlichen Vorgaben im Richtlinienpaket verwiesen. Dieses besteht aus der Rahmen-[151], Zugangs-[152], Genehmigungs-[153] und Universaldienstleistungsrichtlinie[154] für Kommunikationsnetze und -dienste.[155] Diese Richtlinien gelten für

---

148 So kann etwa der Download von ausgesuchten Programmen mit dem Fernsehgerät das Medium Rundfunk (Einordnung nach Inhalt) oder das Medium Internet (Einordnung nach Datenübertragung – Technik) betreffen.

149 So bietet eine erweiterte Palette der Dienstleitungen bei kaum erweiterten Investitionskosten – etwa die erweiterte Produkt- und Dienstleistungspalette der Service Provider bei bestehender Infrastruktur – die Chance zur Gewinnsteigerung. Dies hat ein Zusammenwachsen zu einer Branche „Kommunikation" zur Folge. Sie bietet die Chancen des Preiswettbewerbs, aber auch die Risiken einer Konzentration der Medienmacht, vgl. Weiss, Das Internet und die klassischen Medien Konvergenz – Konkurrenz oder Komplementierung?, 2002, S. 100.

150 Vgl. Einleitung zum IT-Grundschutzhandbuch 2005, S. 11, http://www.bsi.de/gshb/deutsch/index.htm (30.05.2006).

151 Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste, ABl. Nr. L 108, vom 24.04.2002, S. 33. Im Folgenden wird diese Richtlinie als Rahmenrichtlinie abgekürzt bezeichnet.

152 Richtlinie 2002/19/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung, ABl. Nr. L 108, vom 24.04.2002, S. 7. Im Folgenden wird diese Richtlinie als Zugangsrichtlinie abgekürzt bezeichnet.

153 Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über die Genehmigung elektronischer Kommunikationsnetze und –dienste, ABl. Nr. L 108, vom 24.04.2002, S. 21. Im Folgenden wird diese Richtlinie als Genehmigungsrichtlinie abgekürzt bezeichnet.

154 Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzungsrechte bei elektronischen Kommunikationsnetzen und –diensten, ABl. Nr. L 108, vom 24.04.2002, S. 51. Im Folgenden wird diese Richtlinie als Universaldienstrichtlinie abgekürzt bezeichnet.

die Regulierung der Übertragung und Infrastruktur und sind von der Regulierung der Inhalte zu trennen.[156]

Zusammenfassend sei im Hinblick auf die Chancen und Risiken der Konvergenz – angesichts des thematischen Fokus auf Sicherheitslücken und Schwachstellen in IT-Systemen – auf die Risiken der Konvergenz hingewiesen. Konvergenz heißt nicht zuletzt der Schritt in eine vernetzte Alltagswelt, in der der Kühlschrank selbstständig Nachschub ordert und die Ausstattungen des Hauses von auswärts bedient und reguliert werden können. Der Zugriff von außen auf die interne Organisation der Daten erhöht die Anforderungen an die technische Sicherheit als Voraussetzungen zur Bewältigung des Alltags.[157]

II. Systembedingte Sicherheitslücken und Schwachstellen

Die systembedingte Betrachtung soll zeigen, dass das Internet in gewissen Komponenten der Infrastruktur[158], der Technologie und der Dienste eine Anlage für Sicherheitslücken aufweist. Hierauf kann der Einzelne nur bedingt Einfluss nehmen. In der Anwendung kann das Internet vom Nutzer teilweise individuell geprägt werden, was dem Hinnehmen von Sicherheitslücken oder der Installation und Konfiguration von Schutzmaßnahmen entsprechen kann.

---

155 Meist wird die elektronische Datenschutzrichtlinie 2002/58/EG mit zu diesem Paket gezählt – Art. 2 dieser Richtlinie verweist auch auf die Begriffsbestimmungen der Rahmenrichtlinie, Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. Nr. L 201, vom 31.07.2002, S. 37. Ergänzt und vervollständig wird der Rechtsrahmen der Konvergenz durch die Richtlinie 2002/77/EG der Kommission vom 16. September 2002 über den Wettbewerb auf den Märkten für elektronische Kommunikationsnetze und –dienste (Wettbewerbsrichtlinie), ABl. Nr. L 249, vom 17.09.2002, S. 21 und die Entscheidung Nr. 676/2002/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen Rechtsrahmen für die Funkfrequenzpolitik in der Europäischen Gemeinschaft (Frequenzentscheidung), ABl. Nr. L 108, vom 24.04.2002, S. 1.

156 So Erwägungsgrund (5) der Rahmenrichtlinie.

157 Die vernetzte Zukunft im intelligenten Haus ist bereits in der Erprobungsphase, vgl. exemplarisch der Bericht über das Leben im vernetzten Haus im Schweizer Kanton Zug, heise news vom 02.08.2004, http://www.heise.de/newsticker/archiv/ (30.05.2006).

158 Grundlegend zum Begriff Infrastruktur, Sonntag, IT-Sicherheit kritischer Infrastrukturen, 2005, S. 27 ff.

1. Infrastruktur

a) Physikalische Infrastruktur

aa) Netze

So wie das Internet als „Netz der Netze" eine Betrachtung der Konvergenz ist, so ist das Internet in einer infrastrukturellen Annäherung ein dynamisches „Netz aus Netzen". Kommunikationsnetze können durch die Netzstruktur (1), die Übertragungswege (2) und –techniken (3) sowie durch die Versorgungsstruktur (4) klassifiziert werden.

(1) Die Netzstruktur beschreibt die Topologie der Knoten und Verbindungen. Verbindungen sind Leitungen und Knoten Vermittlungsstellen. Die Topologie steht im direkten Zusammenhang mit der Art der Übermittlung. Die Übermittlung von Daten im Internet erfolgt als Paketvermittlung, weshalb das Internet eine dezentrale, nicht hierarchische Struktur besitzt. Das Internet kann aufgrund dieser Struktur beliebig wachsen und neue Netze aufnehmen.[159] Auf diese Weise ist es ein dynamisches „Netz aus Netzen".

(2) Mit der Terminologie des Internets sind die Backbones als Verbindungen und die Peering-Points als Knoten die wesentlichen Übertragungswege.[160]

Der Austausch von Internetdatenpaketen erfolgt in Deutschland hauptsächlich über DE-CIX (Deutscher Commercial Internet Exchange) in Frankfurt/Main.[161] Seit

---

159 Eine Orientierung und praktische Anleitung wie Intranetze oder andere Netzwerke an das Internet angeschlossen werden können, bietet RFC 2901, „Administrative Internet Infrastructure Guide", 2000.

160 Durch Backbones und Peering-Points wird der Durchfluss großer Datenkapazitäten in der Netzstruktur bewältigt. Sie gewährleisten und erhöhen die Verfügbarkeit und die Bandbreite der Netze. Das Backbone ist ein Basisnetz, das weniger leistungsfähige – lokale und regionale – Netze vermascht, vgl. Erklärung im Internetlexikon Wikipedia http://de.wikipedia.org/wiki/Backbone (30.05.2006). Die Peering-Points (Austauschpunkte) gewährleisten und regeln den Datenaustausch zwischen den einzelnen Netzen.

161 Weitere wichtige Austauschpunkte sind etwa M-CIX in München oder BCIX in Berlin. Technisch kann der Austausch gezielt über bestimmte Netzwerke gesteuert und ein transatlantischer Umweg über US-Netzwerke vermieden werden, vgl. http://www.interest.de/cgi-bin/lexika/Peering.html?pos=T10447639&ID=798216297643 (30.05.2006), so aber eine Befürchtung der Europäischen Kommission: Mitteilung der Kommission KOM (2000) 202 vom 11.04.2000, Organisation und Verwaltung des Internets, S. 36: Die transatlantische Kapazität (Bandbreite) des Internet-Grundnetzes sei ein Mehrfaches der Bandbreite zwischen den einzelnen Mitgliedstaaten der EU. Die Folge sei, dass ein höherer Prozentsatz des pan-

Anfang 2004 wurde DE-CiX 3 in Betrieb genommen. Die dreifach redundante Infrastruktur trägt zur Erhöhung der Verfügbarkeit und der Kapazität bei[162] und ist so ein wesentlicher Beitrag zur Erhöhung der Netzsicherheit.

(3) Die Übertragungstechnik ist analog oder digital. Die Übertragung erfolgt per Kupfer-, Koaxial-, Strom- oder Glasfaserkabel (leitergebundene Wege) oder Richt-, Mobil- oder Satellitenfunk (leiterungebundene Wege).[163] Im Zentrum der Übertragungstechnik steht der Zuwachs der Kapazität der Übertragungswege und zunehmend die Sicherheit beim leiterungebundenen Zugang zum Internet. Unabhängig von den Materialen bilden die Netze durch die Übertragungstechnik unterschiedliche Marktsegmente, etwa ISDN- (Integrated Services Digital Network), DSL- (Digital Subscriber Line) Netze oder (Rundfunk)Kabelnetze und Mobilfunknetze.

Welche Netze das Internet nutzt, ist zum einen eine Frage der Kapazitäten und im Verhältnis Telefon- zu Rundfunknetz eine Frage der (wirtschaftlichen) Investitionen.[164] Zum anderen ist es abhängig von der Entscheidung durch die Nutzer. Die Konkurrenz in der Breitbandtechnologie besteht hauptsächlich zwischen DSL und Koaxial(TV)Kabel (Kabel).[165] In Europa und den USA ergehen derzeit sowohl wirt-

---

europäischen Verkehrs über die USA umgeleitet wird. Die Kommunikation in Europa sei somit zu einem großen Teil von der Sicherheit und Zuverlässigkeit der transatlantischen Verbindungen abhängig. In Deutschland und den Mitgliedstaaten werden nationale Austauschknoten bereitgestellt. Die Befürchtungen äußerte die Europäischen Kommission allerdings vor der Errichtung des ersten DE CIX als noch der gesamte innerdeutsche Verkehr über die USA geroutet wurde. *„Jede E-Mail von Berlin nach München lief über den Atlantik und zurück. 1995 schlossen sich die Internet-Diensteanbieter in Deutschland im eco Forum zusammen und errichteten mit dem DE CIX einen eigenen Austauschknoten. Seitdem läuft die E-Mail von Berlin nach München nur noch über Frankfurt.",* vgl. Pressemitteilung vom 09.03.2004, zur Errichtung des dritten DE-CiX unter http://www.eco.de/servlet/PB/menu/1290561/index.html (30.05.2006).

162 Vgl. Pressemitteilung vom 09.03.2004, a.a.O., (Fn. 161).

163 Haaß, Handbuch der Kommunikationsnetze, 1997, S. 18.

164 Die herkömmliche Betriebsart des (Fernseh)Kabels erlaubt nur einen einseitigen Datenaustausch. Eine interaktive Nutzung (zweiseitiger Datenaustausch) erfordert eine technische Aufrüstung des Kabels mit einem Rückkanal. Zu realisieren ist dies durch die Aufrüstung des Koaxial(TV)Kabels mit einem Rückkanal oder durch eine komplementäre Ergänzung des Koaxialkabels mit dem Kupferkabel der Telefonleitung, vgl. Dörr/Gersdorf, Der Zugang zum digitalen Kabel, 2002, S. 49.

165 Es ist eine Konkurrenz zwischen dem Telefonnetz – DSL ist die Ausstattung der Kupferkabel des Telefonnetzes mit DSL-Technologie – und dem Fernsehkabel, welches für die Interaktionen des Internets technisch aufzurüsten ist. Der Breitbandzugang über Kabel führt in Deutschland, das auf die DSL-Technologie setzt, ein Nischendasein. In den USA, Schweden oder Großbritannien erfolgt der Zugang zu knapp der Hälfte über das Kabel. Vgl. Bericht des BITKOM, Daten zur Informationsgesellschaft. Status quo und Perspektive Deutschlands im internationalen Vergleich, 2005, S. 9.

schaftliche als auch rechtliche Entscheidungen zu der Konkurrenz dieser Übertragungswege.[166]

Die Entscheidung für eine bestimmte Übertragungstechnik kann auch die Sicherheit der Nutzung beeinflussen. Sicherheitslücken können durch die Auswahl der entsprechenden Infrastruktur geschlossen werden. So kann etwa der Dialer-Missbrauch durch den Einsatz von DSL als Übertragungstechnik verhindert werden. Bei DSL werden Verbindungen nicht durch Anwahl eines Modems oder durch eine ISDN-Karte hergestellt, sondern anstelle der Telefonwählverbindung der Computer am Netzwerk des Providers angemeldet.[167]

(4) Abschließend soll die Versorgungsstruktur von Netzen in geographischer und personeller Hinsicht betrachtet werden.

Die Bestimmung der Versorgungsstruktur ermöglicht eine Systematisierung nach der geographischen Entfaltung des Netzes. PAN[168], LAN[169], wLAN[170], MAN[171], WAN[172], GAN[173] sind die gängigen Abkürzungen. Das Internet aufgrund seiner

---

166 In der Sache geht es um den Zugang von Internet Service Provider (ISP) zu den Kabelnetzen. Die Betreiber der Netze bieten in der Regel eigene ISP-Dienste an. Andere ISP können ausgeschlossen werden, da die Netzbetreiber in der Regel die „letzte Meile" (entspricht in Deutschland Netzebene 4) besitzen. Der Zugang anderer ISP ist eine Zulassung von Konkurrenz. Letztendlich ist die Einordnung des Internetzugangs über Kabel (cabel modem services) als *„telecommunication service"*, *„information service"* oder *„cable service"* im US-Recht entscheidend. "Information services" sind weitestgehend frei von Regulierung, da die Federal Communications Commission eine so genannte "hands-off" Politik verfolgt, um Innovationen im Internet nicht zu behindern, vgl. Wagner, Die "Open Access Debatte" in den USA, in: MMR 2001, 659, Fn. 17. Als Anbieter von *„telecommunication service"* wären die Netzbetreiber verpflichtet, ISP den Zugang zu gewähren. Zum Zugang der ISP zu den Kabelnetzen: U.S. Court of Appeals for the 9th Circuit, Opinion 06.10.2003, Case No. 02-70518 Brand X Internet Services v. Federal Communications Commission.

167 http://www.dslweb.de/dialer-und-dsl.htm (30.05.2006). Eine Missbrauchsgefahr durch Dialer ist bei DSL nur möglich, wenn zusätzlich eine analoge oder eine ISDN-Verbindung installiert ist. Eine solche zusätzliche Installation zum DSL ist etwa erforderlich, wenn mittels des PC Faxe verschickt werden sollen.

168 Personal Area Network, etwa Funktastatur (Reichweite einige Meter).

169 Local Area Network, etwa Unternehmensnetze (Reichweite einige Meter bis Kilometer). Das Ethernet ist die bekannteste LAN-Standard Technologie.

170 Wireless Local Area Network.

171 Metropolitan Area Network, etwa Kabelfernsehnetz (Reichweite etwa 10 km).

172 Wide Area Network, etwa das Deutsche Forschungsnetz (Reichweite Land oder Kontinent).

173 Global Area Network. Die Einordnung des Internets als GAN provoziert darüber hinaus die Frage, wie global das Internet angesichts der Verbreitung in Afrika tatsächlich ist. Laut einer Studie der OECD „Understanding the Digital Divide" von 2001 und nielsen-Netrating sind in Afrika (unter Ausklammerung Südafrikas) nur 0,5 % der Bevölkerung online, vgl. auch Plenarprotokoll 15/75, S. 6548.

geographischen Reichweite als GAN – zumindest aber als WAN zu bezeichnen – bietet sich an, ist aber strukturell nicht korrekt, da das Internet ein Zusammenschluss unterschiedlich großer geographischer Netze ist (Internetwork[174]). Sicherheitslücken finden sich schon in kleinsten Netzstrukturen. Theoretisch kann bereits mit einem Anschluss eines Rechners des LAN an das Internet, etwa zur Erleichterung der Administration,[175] ein „Schlupfloch" für einen (unbefugten) Zugang zu den scheinbar im Intranet sicher gespeicherten Daten gegeben sein. Sicherheit und damit Sicherheitslücken betreffen stets den einzelnen Nutzer unabhängig von der Größe des Netzes.[176]

In personeller Hinsicht können die Netze als nicht-öffentliche Netze, Corporate oder Virtual Private Network (VPN als virtueller Tunnel durch das Internet) beschränkt werden. Als solche beschränkten Netze können sie durch gezielte Sicherheitsmaßnahmen geringere Sicherheitslücken aufweisen.

Der Informationsverbund Berlin-Bonn (IVBB) ist ein spezialisiertes LAN, das nicht nur für das interne Regierungshandeln eine Informationsinfrastruktur bieten soll, sondern auch für die Realisierung von E-Government[177] eine Unterstützung sein kann. Als behördliches Informationsnetz – mit nicht-öffentlichen Informationen[178] – ist der IVBB in besonderem Maße von der Sicherheit der Infrastruktur abhängig. So wurden bei der Konzeption des Netzes sowohl technische Störungen als

---

174 Der Begriff Internetwork im allgemeinen Sinne meint die Verbindung von mehreren LANs über ein WAN. Eine spezielle Form des Internetwork ist das weltweite Internet. Jeder weitere Anschluss eines Netzes kann, entsprechend jedem PC, als Erweiterung des Internets verstanden werden.

175 So können etwa Updates für Programme aus dem Internet zur Installation auf den Rechnern im LAN bequem heruntergeladen werden.

176 Je größer die Versorgungsstruktur umso mehr Nutzer können durch Sicherheitslücken und Schwachstellen tangiert sein, umgekehrt kann aber nicht geschlossen werden, je kleiner das Netz, desto geringer das Gefährdungspotential durch Sicherheitslücken.

177 Der IVBB ist für das E-Government im Sinne der Leistungserbringung der Verwaltung an den Bürger keine zentrale Infrastruktur. Zu der E-Government Infrastruktur: BSI Schriftenreihe, SAGA Standards und Architektur für E-Government Anwendungen, Version 2.1., vom 06.02.2006, http://www.kbst.bund.de/saga (30.05.2006). E-Government umfasst nach der Initiative BundOnline 2005 alle Prozesse der Entscheidungsfindung und Leistungserbringung in Politik, Staat und Verwaltung, soweit diese unter Nutzung der Informations- und Kommunikationstechnologien stattfinden (vgl. SAGA, S. 37). SAGA beschreibt die technischen Rahmenbedingungen für die Kommunikation mit und Interaktion von Bundesbehörden. Eingebunden in dieses Projekt sind das BSI und die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesministerium des Inneren (KBSt).

178 Nutzer des IVBB sind Bundestag, Bundesrat, Bundeskanzleramt, Bundesministerien, Bundesrechnungshof sowie nachgeordneten Bundesbehörden.

auch unwahrscheinliche Großschadensereignisse in Betracht gezogen[179] und das Netz als exklusives separates LAN mit eigenen Schnittstellen zum Internet betrieben.

bb) Client und Server

Ein Client ist ein Computer, der eine Ressource oder einen Dienst von einem anderen Computer anfordert. Ein Client ist das Endgerät im Internet und kann als solches unterschiedliche Erscheinungsformen haben: PC/Laptop, PDA (Personal Digital Assistant), etc.

Ein Server ist ein Rechner, der Ressourcen für andere Rechner bereithält oder bestimmte Dienste ausführt.[180] So nimmt etwa der Webserver Anfragen von Clients entgegen und sendet die angeforderte Information zurück. Ein Fileserver stellt für Clients Speicherplatz zur Verfügung. Die Server verwalten somit das „Wissen" des Internets. Die Qualität eines Clients oder Servers wird – neben der lokalen Hardware – von der Abstimmung der lokal installierten Software mit der (techno)logischen Infrastruktur bestimmt.

Je nach Konfiguration und (techno)logischer Infrastruktur kann jeder Computer sowohl Client als auch Server sein. Im Hinblick auf die Sicherheit unterscheiden sich die Betriebssysteme von Client und Server. Das Betriebssystem der Server bietet in der Regel ein hohes Maß an Sicherung der Verfügbarkeit und des Zugriffs und verfügt darüber hinaus über Authentifikations- und Protokollierungsfunktionen.[181] Die Verfügbarkeit rund um die Uhr birgt eine Angriffsfläche und ein Sicherheitsrisiko des Servers. Andererseits enthalten typische Client-Betriebssysteme in der Regel nur unzureichende Komponenten zur Identifikation der Anwender und Zugriffskontrolle und sind deshalb etwa für die Speicherung kritischer Daten ohne weitere Vorsorge ungeeignet.[182]

Eine besondere Ausprägung der Client-Server-Struktur ist das Peer-to-Peer Netzwerk. Jeder Benutzer kann gleichzeitig Ressourcen bereithalten und abrufen. Diese

---

179 Vgl. http://www.kbst.bund.de/cln_011/nn_837412/Content/IT_Netze/IVBB_IVBV/-IVBB_Hintergrund/hintergrund_node.html_nnn=true (30.05.2006) mit einem Link zu weiteren Informationen; vgl. dort das Dokument „Der Informationsverbund Berlin-Bonn (IVBB)".

180 Leiden/Wilensky, TCP/IP für Dummies, 2. Aufl. 2001, S. 54.

181 Raepple, Sicherheitskonzepte für das Internet, 2. Aufl. 2001, S. 37. Betriebssysteme für Server sind etwa UNIX oder Windows NT/2000.

182 Raepple, a.a.O., (Fn. 181), S. 37. Betriebssysteme für Client sind etwa LINUX oder Windows XP.

Doppelfunktion des Nutzers birgt aufgrund der doppelten Verwundbarkeit spezifische Sicherheitsrisiken. Bereits mit der Installation der Software zum Filesharing ist etwa konkret zu entscheiden, welche Daten dem Netzwerk zur Verfügung gestellt werden sollen. Um unbewussten Freigaben von Daten vorzubeugen sollte die Software

> *„unbedingt mit sicheren Voreinstellungen geliefert werden oder den Nutzer vor gefährlichen Handlungen warnen."*[183]

Eine besondere Rolle für die Stabilität und Funktion des Internets nehmen die Root Server ein. Diese haben die Adressdateien des Internets gespeichert. Bisher gibt es 13 offizielle Root Server. Hinsichtlich der Sicherheit der physikalischen Infrastruktur und der Netzwerksicherheit sollten die Root Server wie kritische Datenzentren in großen Unternehmen geschützt werden.[184]

b) (Techno)logische Infrastruktur

Die (techno)logische Infrastruktur ist gekennzeichnet durch die technische Infrastruktur, die die logistische Infrastruktur im Sinne von Verbindungs- und Funktionselementen liefert. Sie soll die Elemente funktionsfähig verbinden und die Funktion der Anwendungen ermöglichen. Diese Aufgaben werden hier als (techno)logisch bezeichnet. Im Einzelnen werden an die Verbindung die Anforderungen der Unabhängigkeit und wechselseitige Kompatibilität der Übertragungswege und Endgeräte sowie die Ermöglichung des Zugangs für jedermann gestellt. Darüber hinaus sollte die (techno)logische Infrastruktur stabil, sicher und fehlerfrei funktionieren.

Über das Funktionieren der (techno)logische Infrastruktur geben RFCs (Request for Comments) Auskunft. Die RFCs sind eine Reihe von technischen und organisatorischen Dokumenten zum Internet. Zunächst nur zur Diskussion gestellt können sich RFCs durch Akzeptanz und Gebrauch zu einem technischen oder organisato-

---

183 Möller, Sicherheit in Peer-to-Peer-Netzen, 2001, http://www.heise.de/tp/r4/artikel/7/-7972/1.html (30.05.2006).

184 Network Working Group, Root Name Server Operational Requirements, RFC 2870, Best Current Practice, 2000, S. 2. Im Einzelnen wird für die Sicherheit der physikalischen Infrastruktur Access Control, Intrusion Detection Sensors, Firedetection und für die Netzwerksicherheit Beschränkung auf bestimmte Dienste, Limitation des Vertrauens auf bestimmte Hosts, Schutz mit Firewalls und Logs von Störungen vorgeschlagen (RFC 2870 hebt RFC 2010 auf).

rischen Standard im Internet entwickeln (dann verabschiedet als „standards track RFC“).[185]

aa) Protokolle

Als Protokolle werden in der Informatik die Regeln für den Datenaustausch zwischen Computern bezeichnet. Die Funktionsfähigkeit des Internets wird von unterschiedlichen Protokollen gewährleistet. Namentlich sind dies etwa das Simple Mail Transfer Protocol (smtp), File Transfer Protocol (ftp) oder das Hypertext Transfer Protocol (http). Diese Protokolle können Ursachen für Sicherheitslücken im Internet sein. So kann etwa über http schädlicher, ausführbarer Code übertragen werden.[186] Zur Gewährleistung der Sicherheit kann mit dem Hypertext Transfer Protocol Secure (https) die Verbindung zwischen Client und Server verschlüsselt werden.

Alle Protokolle basieren auf den TCP/IP Protokollen. Das TCP (Transmission Control Protocol) und IP (Internet Protocol) wird meist als TCP/IP einheitlich verstanden und bezeichnet.[187] Das TCP/IP regelt die Art und Weise der Datenübertragung in den Netzen und zwischen den Computern. Das TCP stellt sicher, dass Datenpakete vollständig und fehlerfrei zwischen Sender und Empfänger ausgetauscht werden. Das IP stellt die Adressierung des Internetraumes sicher.[188] Die Entwicklung des Internets wurde von der Verbreitung und Akzeptanz des IP-Protokolls maßgeblich beeinflusst.[189]

---

185 Vgl. http://www.rfc-editor.org/ (30.05.2006). Festgelegt werden die RFCs von der Internet Engineering Task Force (IETF). Diese ist eine globale, offene Gemeinschaft von Netzwerkdesignern, Anwendern, Anbietern und Forschern, die die technischen Ausführungen für die Entwicklung der Internet Architektur und den reibungslosen Betrieb des Internets anfertigen, RFC 3233, Defining the IEFT, Februar 2002.

186 Vgl. http://www.bsi.de/fachthem/sinet/vulner/index.htm (30.05.2006).

187 Das TCP/IP wurde von dem US-Department of Defense zunächst als Interimslösung betrachtet, Kaufmann, ISO-OSI und TCP/IP, in: DFN Mitteilungen 1990, Nr. 19/20, S. 21 (22 f.).

188 Klußmann, 2002, IP, S. 520.

189 In Europa versuchte man für die technische Frage – nicht nur die Amerikaner suchten nach Lösungen um Rechner miteinander zu verbinden und eine Netzwerkkommunikation zu ermöglichen – über einen ISO-Standard eine Lösung zu finden, RFC 1462, „What is the Internet?“, 1993.
Sehr differenziert ist die Geschichte des Internets bei Géczy-Sparwassser, Die Gesetzgebungsgeschichte des Internet, 2003, S. 31ff. dargestellt.

bb) Adressraum

Das Internet besitzt zwei Adressräume, den IP-Adressraum und die Domainnamen, verwaltet und verknüpft durch das Domain Name System (DNS).

Das IP ist für das Zerlegen der Daten in Datenpakete zuständig. Jedes Paket erhält einen „Paketkopf" (Header) mit Absender- und Empfängeradresse in Form einer IP-Adresse.[190] Die Adresse wird statisch oder dynamisch von den Internet Service Providern vergeben.[191] Ein Router wertet in den Datenpaketen enthaltene Adressierungsinformationen aus und ermittelt anhand von Routingtabellen den günstigsten Weg.[192]

Bei dem DNS handelt es sich um eine Reihe von verteilten Datenbanken (Name Servern), die die IP-Adressen mit dem einfacheren und aussagekräftigeren Domainnamen verknüpfen.[193]

Die Domainnamen gliedern sich in die Gruppe der gTLD (generic Top Level Domain) und der ccTLD (country code Top Level Domain)[194] und werden von unterschiedlichen Organisationen vergeben.[195]

---

190 Haselier/Fahnenstich (Hrsg.), Internet, 2000, S. 429.

191 Tierling, Internet - Das kompakte Wissen, 2001, S. 180. Der Adressraum umfasst etwa 4 Milliarden Adressen, http://www.uni-muenster.de/ZIV/Lehre/1999-4/RechnernetzeTechnischeGrundlagen/IPV6/tsld003.htm (30.05.2006). Es wurde davon ausgegangen, dass dieser Raum 2005 ausgeschöpft sein wird, vgl. Aktuelle Kurzinformation in: ITRB 2002, Nr. 4, S. 74. Deshalb wird das bisherige Internet Protokoll (IPv4) durch ein neues IPv6 abgelöst. Es umfasst 128 Bit lange Adressen - theoretisch können 340.282.366.920.938.463.463.374.607.431.768.211.456 Adressen vergeben werden - und stellt einen nahezu unendlich großen Adressraum zur Verfügung. Dem stehen nur 4.294.967.296 Adressen mit IPv4 gegenüber. Weiter Informationen zu IPv6 unter http://www.ipv6tf.de/index2.php (30.05.2006). Die Umstellung des IPv4 auf IPv6 ist bis jetzt aufgrund von Sicherheits- und Stabilitätserwägungen bei den Rootservern noch nicht erfolgt, da eine Adressanfrage und –umwandlung der IPv6 Adressen in Domainnamen derzeit noch nicht zuverlässig von einem Rootserver beantwortet werden kann, vgl. heise news vom 02.02.2004, http://www.heise.de/newsticker/meldung/44256 (30.05.2006).

192 Klußmann, 2002, Router, S. 840.

193 Kyas/a Campo, Internet professionell, 2. Aufl. 2001, S. 43.

194 Die ursprünglichen TLD .com, .edu, .gov, .mil, .net, .org und .int gehören der Gruppe der gTLD an, denen im Laufe der Zeit stets mit Auseinandersetzungen neue hinzugefügt wurden. Die Domains .gov und .mil sind für US-amerikanische Regierungsstellen und militärische Einrichtungen reserviert. Die ccTLD folgen dem existierenden internationalen Standard der Abkürzung für Ländernamen, dem ISO 3166. Eine Ausnahme hiervon ist u.a. Großbritannien. Statt des ISO 3166 „gb" Kürzel wird .uk verwendet. Ebenso .ac, .gg, .im, .je, die auf dem ISO 3166 –1 basieren, http://www.iso.org/iso/en/prods-services/iso3166ma/-index.html (30.05.2006). Ebenfalls zu den ccTLD gehört, obwohl nicht dem ISO 3166 Standard folgend, die .eu-Domain.

Seit 1996 ist in Deutschland die DeNIC (de Network Information Center) für die Registrierung der .de-Domains und den primären Nameserver zuständig.[196]

Das DNS ist als „Schlüsselkomponente" des Internets eine vorrangige ausgenutzte Sicherheitslücke.[197] Gelingt es etwa die Anfrage nach einem Domainnamen mit einer gefälschten IP-Adresse zu übersetzen, so kann die Zieladresse – für den Nutzer unerkannt – maskiert werden.[198]

cc) Adressierung

Die URL (Uniform Resource Locator)[199] gibt konkrete Auskunft über den Ort einer Ressource im Internet. Der Aufbau der URL wird meist von dem verwendeten Protokoll abgeleitet.[200] Nach dem Protokoll des Dienstes, etwa http, https, ftp (um die gängigsten Protokolle zu nennen) kommen der Doppelpunkt und zwei Schrägstriche (://). Danach kommt die Adresse des Host (Domain oder IP); nun folgen getrennt durch Schrägstriche die Verzeichnisangaben und der Dateiname.

Ein weiteres Adressierungselement – und damit eine Sicherheitslücke – ist der Port. Mit Port werden zum einen Hardwareschnittstellen bezeichnet. Zum andern ist ein Port eine Adresskomponente, die Protokollen zugeordnet wird, damit die Daten den entsprechenden Anwendungen zugeleitet werden können.[201] So hat etwa http

---

195 Die Prinzipien der Delegation der Domainregistrierungen an die Registries sind hauptsächlich in drei Dokumenten festgelegt. Das älteste, ein RFC 1591, „Domain Name System Structure and Delegation", 1994, http://www.RFC-editor.org/RFC/RFC1591.txt (30.05.2006), ist durch die „Internet Coordination Policy" (ICP-1) vom Mai 1999 aktualisiert, http://www.icann.org/icp/icp-1.htm (30.05.2006) und wird von einem Dokument des GAC (Governmental Advisory Committee), "Principles ans Guidelines for the Delegation and Administration of Country Code Top Level Domains" vom 05.04.2005 ergänzt, http://194.78.218.67/web/meetings/mtg21/GAC_ccTLD_Principles_MDP.doc (30.05.2006). Die eigentliche Registrierung der Domain durch den Nutzer erfolgt in der Regel über Internet Provider, die für den Nutzer die Registrierung etwa bei der Registry DeNIC vornehmen.

196 Vgl. http://www.denic.de/de/denic/wir_ueber_uns/historie/index.html (30.05.2006).

197 Reimann, Bernd, Domain Name Service, http://www.linuxfibel.de/dns_srv.htm (30.05.2006).

198 Vgl. http://www.bsi.de/fachthem/sinet/vulner/index.htm (30.05.2006).

199 Die technischen Details der URL sind im RFC 1738 standardisiert: RFC 1738, „Uniform Resource Locators (URL)", 1994. Vielfach wird auch die URI (Uniform Ressource Identificator) als Oberbegriff genannt.

200 Vgl. die Ausführungen im Internet Wörterbuch Wikipedia, http://de.wikipedia.org/wiki/URL (30.05.2006).

201 Es gibt drei Arten von Ports, Ports, die von der IANA allgemein bekannten Diensten zugeordnet sind, solche, die für besondere Dienste registrierbar sind, und dynamische, http://www.iana.org/assignments/port-numbers (30.05.2006). Vgl. die Ausführungen im

standardmäßig die Portnummer 80. Die Schwachstelle sind geöffnete Ports, d. h. Ports, bei denen der Datenverkehr nicht kontrolliert wird. Direkt adressiert können sie ein Einfallstor für Hacker sein. So etwa bei Programmen mit einer Back-Door-Komponente, die, installiert, einen Zugriff auf den betroffenen PC erlauben.[202]

Die Adressierung kann eine Schwachstelle des Internet sein, so etwa beim Phishing[203]. Beim Phishing soll der Nutzer mit einer E-Mail veranlasst werden, den (gefälschten) Link zu der Homepage, etwa seiner Bank, zu folgen und dort persönliche Daten, wie Zugangsdaten zu Onlinekonten oder Kreditkartennummern, einzugeben. Immer sophistisierter wird selbst die URL mittels Java-Script im Browser dargestellt,[204] so dass der Nutzer an der Adresse nicht erkennen kann, ob die angezeigte Seite eine Fälschung oder echt ist.[205]

c) Schnittstellen

Die Router oder Gateways sind die Schnittstellen im Zusammenschluss der Netze.

> *„Schnittstellen bilden die definierte Grenze zwischen zwei Hardware-Einrichtungen, Computern, Datenübertragungseinrichtungen oder logischen Softwareeinheiten. Eine Schnittstelle definiert die Gesamtheit der Festlegungen für die physikalischen Eigenschaften der Schnittstellenleitungen sowie die auf den Schnittstellen.“*[206]

Ihre Aufgabe besteht darin, die Kommunikationswege zwischen den Teilnetzen bereitzustellen und die notwendige Protokolladaptierung und Verkehrslenkung in den Teilnetzen durchzuführen.[207]

Ebenso ist eine Firewall eine Schnittstelle. Die Firewall setzt bestimmte Sicherheitsanforderungen an das System um, um externe Angriffe auf einen Netzbereich

---

Internet Wörterbuch Wikipedia, http://de.wikipedia.org/wiki/Port_(Protokoll) (30.05.2006).

202 So etwa bei einigen Versionen des NetSky Virus, vgl. LG Verden, Urteil v. 08.07.2005 – 3-5/05.

203 Phishing ist ein Kunstwort aus Passwort Fishing.

204 Eigentlich eine Manipulation des Browsers, um Anfragen auf eine für den Nutzer nicht sichtbare Adresse umzuleiten, auch Pharming genannt, http://de.wikipedia.org/wiki/-Pharming (30.05.2006).

205 Eine ausführliche Darstellung von Phishing Methoden bei Bleich/Schmidt, Auf Phishzug Passwortdiebstahl im Netz wird immer raffinierter, c´t 2004, Heft 17, S. 178 f.

206 Erläuterungen zu Schnittstellen im Siemens Online-Lexikon, http://www.networks.siemens-.de/solutionprovider/_online_lexikon/2/f006582.htm (30.05.2006).

207 Haaß, Handbuch der Kommunikationsnetze, 1997, S. 181. Grob kann differenziert werden: Gateways übernehmen die erforderliche Adaptierung und Anpassung der verbundenen Netze in einem Internetwork, vgl. Tanenbaum, Computernetzwerke, 4.Aufl. 2003, S. 41. Router werden hingegen als Schnittstelle im Intranetwork eingesetzt.

abzuwehren (Zugangsschutzsystem). Das Zugangsschutzsystem kann mit Hard- und Software umgesetzt werden.[208]

Eine Firewall (Hardware) ist ein Rechner, der den Datenverkehr zwischen einem LAN und einem anderen Netz (etwa dem Internet) regelt und die einzige Verbindung von dem LAN nach außen ist.[209] In dieser Funktion kann auch der Router als Firewall fungieren.

Eine Personal Firewall ist aber auch eine nur auf dem lokal zu schützenden Rechner installierte Software (und somit keine Schnittstelle im eigentlichen Sinne). Sie kann ebenso so konfiguriert werden, dass sie bestimmte Sicherheitsanforderungen an das System (Security Policy) umsetzt. Diese Umsetzung dient der Kontrolle und Steuerung des Datenverkehrs.[210] Es gibt hierbei zwei Arten von Firewalls.[211]

Obwohl der Sicherheit des Datenverkehrs und der Anwendungen dienend, ist die Firewall kein standardmäßiges Sicherheitsinstrument und die Verwendung liegt somit in der Entscheidung des Nutzers. Ob die Installation einer Firewall eine Obliegenheit oder eine rechtliche Verpflichtung zur Schadensminderung ist, ist der Rechtsprechung in Zukunft überlassen.[212]

d) Kritische Infrastruktur

Während Sicherheitslücken in der physikalischen und (techno)logischen Infrastruktur zunächst eine technische Betrachtung sind, sind unter dem Aspekt der kritischen Infrastruktur[213] die gesellschaftliche Relevanz und Implikationen eben dieser Sicherheitslücken zu diskutieren.

---

208 Eine Firewall kann somit sowohl ein Element der physikalischen als auch der (techno)logischen Infrastruktur sein.

209 Vgl. im Internetlexikon netlexikon, http://www.net-lexikon.de/Firewall.html (30.05.2006).

210 Weiterführende Informationen zur Funktionsweise im Internetlexikon Wikipedia, http://-de.wikipedia.org/wiki/Firewall (30.05.2006).

211 Vgl. http://www.nur-sicherheit.de/themen/firewall.htm (30.05.2006): Die Paket Filter Firewall arbeitet als Paketfilter nur auf den unteren Protokollebenen und hat keine Kontrolle über die Anwendungen. Die Application Level Firewall arbeitet auf der obersten Protokollebene und muss für jeden Dienst einzeln konfiguriert werden.

212 So hat der BGH „Dialer", Entscheidung v. 04.03.2004 - III ZR 96/03, MMR 2004, 308 entschieden, dass keine Obliegenheit des Nutzers besteht, ein Dialerschutzprogramm zu installieren. Ob diese Entscheidung auf die Installation einer Firewall übertragen werden kann, ist fraglich.

213 Kritisch zur „kritischen" Infrastruktur, Sonntag, IT-Sicherheit kritischer Infrastrukturen, 2005, S. 36.

Im Zusammenhang mit kritischen Infrastrukturen nimmt das Internet als Kommunikationsnetz eine vielschichtige Rolle ein.

Als kritische Infrastrukturen können Organisationen, Einrichtungen und sachliche Infrastrukturen bezeichnet werden. Sie haben

> *„(lebens-)wichtige Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Störung für größere Bevölkerungsgruppen nachhaltig wirkende Versorgungsengpässe oder andere dramatische Folgen eintreten'*[214].

Kritische Infrastrukturen sind demnach Energieversorgung (Elektrizität, Öl und Gas), Bank-, Finanz- und Versicherungswesen, Transport- und Verkehrswesen, Gesundheitswesen (einschließlich Lebensmittel- und Trinkwasserversorgung), Notfall- und Rettungsdienste, Regierung und öffentliche Verwaltung (einschließlich Polizei, Zoll und Bundeswehr) und Telekommunikation.[215] In Deutschland befindet sich ein Großteil der kritischen Infrastruktur durch Deregulierungsmaßnahmen in privatwirtschaftlicher Hand.

Damit kommt den Informations- und Kommunikationstechnologien eine zweifache Rolle zu. Zum einen sind sie selbst eine kritische Infrastruktur, zum anderen haben die traditionellen kritischen Infrastrukturen zunehmend Berührungspunkte mit Informations- und Kommunikationstechnologien.[216] So nutzen etwa die Online-Handelssysteme der Börsen oder das E-Government-Projekt der öffentlichen Verwaltung die Informations- und Kommunikationstechnologie für operative Abwicklungen. Nicht zuletzt sind kritische Infrastrukturen damit auch vom Internet

---

214 Sonderstab des BSI „kritische Infrastrukturen" http://www.bsi.bund.de/fachthem/-kritis/index.htm (30.05.2006). Kritische Infrastrukturen werden weltweit unterschiedlich beurteilt. So tritt in den USA neben das Konzept der Abhängigkeit ein Konzept der symbolischen Funktion. Es bedarf in den USA nicht ausschließlich einer lebenswichtigen Funktion: Kritische Infrastrukturen sind Ziele, dessen, *„destruction would not endanger vital systems, but could create local disaster or profoundly damage our nation's morale and confidence"*, Moteff, John,/Copeland, Claudia/Fischer, John, Critical Infrastructures: What makes an Infrastructure Critical? Congressional Research Service (CRS) report for Congress RL31556, 29.01.2003, http://www.fas.org/irp/crs/RL31556.pdf (30.05.2006).

215 Sonderstab des BSI „kritische Infrastrukturen", http://www.bsi.bund.de/fachthem/-kritis/index.htm (30.05.2006). Die kritische Infrastruktur Telekommunikation wird lediglich begrifflich traditionell aufgeführt, inhaltlich ist der Begriff mit den Ausprägungen der Informations- und Kommunikationstechnologien zu füllen.

216 So wurde etwa durch einen Softwarefehler das Telefonnetz in Mittelhessen für mehrere Stunden lahm gelegt, Ursache war ein Absturz der Vermittlungssoftware in einem zentralen Netzknoten, vgl., heise news vom 11.11.2004, http://www.heise.de/newsticker/-meldung/53162 (30.05.2006).

abhängig. Der Schutz der kritischen Informations- und Kommunikationsinfrastruktur ist eine Aufgabe der IT-Sicherheit fokussiert auf die Sicherheit im Internet.[217]

Zu dem Verhältnis der kritischen Infrastrukturen und den Informations- und Kommunikationstechnologien sollen drei Punkte hervorgehoben werden.

Erstens, die bereits angedeutete Interdependenz der kritischen Infrastrukturen. Diese kann allerdings nicht auf die Abhängigkeit von den Informations- und Kommunikationstechnologien reduziert werden, da diese ebenfalls abhängig von der Energieversorgung sind. Dies wird auch als *„interrelated trio of electrical energy, communication and computers"* [218] bezeichnet. Die Abhängigkeit von den Informations- und Kommunikationstechnologien ist im zunehmenden Maße auch eine Abhängigkeit von der Ausgestaltung ihrer Standards:

> *„Das Funktionieren der kritischen Infrastrukturen, wie Energieversorgung, Telekommunikation, Banken-, Notfall- und Rettungswesen, Wasserversorgung, usw., hängt in zunehmendem Maß von den unterstützenden Informations- und Kommunikationssystemen ab. So rücken Normen und Standards ins Blickfeld, mit denen technische Aspekte überwacht und die Zusammenschaltung und Interoperabilität von Netzen sichergestellt werden sollen, da sich die Grenzen zwischen Telefon und Computer einerseits und zwischen Sprach- und Datenkommunikation andrerseits langsam auflösen."* [219]

Zweitens, die Relation der Wahrscheinlichkeit zu der Machbarkeit eines Angriffs erweist sich bei den Informations- und Kommunikationstechnologien als äußerst günstig. Während das Bedrohungspotenzial etwa bei der Atomkraft mit einer geringen Wahrscheinlichkeit des Angriffs zu einer schweren Machbarkeit relationiert werden kann, steht bei den Informations- und Kommunikationstechnologien eine hohe Wahrscheinlichkeit einer leichten Machbarkeit gegenüber.[220] Dieses realisiert sich etwa in den Denial of Service (DoS) Angriffen[221] auf Informations- und Kommunikationssysteme. DoS Angriffe unterliegen nicht nur einer hohen Wahrscheinlichkeit, sondern sind kostengünstige und technisch einfach machbare (ohne großen Aufwand und Kenntnisse) Angriffe.

Drittens werfen Angriffe auf die kritische Infrastruktur Informations- und Kommunikationstechnologie die Frage nach der Abgrenzung innerer und äußerer Si-

---

217 Wenger/Metzger (Hrsg.), International CIIP Handbook 2004, An Inventory and Analysis of Protection Policies in Fourteen Countries, 2004, S. 22.

218 Wenger/Metzger (Hrsg.), a,a.O (Fn. 217), S. 18.

219 Jahresbericht der RegTP 2003, S. 62, a.a.O., (Fn. 145).

220 Eine Tabelle mit den entsprechenden Relationen findet sich bei Hutter/Neubecker, Kritische IT-Infrastrukturen, in: DuD 2003, 211 (212).

221 DoS Attacken sind gezielte Anfragen auf einen Server, die dieser in der Quantität nicht bearbeiten kann und diesen zusammenbrechen lassen sollen, http://www.bsi-fuer-buerger.de-/abzocker/05_04.htm (30.05.2006).

cherheit auf. Begriffe wie *„Cyberwar"*[222] und *„Information Warfare"*[223] deuten auf eine Angelegenheit der äußeren Sicherheit hin, während die innere Sicherheit etwa durch Sachverhalte wie der Verbreitung pornographischer Inhalte betroffen sein kann.

2. Anwendungen und Dienste – Software

a) Anwendungen und Dienste

Anwendungen sollen hier in interne und externe Anwendungen unterteilt werden. Interne Anwendungen sind Anwendungen, die die Installation einer Software voraussetzen, etwa das Betriebssystem, Office-Anwendungen oder lokal installierte Computerspiele, und grundsätzlich nicht vom Netz abhängig sind. Ist der Rechner als Client an das Internet angeschlossen, können interne Anwendungen Bedeutung für die Sicherheit des Systems[224] haben. So können Eigenschaften der Infrastruktur von internen Anwendungen unterstützt werden. Insbesondere kann die Wahl des Betriebssystems bei der Stabilität des Rechners – und somit bei der Sicherheit – eine große Rolle spielen.

Externe Anwendungen soll als die Interaktion von installierter Software und (techno)logische Infrastruktur (Dienste) begriffen werden. Sicherheitslücken können dann entstehen, wenn die interne Anwendung und die (techno)logische Infrastruktur interagieren. So verstandene externe Anwendungen sind Dienste, die durch einen externen Diensteanbieter (Anbieter von Infrastruktur oder Webseiten) auf dem Client (durch installierte Software) ermöglicht werden. Hierunter fallen etwa Anwendungen wie E-Mail, http oder ftp. Das www[225] – ein weit verbreitetes Angebot des Internets – ist kein Dienst, sondern eine Plattform für verschiedene Dienste. Die Nutzung des www wird durch den Browser ermöglicht. Der Browser ist eine

---

222 So probte etwa die Bundeswehr 2001 in einem virtuellen Planspiel den Cyberwar: http://www.uni-kassel.de/fb10/frieden/themen/Infowar/probe.html (30.05.2006).

223 Mit „Information Warfare" wird der Kampf auf militärischer oder wirtschaftlicher Ebene um Informationen bezeichnet, Minkwitz/Schöfbänker, „Information Warfare, telepolis vom 31.05.2000, http://www.heise.de/tp/r4/html/result.xhtml?url=/tp/r4/artikel/6/6817/-1.html&words=Information%20warfare (30.05.2006).

224 Unter System wird hier die Gesamtheit der infrastrukturellen und anwendungsbedingten Komponenten verstanden.

225 Das www (World Wide Web) ist kein Dienst, sondern ist ein Hypertext System, das verschiedene Dienste integrieren und durch Hyperlinks ausführen kann. Es erlaubt von einer Information zur nächsten zu springen, auch wenn diese auf unterschiedlichen Servern gespeichert sind. Dadurch entsteht die Vernetzung von Information, die das „Internet" (so liegt die Gleichsetzung von www und Internet nahe) ausmachen.

Software mit dessen Hilfe Inhalte im Internet dargestellt werden. Hierbei unterstützen Browser Dienste wie http oder ftp. Die Dienste sind in der Regel durch die (techno)logische Infrastruktur definiert. So wird der Dienst E-Mail durch das smtp-Protokoll ermöglicht.

Zur Darstellung der Inhalte und Gestaltung der Webpräsenz werden bestimmte Programmiersprachen eingesetzt. Eine häufig verwandte Sprache ist hierbei html[226]. Sprachen wie Java-Script (oder Module wie ActiveX) ermöglichen dynamische Darstellungen zulasten der Sicherheit. JavaScript ist eine Sprache, die auf dem Client ausgeführt wird. Dabei können Elemente der Website manipuliert werden, nachdem sie auf den Client übertragen wurden.[227]

Eine das Surfen erleichternde Anwendung ist der Cookie, eine kleine Datei, die auf dem Client die Daten der Internet-Session speichert. So werden bei der Onlinebestellung die Funktionen des Einkaufskorbs oder die Speicherung von Benutzereinstellungen ermöglicht. Dabei gibt es Cookies, die dauerhaft, und solche, die nur für die Session gespeichert werden.[228] Er ermöglicht es, die Session und mögliche Passwort- und Benutzereingaben zu rekonstruieren und bietet damit ein hohes Missbrauchspotenzial.[229]

Diese Beispiele sollen das Verhältnis von Benutzerfreundlichkeit und Sicherheit verdeutlichen. Gerade Software, die eine bestimmte interaktive Nutzung des Internets erst ermöglicht, kann eine potenzielle Sicherheitslücke des Internets darstellen, weshalb im Folgenden Software näher behandelt werden soll.

b) Software

aa) Software 1 – proprietäre Software

„Proprietär" – ein Begriff mit Nuancen – kann Software klassifizieren. Im juristischen Kontext urheberrechtlich entsprechend, kann proprietär im technischen Bereich nicht ohne weiteres so verstanden werden. Proprietäre Software ist grundsätzlich Software, die keine „freie" Software ist.

---

226 Hypertext Markup Language.

227 Vgl. die Ausführungen in dem Internet Lexikon Wikipedia, http://de.wikipedia.org/-Fwiki/JavaScript (30.05.2006).

228 Weiterführende Informationen im Internetlexikon Wikipedia, http://de.wikipedia.org/-wiki/Cookie (30.05.2006).

229 Daneben besteht die Gefahr, dass durch Cookies Nutzerprofile erstellt werden können, wenn etwa der Kundenname und die besuchten Webseiten zusammengeführt werden.

„Proprietäre“ Software wird in dieser Arbeit verstanden als Software, die in jedem Fall urheberrechtlich geschützt ist, deren urheberrechtlicher Schutz auch nicht (freiwillig) eingeschränkt ist und deren Quellcode grundsätzlich[230] nicht offen gelegt wird. Der Quellcode ist der lesbare Programmtext in einer Programmiersprache.[231] Sein Studium kann wichtig für die Beurteilung der Sicherheit und der Qualität der Software sein. Ohne Kenntnis von diesem kann der Nutzer nur auf die Angaben des Herstellers vertrauen.

bb) Software 2 – Open Source Software, Freeware und Shareware

Die Open Source Software ist dadurch gekennzeichnet, dass der Quellcode des Programms der Anwendung offen gelegt wird.[232] Mit dem Quellcode kann das Programm als Software frei[233]verbreitet werden. Durch die Möglichkeit aller Anwender zur Verbesserung beizutragen steht die Open Source Software in dem Ruf sehr stabil zu sein.[234] Die Open Source-Bewegung kann als interdisziplinäres Projekt der Informatik (ubiquitäre Entwicklung und Optimierung von Software), der Ökonomie (ist Open Source Software betriebswirtschaftlich sinnvoll?) und des Rechts (welche

---

230 „Grundsätzlich“ will die Ausnahme andeuten, die etwa ein Hersteller einer weit verbreiteten Software Regierungskreisen anbietet. Im “Government Security Program (GSP)” will dieser Hersteller aus Gründen der Sicherheit der IT-Systeme Regierungsbehörden den Quellcode offenlegen, vgl. http://www.microsoft.com/presspass/features/2003/Jan03/01-14gsp-mundie.asp (30.05.2006): *“Recognizing that government agencies have a vital interest in building and implementing information systems that they can trust to be safe and secure, Microsoft has established a new program that provides national governments with access to Windows source code and other technical information. Called the Government Security Program (GSP) this new initiative is designed to provide governments and international organizations with information about the Windows Platform, enhancing their ability to design and deploy secure computing infrastructures.”*

231 Vgl. die Ausführung im Internetlexikon Wikipedia, Quellcode ist der für Menschen lesbare in einer Programmiersprache geschriebene Text eines Programms oder Software, http://de.wikipedia.org/wiki/Quellcode (30.05.2006).

232 Eine genaue Definition der Open Source Software findet sich bei der ISO in der derzeit gültigen Version 1.9, vgl, Kharitoniouk/Stewin, Grundlagen und Erfahrungen, in: Gehring/Lutterbeck (Hrsg.), Open Source Jahrbuch 2004, 2004, S. (7). Nach der Free Software Foundation muss eine Freie Software folgende Aspekte erfüllen: 1. Die Freiheit, ein Programm für jeden Zweck einsetzen zu dürfen, 2. Die Freiheit untersuchen zu dürfen, wie ein Programm funktioniert und es den eigenen Bedürfnissen anzupassen, 3. Die Freiheit, Kopien für andere machen zu dürfen und 4. Die Freiheit, das Programm verbessern zu dürfen und diese Verbesserung zum allgemeinen Wohl zugänglich zu machen.

233 „*Freie Software‘ hat etwas mit Freiheit zu tun, nicht mit dem Preis. Um das Konzept zu verstehen, ist an ‚frei‘ wie in ‚freier Rede‘, und nicht wie in ‚Freibier‘ zu denken.“*, Free Software Foundation (2002): Die Definition Freier Software, http://www.gnu.org/philosophy/free-sw.de.html (30.05.2006).

234 Kharitoniouk/Stewin, a.a.O., (Fn. 232), S. 1 (1).

Implikationen hat eine Lizenz einer Open Source Software?) begriffen werden.[235] Ein prominentes Beispiel für eine Open Source Software ist Linux, ein Betriebssystem.

In einem ökonomischen Kontext sollte zwingend von Open Source statt von freier Software gesprochen werden, denn der Begriff frei vermittelt das für Open Source Software nicht immer zutreffende Attribut einer kostenlosen Distribution.

Zwischen dem Internet und der Open Source Software können Interdependenzen in der Entwicklung und Unterstützung von Anwendung und (techno)logischer Infrastruktur bestehen; so basiert das DNS hauptsächlich auf einer Open Source Software.[236]

Freie Software im Sinne von kostenlos wird als Freeware bezeichnet. Freeware heißt aber nicht, dass die Software frei von Rechten ist. Wie frei verfügbar Freeware daher angeboten wird und welchen Einschränkungen die Weiterverbreitung unterliegt, ist den Lizenzbedingungen im Einzelfall zu entnehmen.

Eine Zwischenstellung nimmt die Shareware ein. Shareware ist in der Regel die Überlassung einer (Teil-)Version mit einer meist zeitlich auflösenden Bedingung der Bezahlung nach einer Testphase. Shareware ist demnach ein Vertriebskonzept.

cc) Software 3 – Sicherheitslücken

Der Lebenszyklus von Software unterscheidet sich von herkömmlichen (materiellen) Produkten. Während der Lebenszyklus von herkömmlichen Produkten in mehreren Phasen unterteilt werden kann und die Entwicklung grundsätzlich in einer bestimmten Phase abgeschlossen ist,[237] unterliegt die Software einer „lebenslangen" Entwicklung.[238] Nicht selten spricht man bei Software von *„Bananensoftware"*,

---

235 Diese Ausgangspunkte der Betrachtung (inklusive eines soziologischen Ansatzes) finden sich bei Gehring/Lutterbeck (Hrsg.), Open Source Jahrbuch 2004, 2004, http://ig.cs.tu-berlin.de/osjb/OpenSourceJahrbuch2004.pdf (30.05.2006).

236 So ist BIND (Berkeley Internet Name Domain), eine Software zum Betrieb eines Domain Nameservers, eine Open Source Software, http://de.wikipedia.org/wiki/Domain_Name_System (30.05.2006).

237 Einführungsphase, Wachstumsphase, Reifephase und Altersphase, vgl. Stolpmann, Konzeption eines Software-Lifecycle-Managementsystems, 2003, http://miless.uni-essen.de/servlets/DerivateServlet/Derivate-11865/dissertation.pdf (30.05.2006).

238 „*Der wesentliche Unterschied zwischen den beiden Prozessen wird durch die beiden letzten Teilbereiche Anwendung und Wartung ausgelöst. Der Softwareentwicklungsprozess ist streng genommen durch die Auslieferung noch nicht beendet, da durch die Anwendung erhebliche Änderungen und Erweiterungen von dem Produkt gefordert werden können, was wiederum nicht nur den Erhalt der Funktionalitäten bedeuten kann sondern auch zu einer völligen Neuentwicklung führen kann.*", vgl. Stolpmann, a.a.O., (Fn. 237), S. 13.

die, ähnlich der Frucht, beim Nutzer reift.[239] Nicht selten reift die Software auch in ihren Sicherheitsbestimmungen.

Als technischer Laie ist man geneigt zu fragen, warum die Erreichung von Sicherheit bei Software so schwierig erscheint. Wie für jedes Produkt gibt es auch für Software eine Phase der Erprobung. Hierbei soll es ungleich komplexer sein, die Software auf Sicherheit als auf Funktionalität zu testen:

> *„Security testing is quite different from typical software testing. Normal software testing checks for the accuracy of output from given input and tests for the reporting of specific errors. However, security testing deals with how the system responds to the unexpected.“*[240]

Sicherheit kann nur aussagekräftig bewertet und getestet werden, wenn es Sicherheitsspezifikationen gibt, d. h. Sicherheitskriterien, die als einheitliche und verbindliche Standards für Software gelten.[241]

Die Begriffe Software und Sicherheitslücke können mit dem Exploit gleichsam auf den Punkt gebracht werden. Zudem repräsentiert er die Ambivalenz von Information und Sicherheitslücke: Als Programm zur Demonstration der Sicherheitslücke geschrieben ist es grundsätzlich eine nützliche Information. Eingesetzt zur Ausnutzung der Sicherheitslücke trägt es eine spezifische „Schadinformation“ in sich.

Als häufigste Sicherheitslücke soll hier exemplarisch der „Buffer Overflow“ kurz vorgestellt werden.[242] Als „Buffer Overflow“ ist ein Fehler im Programm zu bezeichnen, durch den große Datenmengen in einen unterdimensionierten Speicherbereich geschrieben werden, wodurch möglicherweise schadhafter Code in den Speicher geschrieben wird. „Verantwortlich“ für die Sicherheitslücke sind somit die Programmierer. In den meisten Fällen führt der Buffer Overflow zu einem Absturz der Anwendung. Der Buffer Overflow kann jedoch auch als Schwachstelle ausgenützt werden, da er zur Folge haben kann, dass das rückführende Unterverzeichnis durch beliebige Informationen überschrieben und so ein beliebiger, ausführbarer Code eingeführt werden kann.

Die Affinität von proprietärer Software, Open Source Software, Freeware oder Shareware zu Sicherheitslücken wird mannigfach beurteilt. Die Ambivalenz kann anhand folgenden Zitats für eine proprietäre Software deutlich gemacht werden:

---

239 Heussen, Unvermeidbare Softwarefehler, in: CR 2004, 1 (2).

240 Pipkin, Information Security, 2000, S. 41.

241 Lutterbeck/Horns/Gehring, Sicherheit in der Informationstechnologie und Patentschutz für Software-Produkte, 2000, S. 111, http://www.ipjur.com/data/LuGeHo.pdf (30.05.2006).

242 Vgl. etwa Kallnik/Pape/Schröter/Strobel, Das Sicherheitsloch, 2001, http://www.heise.de/-ct/01/23/216/ (30.05.2006).

Der marktbeherrschende Browser,

> *„weist durch die starke Integration in das Betriebssystem Windows und die ActiveX-Funktionen allerdings auch mit Abstand die meisten Sicherheitslücken auf (bzw. sind die meisten bekannt).“*[243]

Diese Ausführung wurde zitiert, um den ambivalenten Beitrag von Software für die Sicherheit in der Abhängigkeit von der Verbreitung hervorheben zu können. Zum einen kann auf die weite Verbreitung proprietärer Software, trotz bekannter Sicherheitslücken, hingewiesen werden. Zum anderen sind Alternativen (etwa in der Open Source Software) vielleicht gar nicht sicherer, sondern nur weniger Ziel von Angriffsversuchen.[244] Sicherheit könnte demnach keine Frage von proprietärer oder Open Source Software, sondern deren Verbreitung sein.

III. Nutzungs- und nutzerbedingte Sicherheitslücken und Schwachstellen

Im Folgenden sollen die in der Infrastruktur angelegten Sicherheitslücken in ihren Auswirkungen bei der Nutzung durch Praxisbeispiele dargestellt werden. Hierbei bietet sich eine Differenzierung nach Art der Nutzung an. Zunächst sollen jedoch kurz die Akteure der Nutzung des Internets dargestellt werden.

1. Hersteller, Anbieter und Nutzer

Differenziert wird grundsätzlich zwischen dem Hersteller, dem Anbieter und dem Nutzer. Während der Hersteller von Software ein verständlicher Begriff ist, bedarf das dieser Arbeit zu Grunde liegende Verständnis des Anbieters einer Einführung.

---

243 Statt vieler die Ausführungen in dem Internet Lexikon Wikipedia, http://de.wikipedia.org/wiki/Webbrowser (30.05.2006). ActiveX ist ein Softwaremodul, das die Einbettung beliebiger Objekte in fremde Dokumente erlaubt. Sie werden vom Browser aufgerufen und können dann unabhängig vom Browser laufen, http://de.selfhtml.org/intro/technologien/activex.htm (30.05.2006).

244 Diesen Aspekt will das BSI mit Empfehlungen augenscheinlich nutzen. Wie einer Meldung bei heise news zu entnehmen ist, empfiehlt ein Sprecher des BSI in einem Zeitungsinterview einen Wechsel vom Internet Explorer etwa zu Mozilla oder Opera, mit der Begründung, dass die meisten Viren und Würmer auf Microsoft-Programme zugeschnitten sind, vgl. heise news, Bundesamt empfiehlt Browser-Wechsel, vom 11.09.2004, http://www.heise.de/newsticker/meldung/50965 (30.05.2006). In dem betreffenden Artikel in der Berliner Zeitung heißt es weiterhin: „*Zudem wiesen auch Explorer-Konkurrenzprodukte Sicherheitslücken auf. Jedoch seien die meisten PC-Viren auf die weit verbreiteten Microsoft-Programme zugeschnitten. Sein Amt würde daher das Entstehen eines "Mischwaldes" aus verschiedenen Browserprogrammen begrüßen, sagte er.*“, Wendel, Thomas, Warnung vor Internet-Banking, Berliner Zeitung, 11.09.2004.

a) Hersteller

Unter Hersteller werden in dieser Arbeit diejenigen zusammengefasst, die Hardware herstellen, oder die Software programmieren, produzieren und an den Nutzer distribuieren.[245] Hierbei kommt es nicht auf die Absicht an gewerblich zu handeln oder Gewinn zu erzielen. Hersteller ist in diesem Sinne auch der private Programmierer, der mit seinen Programmen die Nutzer des Internets bereichern will und nicht sich selbst.

b) Anbieter

In der Umgangssprache sind Anbieter als Provider,[246] diejenigen, die Internetdienste anbieten. In der Gesetzessprache finden sich diese als Diensteanbieter im Telekommunikationsgesetz (§ 3 Nr. 6 TKG) Teledienstegesetz (§ 3 Nr. 1 TDG), und Mediendienstestaatsvertrag (§ 3 Nr. 3 MDStV) definiert. Ohne sich hier mit den inhaltlichen Unterschieden der Gesetze auseinandersetzen zu müssen, soll exemplarisch auf § 3 Nr. 1 TDG verwiesen werden:

> *„(…) jede natürliche oder juristische Person, die eigene oder fremde Teledienste zur Nutung bereit hält oder den Zugang zur Nutzung vermittelt;“*

Im Folgenden soll mit diesem weiten Verständnis „*jeder nur denkbare Handelnde*“[247] als Anbieter verstanden werden, ohne auf eine funktionelle Trennung des Anwendungsbereichs entsprechend dem TDG und MDStV Rücksicht nehmen zu müssen.

Als Anbieter wird darüber hinaus auch der Inhaber der Domain verstanden. Anbieter ist mithin der Verantwortliche, der Entscheidungen über das Angebot und seine Außenwirkung treffen kann und in dessen Interesse der Webauftritt angeboten wird. Soweit wie im Szenario 3 die Administration des Internetauftritts einem Provider übertragen wurde, wird als Anbieter der Inhaber des Online-Shops verstanden.

Ungeachtet der staatlichen[248], gewerblichen oder privaten Verfasstheit des Akteurs wird jeder als Anbieter verstanden, der informierende oder interaktive Informationsangebote für den Nutzer bereithält.

---

245 Hier kann etwa auf den Produzenten im Rahmen der Produzentenhaftung verwiesen werden, vgl. etwa MünchKommBGB/*Wagner,* § 823 Rd. 556 ff.

246 Nicht immer trennscharf wird etwa zwischen Access-, Hosting-, (Internet) Service- und Application Service-Provider unterschieden.

247 Spindler/Schmitz/Geis-*Spindler* TDG § 3 Rd. 3.

c) Nutzer

Nutzer ist zunächst ungeachtet der staatlichen, gewerblichen oder privaten Verfasstheit des Akteurs jeder, der Angebote im Internet nachfragt. Exemplarisch kann auf die Definition in § 3 Nr. 2 TDG verweisen werden:

> *„(…) jede natürliche oder juristische Person, die zu beruflichen oder sonstigen Zwecken Teledienste in Anspruch nimmt, insbesondere um Informationen zu erlangen oder zugänglich zu machen;"*

Soweit nach dieser Definition auch Anbieter Nutzer sein können,[249] soll das Verständnis des Nutzers für diese Arbeit eingeschränkt werden. Nutzer ist hier grundsätzlich nur derjenige – ungeachtet der staatlichen, gewerblichen oder privaten Verfasstheit – der Informationen abfragt. Soweit sich die Ausführungen auf den privaten Nutzer beschränken, wird dies im Text deutlich gemacht.

2. Nutzungsbedingte Sicherheitslücken und Schwachstellen

Die Nutzungen des Internet lassen sich am Akteur orientiert in E-Commerce (b2c[250]), E-Procurement (b2b[251]) und E-Government (g2g[252], g2c[253] und g2b[254]) sowie sonstiger Kommunikation c2c[255] einteilen. Auf beispielhafte Sicherheitslücken und Schwachstellen soll im Folgenden ungeachtet der Verfasstheit des Akteurs am Angebot orientiert hingewiesen werden.

a) Informative Webpräsenz

Bei einer Webpräsenz, d. h. ein Informationsangebot, gilt für die damit verbundenen Sicherheitsanforderungen: Gewünscht ist der lediglich lesende Zugriff der Interessenten auf die Daten. Geschützt werden müssen die Daten vor dem unberechtigt schreibenden Zugriff mithin vor Manipulation (Schutz der Integrität) und dar-

---

248 Zu den kommunalverfassungsrechtlichen Spielräumen der Kommunen als Diensteanbieter im Internet, Holznagel/Temme, Kommunen im Internet, in: Hoeren/Sieber, Handbuch Multimediarecht. Teil 26, 1999.

249 Vgl. Ausführungen bei Spindler/Schmitz/Geis-*Spindler* TDG § 3 Rd. 17 f.

250 Business to Customer.

251 Business to Business.

252 Government to Government.

253 Government to Citizen; anders: Boehme-Neßler, Electronic Government, in: NVwZ 2001, 374 (367): A2C-eCommerce (Adminstration-to-consumer-electronic-commerce).

254 Government to Business.

255 Client to Client.

über hinaus vor Ausfall (Schutz der Verfügbarkeit) geschützt werden. Gefährdungspotenziale sind hierbei unternehmens- und behördenintern sowie -extern zu suchen. Der Prozess der redaktionellen Veröffentlichung und Pflege der Webpräsenz soll durch einen internationalen Standard abgesichert werden,[256] in dem sich die Gefährdungen durch Manipulation und Ausfall widerspiegeln.[257]

Ein Fall der Manipulation, der in der Presse bekannt wurde, war die des Bundeswehrservers in Straußberg. Der Inhalt der Webpräsenz bundeswehr.de war vorübergehend nicht erreichbar, stattdessen informierte das Foto zweier Herren und der Slogan „Make love, not war ;)" interessierte Bürger.[258] Diese Meldung macht deutlich, dass Sicherheit im Internet nicht immer eine ernsthafte Gefährdung für Rechtsgüter darstellen muss, ein lediglich „humoriger Auftritt" zumindest aber die Reputation gefährden kann. Diese Meldung zeigt aber auch, wie in der Praxis über aufgedeckte Sicherheitslücken informiert wird. Teilweise werden ohne Rücksichtnahme auf die Reputation Sicherheitslücken öffentlich bekannt gemacht.

Die Trennung zwischen der informativen Webpräsenz und der im Folgenden beschriebenen interaktiven Webseite ist beim Einsatz von Cookies, die auf dem Rechner des Nutzers abgelegt werden, nicht immer trennscharf möglich.

b) Interaktive Webseite

Eine im Vergleich zur bloßen Webpräsenz „gesteigerte" Form – und damit E-Commerce und E-Government im eigentlichen Sinne – ist der Vertragsschluss bzw. die Verwaltungsabwicklung im Internet. Dieser erfordert neben einer Webpräsenz[259] zusätzlich die Möglichkeit zur Interaktion. Interaktion bezeichnet die in-

---

256 RFC 2518, HTTP Extensions for Distributed Authoring – WEBDAV, 1999, http://-www.faqs.org/RFCs/RFC2518.html (30.05.2006). WebDAV steht für Webbased Distributed Authorig and Visioning. Das RFC 2518 ergänzt RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1, 1999, http://www.faqs.org/RFCs/RFC2616.html (30.05.2006) und wird selbst durch das RFC 3253, Versioning Extensions to WebDAV, 2002, http://www.faqs.org/RFCs/RFC3253.html (30.05.2006) ergänzt.

257 So wird als Maßnahme die Authentifizierung empfohlen. Im RFC 2518, Punkt 17.1 heißt es: *"…WebDAV servers need to use authentication technology to protect not just access to a network resource, but the integrity of the resource as well."*

258 Vgl. heise news vom 20.01.2003, http://www.heise.de/newsticker/meldung/33818 (30.05.2006).

259 In diesem Fall ist der wertschöpfende Geschäftsprozess unmittelbar von der Verfügbarkeit der Webpräsenz abhängig. Die Anforderungen an Manipulation und Ausfall der Webpräsenz sind deshalb höher zu bewerten, wenn es um mehr geht als den guten Ruf, vgl. Raepple, Sicherheitskonzepte für das Internet, 2001, S. 316.

dividuelle Reaktion eines Systems auf die Eingaben seiner Nutzer.[260] Diese Interaktionsmöglichkeiten reichen im E-Commerce von der Nutzung einer Suchmaschine, in der Regel ohne rechtlichen Bindungswillen, über die Hotelreservierung bis zum Vertragsschluss über das Internet, etwa bei der Bestellung eines Buches. Im E-Government kann etwa die elektronische Auftragesvergabe e-Vergabe[261] genannt werden.

Ausgehend von einem virtuellen Vertragsschluss reicht ein anonymer Modus Operandi nicht aus und ein Nachweis der gegenseitigen Identität ist erforderlich.[262] Hierbei müssen sowohl die Kundendaten, etwa Bankverbindungen, vor „Blicken Dritter" (Vertraulichkeit), als auch die Kunden- und Transaktionsdaten vor Manipulation (Integrität) geschützt werden.[263]

c) Internetzugang

Entschließt sich das Unternehmen oder die Behörde, das Internet als Mittel der Informationsbeschaffung und Kommunikation für seine Mitarbeiter einzusetzen, so gilt die Aufmerksamkeit wohl der Zugriffskontrolle. Diese Kontrolle soll sowohl den unberechtigten Lese- als auch Schreibzugriff auf Daten des internen Unternehmensrechners oder -netzes verhindern. Daneben ist zur Minimierung der Sicherheitsrisiken zu überlegen, welche Protokolle und Dienste für welche Mitarbeiter erforderlich sind. Insgesamt ist für die Anbindung an und Nutzung des Internets ein Sicherheitskonzept zu erarbeiten.

Eine qualifizierte Form des Internetzugangs ist das Extranet. Darunter ist der Zusammenschluss der Intranets mehrerer geographisch verteilter Niederlassungen zu einem Netz zu verstehen. Ziel ist es, den Außenstellen-Mitarbeitern des Unternehmens oder der Behörde die gleichen Unternehmensressourcen zur Verfügung zu stellen, wie den Mitarbeitern am Hauptsitz. Die Übermittlung des Datenverkehrs erfolgt hierbei über das Internet. Der Fokus der Sicherheitsanforderungen liegt hier auf der Verfügbarkeit (soweit der Zusammenschluss im Betriebsablauf vorausge-

---

260 Raepple, a.a.O., (Fn. 259), S. 327.

261 Vgl. etwa staatliche Ausschreibungen und Vergabe auf http://www.e-vergabe.bund.de (30.05.2006).

262 Raepple, a.a.O., (Fn. 259), S. 328.

263 Zum Schutz des Abrufs von personenbezogenen Daten der Kunden soll demnach grundsätzlich eine vorherige Authentifizierung mittels Benutzername und Passwort erforderlich sein. Zusätzlich sollte die Übermittlung der Daten mittels einer SSL (Secure Sockets Layer) verschlüsselt werden.

setzt wird), der Integrität und Vertraulichkeit der Datenübermittlung. Abgesichert wird dies in der Regel über VPN-Gateways[264].

Einen innovativen Ansatz verfolgt der Finanzsenat Bremen, der Sicherheit durch Kompetenz schaffen will. Der Finanzsenat Bremen hat eine Internetrichtlinie *„Richtlinie für die Bereitstellung und Nutzung von Internet-/Intranetzugängen"*[265] verabschiedet. Diese interne Dienstanweisung will die Medienkompetenz der Mitarbeiter fördern, was letztendlich auch der Sicherheit dient. Gemäß Nr. 3 Abs. 3 der Internetrichtlinie, soll die Dienststelle die

> *„Teilnahme der Mitarbeiter und Mitarbeiterinnen an Schulungen und Informationen über Sicherheitsrisiken und die geeigneten Maßnahmen zur Gewährleistung von Datenschutz und –sicherheit am Arbeitsplatz"*

sicherstellen.

3. Nutzerbedingte Sicherheitslücken und Schwachstellen

Nicht immer trennscharf von den system- und nutzungsbedingten Sicherheitslücken und Schwachstellen zu differenzieren ist der Nutzer, der als „Faktor Mensch" die größte Sicherheitslücke darstellt. Aufgrund der praktischen Bedeutung sollen einige Ausführungen gemacht werden.

> *„Das schwächste Glied in der Kette der ITSicherheit ist jedoch in vielen Fällen der Risiko-Faktor Mensch."*[266]

> *„Bedeutendster Gefahrenbereich bleibt „Irrtum und Nachlässigkeit eigener Mitarbeiter" (…)."*[267]

Hierbei „unterstützen" und ergänzen sich menschliche und technische Sicherheitslücken gegenseitig:

> *„Meist handelt es sich aber um menschliche Schwächen, die einen Rechner unsicher machen: fehlerhaft eingestellte Zugriffsrechte für Dateien, Benutzeraccounts ohne Paßwort, Verwendung von unsicheren Programmen und ähnliches."*[268]

Der Nutzer ist Rezipient und Adressat der oben dargestellten Angebote. Bezüglich der Sicherheit kann er allerdings selbst aktiv sein. Je nach Verfasstheit kann dies

---

264 Virtual Private Network.

265 Diese Richtlinie ist im Amtsblatt der Freien Hansestadt Bremen, Brem.ABl. Nr. 20 vom 10.02.2004, S. 77 ff., veröffentlicht.

266 Hirschmann/Romeike, IT-Sicherheit als Rating-Faktor, http://www.basel-ii.info/-artikel76.html (30.05.2006).

267 KES und Micrososft Sicherheitsstudie 2004, S. 3, http://www.kes.info/archiv/material/-studie2004/kes-Microsoft-Studie2004-Sonderdruck.pdf (30.05.2006).

268 Plate, Jürgen, Sicherheitsaspekte, in: Fachforum „IT-Sicherheit", http://www.fitug.de/-bildung/kongress/sicher.html#s.4 (30.05.2006).

durch IT-Abteilungen oder Administratoren professionalisiert sein.[269] Allerdings kann selbst der private Nutzer Sicherheitslücken, respektive Angriffen, strukturell durch die Installation oder Aktualisierung spezifischer Software oder die Kenntnis der Sicherheitslücken vorbeugen.

Bei Sicherheitslücken respektive Angriffen – etwa dem Phishing, mit denen konkrete Nutzer angesprochen werden – kann bereits durch einen informierten Nutzer die Realisierung der Gefahr minimiert werden.

Eine neue Qualität besitzt der Nutzer, der von außerhalb über das Internet auf seinen privaten Server zu Hause zugreifen will. Die neue Qualität liegt in der Erhöhung des Gefahrenpotenzials. Der eigene Webserver zu Hause ist eine notwendige Voraussetzung für die Nutzung des „Intelligenten Hauses". Soweit etwa elektrische Geräte von außen bedient werden können oder der Wasserfluss reguliert werden kann – etwa zum Blumengießen während einer längeren Abwesenheit – sind neue Bedrohungen durch Sicherheitslücken des Servers denkbar, wenn dieser von unberechtigten Dritten gesteuert werden kann. Neben der Sicherheitslücke in der physikalischen oder (techno)logischen Infrastruktur ist der Nutzer selbst ein Sicherheitsrisiko, solange er keine fundierten Kenntnisse über die Konfiguration und Implementierung besitzt.

Der Faktor Mensch als Sicherheitslücke kann nur durch aufklärende Informationen minimiert werden. Diese decken sich nicht mit dem Gegenstand der fokussierten Informationsrechte und –pflichten. Diese konzentrieren sich bei Auftreten einer system- oder nutzungsbedingten Lücke auf den Umgang mit dieser und sollen verhindern, dass sich ihr Schadenspotential realisiert. Sie dienen somit weniger der Prävention denn der Reaktion und setzen damit eigentlich bereits eine (teilweise) Überwindung der nutzerbedingten Sicherheitslücke voraus.

IV. Honeypot – bewusste Sicherheitslücke

Ein Honeypot[270] ist ein Computer, dessen Zweck darin besteht, gescannt und angegriffen zu werden.[271] Sinn dieser bewussten Sicherheitslücke ist der Schutz des eigenen Systems durch Penetrationstests um Kenntnisse über die Techniken und

---

269 Durch das Raster fällt der Kleinunternehmer oder ein mittelständischer Betrieb ohne entsprechendes Personal und Ausstattung.

270 Honeynet, wenn mehrere Honeypots zusammengeschlossen werden.

271 Biecker, Fabian, Honeypots, in: Datenschleuder, Nr. 81, Juli 2003, https://ds.ccc.de/-081/honeypot (30.05.2006).

Werkzeuge der Angreifer zu erhalten. Als technischer „agent provocateur“ kann der Anbieter eines Honeypot den Grundsätzen des rechtlichen „agent provocateur“ unterworfen sein. Rechtlich käme etwa eine Anstiftung zum Ausspähen von Daten nach § 202a StGB in Betracht.[272] Soweit allerdings Angriffe auf Honeypots erwünscht sind,[273] fehlt es wohl regelmäßig an dem unbefugten Zugang und somit an der rechtswidrigen Tat im Sinne des § 26 StGB.

V. Reaktion auf Sicherheitslücken – Schutzmaßnahmen

Dieser Abschnitt gibt einen Überblick über die Instrumente des Auffindens und Schließens von Sicherheitslücken. Hierbei gilt: Sicherheit kann auch durch das Wissen um eine Sicherheitslücke gesteigert werden, da dieses Wissen – wenn keine mildere Schutzmaßnahme möglich ist – eine Trennung vom Netz rechtfertigen kann.

Allen Maßnahmen gemein ist, dass sie präventiv, operativ und reaktiv ergriffen oder vorgeschrieben werden können. In zeitlicher Hinsicht kann der Sicherheitslücke präventiv vorgebeugt, diese operativ überwacht und kontrolliert oder reaktiv geschlossen werden.

1. Technische Maßnahmen

Klassische technische Maßnahmen zum Aufspüren von Sicherheitslücken sind entsprechend konfigurierte Programme. Durch so genannte Port-Scanner kann etwa nach fehlerhaften Konfigurationen in der (techno)logischen Infrastruktur und der Dienste gesucht werden. Eine versteckte technische Option bei der Suche nach Sicherheitslücken sind die bereits dargestellten „Mobile Agenten“[274]. Das sind Programme, die – in das System eingebracht – dieses nach Sicherheitslücken erkunden können.

---

272 Je nach Konfiguration des Honeypot sind auch anderer Sachverhalte und Tatbestände denkbar. So wurde in der Presse ein Fall bekannt, in dem mit einem simulierten offenen Proxy-Server (ein Server zur Weiterleitung von Daten) ein Spammer identifiziert werden konnte, vgl. Spiegel Online vom 17.01.2006, http://www.spiegel.de/netzwelt/politik/-0,1518,395648,00.html (30.05.2006).

273 Stevens/Pohl, Honeypots und Honeynets, in: Informatik Spektrum, Band 27, Nr. 3 2004, 260 (260).

274 Vgl. Kapitel 2 A I. 1.

Exemplarisch soll eine präventive technische Schutzmaßnahme vorgestellt werden. Im Zuge der unterschiedlichen Verbreitungsformen von Software (proprietäre Software, Open Source Software und Freeware) gibt es die Auseinandersetzung darum, ob die Offenlegung des Quellcodes eine Sicherheitsmaßnahme sein kann. Nur Software, die von jedermann technisch geprüft und weiterentwickelt werden kann, soll ein akzeptables Sicherheitsniveau ermöglichen und erreichen.[275] Open Source Software steht deshalb im Ruf, aufgrund der Offenlegung des Quellcodes sicherer als proprietäre Software zu sein. Grundsätzlich unterliegt Open Source Software einer modularisierten und verteilten Entwicklung und ist im Evaluierungsprozess überschaubarer und überprüfbar.[276]

Allerdings kann die Offenlegung allein noch kein Garant für Sicherheit sein.[277] Theoretisch sollen sich jedoch durch eine Evaluierung des Quellcodes eine Reihe klassischer Sicherheitsrisiken ausschließen und aufdecken lassen: etwa Buffer-Overflows, Parasiten, Sniffer, Spoofing, Trojaner und Viren.[278] Praktisch ist der Quellcode häufig mehrere Millionen Zeilen lang. Demnach wird hinsichtlich der Erhöhung der Sicherheit offen konstatiert:

> *„I'm a fan of open source, and believe it has the potential to improve security. But software isn't automatically secure because it is open source, just as it isn't automatically insecure because it is proprietary."*[279]

Virulent wird diese Frage nicht nur im Kontext von Softwarepatenten.[280] Mit der Patentierung kann der technische Lösungsansatz von einer ökonomischen Kom-

---

275 So das BSI, Bundesamt für Sicherheit in der Informationstechnik: Empfehlungen zum Schutz vor verteilten Denial of Service-Angriffen im Internet. Version 1.1 vom 20.6.2000, http://www.bsi.bund.de/fachthem/sinet/ddos.htm (30.05.2006); Lutterbeck/Horns/Gehring, Sicherheit in der Informationstechnologie und Patentschutz für Software-Produkte, 2000, S. 3, http://www.ipjur.com/data/LuGeHo.pdf (30.05.2006); einschränkend Köhntopp/Köhntopp/Pfitzmann, Sicherheit durch Open Source? Chancen und Grenzen., in: DuD 2000, 508 (512).

276 Durch einen Code-Review können Sicherheitslücken ausfindig gemacht werden, Fehler behoben oder Patches zur Verfügung gestellt werden, vgl. Köhntopp/Köhntopp/Pfitzmann, a.a.O., (Fn. 275), 508 (511 und 513).

277 Hinzu kämen Faktoren wie die tatsächliche und nicht nur mögliche Fehleranalyse, die Durchführung der Fehleranalyse nach den Maßstäben der Qualitätssicherung (übersichtliche Gestaltung, Modularisierung, Dokumentation und entsprechende Tests vor Auslieferung), komfortable Bedienungsoberfläche für Software, deren Sicherheitsoptionen von den Einstellungen des Nutzers abhängig sind. Nicht zuletzt hänge die Sicherheit auch von der Informationspraxis des Nutzers ab, der sich über aktuelle Sicherheitslücken und Patches informieren müsse, Köhntopp/Köhntopp/Pfitzmann, a.a.O., (Fn. 275), 508 (512 f.).

278 Lutterbeck/Horns/Gehring, a.a.O., (Fn. 275) S. 114, http://www.ipjur.com/data/LuGeHo.pdf (30.05.2006), mit Verweis auf Pipkin, Information Security, 2000, S. 44 ff.

279 Schneier, Secrets & Lies, 2000, S. 345.

ponente geprägt sein oder kann sogar durch die ökonomische Praxis, sollten die Softwarepatente sich durchsetzen, verhindert werden.

Unter Berücksichtigung des Nutzers sind technische Spezifikationen der Sicherheit – in proprietärer oder Open Source Software – regelmäßig ambivalent. So stehen sowohl bei präventiven, als auch reaktiven Maßnahmen die Bedienungsfreundlichkeit und Nutzungsmöglichkeiten der Sicherheit entgegen.[281] Der Verzicht auf Ausstattung verringert jedoch die Komplexität, was eine Überprüfung der Software auf Sicherheitslücken erleichtern würde.[282]

Festzuhalten ist, die Implementierung technischer Sicherheit hängt von den Erwartungen und Wünschen des Nutzers und damit nicht zuletzt von den Prioritäten bei der technischen Umsetzung ab.

2. Personelle und konzeptionelle Maßnahmen

Personelle Maßnahmen werden regelmäßig ex ante ergriffen, um das Entstehen von Sicherheitslücken zu verhindern oder um diese schnell erfassen zu können. Der zweite Aspekt bietet einen Anknüpfungspunkt für die hier interessierenden Informationen über Sicherheitslücken. Personelle Maßnahmen sind etwa die Etablie-

---

[280] Im Zusammenhang mit Softwarepatenten: Lutterbeck/Horns/Gehring, a.a.O., (Fn. 278). Für die Erhöhung von Sicherheit durch Offenlegung des Quellcodes: vgl. Gehring, Sicherheit mit Open Source, in: Gehring/Lutterbeck (Hrsg.), Open Source Jahrbuch 2004, S. 209 (229): Die Faktoren [d. Verf.] *„(…) lassen es in ihrer Gesamtheit als gerechtfertigt erscheinen, die Frage danach, ob denn Open-Source bessere – und sicherere – Software hervorbringen würde, mit „ja, oft " zu beantworten."*; Köhntopp/Köhntopp/Pfitzmann, a.a.O., (Fn. 275), 508 (508 ff.). Keine nachweisbare Erhöhung der Sicherheit durch Offenlegung des Quellcodes: Oppliger, Sicherheit von Open Source Software, in: DuD 2003, 669-675; Anderson, Open and Closed Systems are Equivalent (that is, in an ideal world), 2003, http://www.cl.cam.ac.uk/ftp/users/rja14-/toulousebook.pdf (30.05.2006), der ausführt, dass Open Source Software und proprietäre Software grundsätzlich gleich sicher sind. Diese Balance wird durch andere Faktoren wie, *„transient effects, transaction costs, featuritis, interdependent or correlated vulnerabilities, selection effects, incentives for coders and tester (…)"* zugunsten des einen oder anderen Systems verschoben.

[281] So sind im präventiven Bereich etwa bei einer grundsätzlichen Deaktivierung von Cookies bestimmte Funktionen nicht mehr möglich, eine das Surfverhalten überwachende Firewall muss erst „angelernt" werden, was während der Bedienung permanente Entscheidungen des Nutzers über die Vertrauenswürdigkeit bestimmter Seiten oder Cookies erfordert. Reaktive Maßnahmen, etwa eine erforderliche Neuinstallation eines Programms können, zu Datenverlusten führen.

[282] Schneier, Secrets & Lies, 2000, S. 354 f.: *„Complexity is the worst enemy of security. This has been true since the beginning of computers, and is likely to be true for the foreseeable future. (…) The first reason is the number of security bugs. (…) As the complexity of the software goes up, the number of bugs goes up. And a percentage of these bugs will affect security, and not always in tangible ways."*

rung eines Sicherheitsbeauftragten, § 109 Abs. 3 TKG. Als überwachende und kontrollierende Instanz wäre er geeignet, Informationen über Sicherheitslücken zu steuern. Jedoch bietet das Recht keine konkreten Vorgaben im Umgang mit der Information.[283] Es bleibt jedem Unternehmen unbenommen, in einem Sicherheitskonzept die Chancen und Risiken der Information abzuwägen und dem Sicherheitsbeauftragten diesbezüglich Handlungsanweisungen zu geben.

Konzeptionelle Maßnahmen bestehen etwa in der Ausarbeitung eines Sicherheitskonzepts, welches für bestimmte Bereiche in § 109 Abs. 3 TKG vorgeschrieben wird. Sicherheitskonzepte finden sich regelmäßig in größeren Unternehmen, wo sie nicht zuletzt durch § 91 Abs. 2 AktG gefordert werden.

Der Einbindung und Nutzung von Informationen bei personellen und konzeptionellen Maßnahmen sollte regelmäßig eine Interessenabwägung zu Grunde liegen. Zum einen sind die Interessen des Unternehmens (Reputation) bei Bekanntwerden von negativen Informationen über Sicherheit zu schützen. Zum anderen sind die Chancen (Gegenmaßnahmen werden bei Informationen über Sicherheitslücken möglich) und die Risiken (Ausnutzung der veröffentlichten Sicherheitslücken wird möglich) gegeneinander abzuwägen.

3. Information als ambivalente Maßnahme

Der Aspekt Information widmet sich in ambivalenter Weise dem Faktor Mensch. Unter der Prämisse, dass der Mensch das größte Sicherheitsrisiko ist,[284] ist Information eine essenzielle Voraussetzung dafür, dass Menschen die (Eigen)Verantwortung für Sicherheit überhaupt wahrnehmen können. Erst die Information über das „Ob" der Sicherheitslücke erlaubt die Beseitigung der Sicherheitslücke (Information als Schutzmaßnahme).

Andererseits erlaubt erst die Information dem Menschen, eine Sicherheitslücke ausnutzen zu können (Information als Sicherheitslücke). Nach einer Studie erfolgten 2004

> *„etwa 30% aller Angriffe auf IT-Systeme unter Ausnutzung einer bekannten und 15% unter Ausnutzung einer noch nicht bekannten Schwachstelle im Betriebssystem."*[285]

---

283 Vgl. Kapitel 5 B V. zu der Frage, ob sich dem Arbeitsrecht Vorgaben entnehmen lassen; ebenso Mielke, Beruf: Komplize, c´t 2006, Heft 8, S. 170 (170).

284 Schneier, Secrets & Lies, 2000, S. 255.

285 BSI, Lage der IT-Sicherheit in Deutschland 2005, S. 15 f., http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf (30.05.2006).

Die Ambivalenz der Wirkung von Information verschiebt sich jedoch ins Positive, je größer der Informationsvorsprung derjenigen ist, die Information als Schutzmaßnahme begreifen. Insoweit besitzt die Informationsweitergabe als Sicherheitsvoraussetzung neben der inhaltlichen eine starke dynamische und zeitliche Komponente.

Soweit die Kunden – wie im Szenario 3 – nicht unbedingt auf die technischen Details des unbefugten Zugangs, sondern darauf angewiesen sind, überhaupt informiert zu werden „dass" ein unbefugter Zugang zu ihren Daten stattfand, kann sich die Ambivalenz der Information auf eine andere Wirkung beziehen. Durch das Eingeständnis von Schwachstellen geht der Anbieter das Risiko ein, Kunden an Konkurrenten zu verlieren (die möglicherweise Geheimhaltung im Umgang mit Schwachstellen praktizieren).

VI. Zusammenfassung

Die Einteilung in system-, nutzungs- und nutzerbedingte ordnet Sicherheitslücken und Schwachstellen des Internets unter unterschiedlichen Gesichtspunkten. Die systembedingten Sicherheitslücken und Schwachstellen betonen den Beitrag der einzelnen Komponenten des Internets, die nutzungsbedingten Sicherheitslücken und Schwachstellen betonen die Auswirkungen der Anwendungsoptionen des Internets. Die nutzerbedingten befassen sich mit dem Rezipienten. Soweit individuelle Sicherheitslücken – etwa durch die Nachlässigkeit eines Mitarbeiters geschaffen werden – soll die Rolle des Nutzers bei der Verursachung von Sicherheitslücken nicht im Fokus der Frage nach den Informationsrechten und –pflichten stehen. Dem Faktor Mensch als nutzerbedingte Sicherheitslücke ist grundsätzlich eher durch präventive Information zu begegnen. Informationsrechte und –pflichten bedürfen eines Rezipienten, der selbst keine nutzerbedingte Sicherheitslücke ist, da dieser die Information andernfalls kaum als Basis für eigenverantwortliches Handeln wahrnimmt.

Für den weiteren Verlauf der Arbeit sind systembedingt Schwachstellen in der Adressierung (Szenario 3) und Sicherheitslücken in der Software (Szenario1) relevant. Szenario 2 und 4 thematisieren den Umgang mit Sicherheitslücken und Schwachstellen und sind mithin auf den nutzungsbedingten Aspekt fokussiert.

Hervorgehoben werden soll, dass die Vorstellung des Internets sich in jedem Fall von dem PC als Endgerät lösen muss. Die These der Konvergenz indiziert vielmehr, dass auch das Handy oder der Fernseher Ziel von Angriffen sein kann, und

sich damit in der Nutzung dieser Geräte die Gefahren von Sicherheitslücken und Schwachstellen realisieren können.

C Ergebnis

Soweit Sicherheit ex ante oder ex post durch gesetzliche Pflichten gewährleistet werden kann, werden diese in Kapitel 5 als Informationspflichten dargelegt. Im Ergebnis soll hier vielmehr die Kategorie der (Eigen)Verantwortung des Nutzers hervorgehoben werden.

Ob diese nun auf der Infrastrukturverantwortung des Staates beruht, eine bloße Appellfunktion besitzt oder als haftungsrelevante Verantwortung auszufüllen ist, ist in jedem Fall, die Notwendigkeit von Information für die Wahrnehmung von Eigenverantwortung zu betonen. Sicherlich kommt der Eigenverantwortung – soweit sie als Obliegenheit rechtlich zu berücksichtigen ist – gerade im Hinblick auf die Informationspflichten eine entscheidende Rolle zu.

Soweit Sicherheit durch technische und rechtliche Gegebenheiten und das ökonomisch Vernünftige konturiert ist, können diese Begrenzungen durch Information teilweise behoben werden. So kann der Kompromiss zwischen dem technisch Machbaren und ökonomisch Vernünftigen ex post durch Informationen über Sicherheitslücken kompensiert werden. Stets ist allerdings ex ante abzuschätzen, ob Information als Schutzmaßnahme wirkt oder eine weitere Sicherheitslücke darstellt. Diese Auswirkungen sind in den Überlegungen in Kapitel 5 bei der Bestimmung der Informationsrechte und –pflichten zu Grunde zu legen.

Die Arbeit ist auf Sicherheitslücken und Schwachstellen des IT-Systems fokussiert, die von einem entfernten Rechner über die Schnittstelle zum Internet, oder auch durch Viren ausgenutzt werden können. So kann ein Beitrag zur Eigenverantwortung des Nutzers und Basis für mögliche Reaktionen etwa die Konfiguration des Clients, der Firewall und der (techno)logischer Infrastruktur geleistet werden.

KAPITEL 3 SICHERHEIT UND INFORMATION

A Information und Geheimhaltung

I. Begriff: Information

Das Verständnis des Begriffes Information wurde und konnte bisher vorausgesetzt werden, da keine begriffliche Konkretisierung erforderlich war. Da im Folgenden „Information" ein zentraler Aspekt des Untersuchungsgegenstandes ist, soll eine Konkretisierung erfolgen, um die Vielfalt von Verständnismöglichkeiten einzugrenzen.[1] Nichts desto trotz soll zur Charakterisierung und Differenzierung eine Definition des Begriffes versucht werden. Hierbei kommt es auf die Herausarbeitung von erklärenden Elementen an.

1. Inhalte als „materielle Information"

Eine begriffliche Legaldefinition von Information findet sich etwa in den Informationsfreiheitsgesetzen.[2] Die eigentliche Aussage dieser Definitionen bezieht sich auf den verkörperbaren Charakter von Informationen. In der Definition den techni-

---

1 Vgl. Traumüller/Wimmer, Daten – Informationen – Wissen – Handeln, in: Reinermann (Hrsg.), Regieren und Verwalten im Informationszeitalter, 2000, S. 482 (482 f.); Gasser, Framing Information Quality Governance Research, in: Gasser (Hrsg.) Information Quality Regulation, 2004, S. 3 (5), *"With regard to law, it has been argued elsewhere that the legal system, generally speaking, has to ensure its permeability for different meanings of "information"*; Dreier, Informationsrecht in der Informationsgesellschaft, in: Bizer/Lutterbeck/Rieß (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft, 2002, S. 65 (68 f.), mit dem Ergebnis, dass es keines einheitlichen Informationsbegriffs bedürfe, da die Vielfalt unterschiedliche Blickwinkel ermögliche.

2 Sehr knapp etwa im Bundesinformationsfreiheitsgesetz, § 2 Nr. 1:
„Im Sinne dieses Gesetzes ist
1. amtliche Information: jede amtlichen Zwecken dienende Aufzeichnung, unabhängig von der Art ihrer Speicherung. (…)".
Informationsfreiheitsgesetze finden sich auf europäischer Ebene als Informationszugangsverordnung (Verordnung Nr. 1049/2001 vom 30.05.2001, ABl. Nr. L 145, vom 31.05.2001, S. 43) und in einzelnen Bundesländern (etwa Berlin, Brandenburg, Nordrhein-Westfalen, Schleswig-Holstein). Auf Bundesebene trat das Informationsfreiheitsgesetz nach einigen Anläufen im Gesetzgebungsverfahren am 01.01.2006 in Kraft. Sektorspezifisch gibt es das Umweltinformationsgesetz (UIG).

schen Aspekt betonend werden Informationen in § 3 Abs. 2 Umweltinformationsgesetz[3] als „Daten" wiedergegeben.

Eine Gleichsetzung von Information und Inhalt betont weniger den technischen als den funktionalen Sinn und Zweck der Verwendung von Information. Diese Gleichsetzung ist etwa einer Gesetzesänderung zum Teledienstegesetz zu entnehmen. In der ursprünglichen Fassung noch als „Inhalte" bezeichnet, wurde diese Formulierung in der Gesetzesänderung durch „Informationen" ersetzt.[4]

Festzuhalten ist, dass die wenigen Legaldefinitionen von Information aus technischer Sicht formuliert sind. Die begriffliche Konzentration auf Information als Inhalt soll jedoch weniger den technischen Datenverarbeitungsvorgang betonen als vielmehr ein weiteres Element der Information, den Informationsvorgang, materiell ergänzen.

2. Kommunikation als Informationsvorgang

Information als Inhalt kann als rein statisches Konzept Information nicht umfassend begrifflich wiedergeben. Information gewinnt erst durch die prozessorientierte Komponente des Informationsvorgangs Bedeutung für die Gesellschaft. Als Prozess ist der Informationsvorgang des „Informierens" und „sich Informierens" von der Kommunikation abzugrenzen[5] bzw. wird teilweise mit dieser gleichgesetzt.[6] Der

---

3 § 3 Abs. 2 UIG
„(2) Informationen über die Umwelt sind alle in Schrift, Bild oder auf sonstigen Informationsträgern vorliegenden Daten (…)".

4 § 5 Abs. 1 TDG in der ursprünglichen Fassung vom 22.07.1997: *„Diensteanbieter sind für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich."* Dieser wurde durch § 8 Abs. 1 TDG in der Fassung vom 14.12.2001 ersetzt: *„Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich."*

5 Kommunikation und Information stehen in einem engen Verhältnis zueinander, was eine Abgrenzung schwierig macht. Ein Versuch der Abgrenzung lohnt an dieser Stelle nur, wenn sie einen Erkenntnisgewinn für das Recht besitzt. Einen solchen Versuch hat etwa Druey unternommen, Druey, Information als Gegenstand des Rechts, 1995, S. 26 ff.: Information (statisch: Wissen und Inhalt) könne Resultat von Kommunikation (dynamischer Vorgang) sowie ein Element von Kommunikation sein. Die Spezifikation der Kommunikation sei der Mensch, der im Blickfeld der Kommunikation (am Anfang und Ende) steht und der der Information über die Kommunikation ein zusätzliches Inhaltselement gebe, einen Hinweis, wie Information zu verstehen sei. Damit könne das Verhältnis von Information und Kommunikation als Zweck-Mittel-Relation zur Normquelle werden.

6 Eine Gleichsetzung unternimmt Kloepfer, Informationsrecht, 2002, § 1 Rd. 60, der Kommunikation als intendierte Information begreift. Keine Kommunikation läge dann etwa bei dem für Dritte vernehmbaren Selbstgespräch vor.

Informationsvorgang selbst setzt ein Angebot des Informierenden und einen bestimmten oder bestimmbaren[7] Rezipienten voraus. Der Informationsvorgang ist dadurch regelmäßig durch ein Element der Differenz und der Motivation zum Ausgleich ungleicher Informationsverteilung der Beteiligten gekennzeichnet.

Diese wechselseitige Komponente der Kommunikation muss grundsätzlich realisiert werden, d. h. die Information als Inhalt beim Rezipienten ankommen. So bleibt etwa ein Aushang am schwarzen Brett lediglich ein Informationsangebot, wenn er nicht gelesen wird.

Entsprechend der technischen Sicht der Daten als Information kann Kommunikation als Vernetzung von Client und Server auch als Datenverarbeitungsvorgang bezeichnet werden. Bezogen auf die inhaltliche Komponente ist die Kommunikation allerdings auch ein Prozess, der wesensspezifisch dem Menschen zu Eigen ist.

3. Wissen als Informations(zu)stand

Für den Begriff Wissen findet sich keine Legaldefinition. Eine begriffliche Auseinandersetzung mit Wissen unternimmt jedoch Kloepfer, der ausführt,

> *„dass der Begriff der Information nicht identisch mit dem des Wissens ist. Informationsinhalte und Kommunikationsvorgänge sind Voraussetzungen für Wissen. Wissen ist eine organisierte und systematisierte Informationsmenge, welche Verstehens- und Interpretationsvorgänge erlaubt."*[8]

Aus diesem Verhältnis von Information und Wissen ergibt sich neben dem Inhalt und dem Vorgang ein drittes Element von Information, dem Wissen als „angehäufter" Informations(zu)stand. Das Wissen erlaubt Verknüpfungen von Informationen und gibt dem Informationsinhalt eine Chance auf, aber nicht zwangsläufig eine bestimmte Bedeutung (so kann zwischen nutzbarem und unnützem Wissen unterschieden werden).

Obwohl Information in der Regel auf die Veränderung des Informationszustandes zielt, ist diese nicht zwangsläufig eine notwendige und hinreichende Voraussetzung für die Vermehrung von Wissen. Notwendig ist Information nicht, wenn Wissen deduktiv aus erworbenem Wissen gebildet werden kann. Hinreichend ist sie nicht, wenn der Informationsvorgang Informationsinhalte überträgt, die bereits im Wissen des Rezipienten vorhanden sind.

---

7 Bestimmbar, im hier verstandenen Sinne sind auch Massen als Rezipienten.

8 Kloepfer, Informationsrecht, 2002, § 1 Rd. 60. In diesem Sinne werden der Interpretationsspielraum und der Bedeutungsgehalt von Wissen als Informationschance nur angedeutet.

Festzuhalten bleibt: Elemente von Information sind Inhalt, Vorgang (Kommunikation) und Zustand (Wissen).[9] Für den weiteren Verlauf der Arbeit soll darüber hinaus betont werden, dass der Informationsvorgang dem Ausgleich von ungleichen Informations(zu)ständen dient (Informationsasymmetrien).

II. Geheimhaltung

Geheimnis und Geheimhaltung sind im rechtlichen Kontext nicht unbedingt synonym zu verwenden. Im rechtlichen Kontext ist das Geheimnis von drei Elementen geprägt, Unbekanntheit, Geheimhaltungswille und –interesse.[10] Alle drei Elemente beziehen sich damit auf einen Informationsinhalt, der unbekannt bleiben soll. Das Schutzziel ist demnach der Informationsinhalt selbst.

Geheimhaltung ist als Nicht-Informierung grundsätzlich eine Begrenzung des Informationsvorgangs. Die rechtliche Begrenzung erfolgt unter Berücksichtigung von Interessen und sonstiger Schutzziele.

Zum einen ist derjenige zur Geheimhaltung berechtigt oder verpflichtet bzw. hat derjenige ein berechtigtes Interesse an Geheimhaltung, der Gründe für die Permanenz der Informationsasymmetrie hat. Rechtlich anerkannt ist etwa das Geheimhaltungsinteresse bei Betriebs- und Geschäftsgeheimnissen.

Zum anderen sind rechtliche Regelungen der Geheimhaltung dort zweckmäßig, wo der Informationsvorgang kontraproduktiv ist. Sei es, weil der Informationsinhalt sich „ungünstig" auf Rechtsgüter auswirken kann, sei es, weil eine Verminderung der Informationsasymmetrie aus anderen Gründen nicht gewollt ist.

Im technischen Kontext der Sicherheit entsprechen der Geheimhaltung die Anonymisierung (Schutz der Identität), die Verschlüsselung (Schutz des Inhaltes – Integrität), Passwörter (Zugangsschutz) oder eben die Geheimhaltung der Funktionsweise oder von Sicherheitslücken (*„security by obscurity"*[11]).

---

9 Im Ergebnis so auch Kloepfer, Informationsrecht, 2002, § 1 Rd. 56 ff., der diese Begriffe aus einer Arbeit von Druey gewonnen hat, Druey, Information als Gegenstand des Rechts, 1995. Weitere Definitionsansätze sind aufgenommen bei: Poledna, Staatliche Informationspflichten, in: Koller/Koller (Hrsg.), Recht und Rechtsdaten, S. 69 (69 ff.), http://www.-informatiquejuridique.ch/de/tagungsband_2003_de.html (30.05.2006).

10 Druey, Information als Gegenstand des Rechts, 1995, S. 256.

11 Vgl. etwa Schneier, Secrets & Lies, 2000, S. 371, mit einem Beitrag gegen *„security by obscurity"*.

1. Geheimhaltungspflichten

Geheimhaltungspflichten sind grundsätzlich durch ein Spannungsverhältnis zwischen dem Interesse an der Geheimhaltung und dem Interesse an der Aufhebung der Informationsasymmetrie gekennzeichnet. Pflichten zur Geheimhaltung können gesetzlich, durch Richterrecht oder vertraglich (bzw. vorvertraglich) begründet werden.

Pflichten zur Geheimhaltung lassen sich verschiedenen Normen entnehmen: Beteiligte an einem Verwaltungsverfahren haben etwa nach § 30 VwVfG einen Anspruch darauf, dass ihre

> *„zum persönlichen Lebensbereich gehörenden Geheimnisse sowie die Betriebs- und Geschäftsgeheimnisse, von der Behörde nicht unbefugt offenbart werden."*

§ 30 VwVfG versucht das Spannungsverhältnis zwischen einem effektiven und transparenten Verwaltungsverfahren und dem Geheimnisschutz zu lösen. Ein solches Spannungsverhältnis besteht auch im Gerichtsverfahren (Rechtsschutz kontra Geheimhaltung). Lösungen gibt es einerseits zugunsten der Geheimhaltung bei Zeugnisverweigerungsrechte[12], andererseits zugunsten des Rechtsschutzes bei Auskunftsrechten[13] oder Erklärungspflichten[14].

Soweit personenbezogene Daten betroffen sind, ist zusätzlich das „Datengeheimnis" nach § 5 BDSG zu beachten. Damit ist es Personen, die mit der Datenverarbeitung beschäftigt sind, untersagt, unbefugt personenbezogene Daten zu verarbeiten oder zu nutzen. Dieses Datengeheimnis besteht auch bei Beendigung der Tätigkeit fort, § 5 S. 3 BDSG.

Ein prominentes Beispiel einer durch Richterrecht begründeten Pflicht zur Geheimhaltung lässt sich dem Arbeitsrecht entnehmen. Eine allgemeine Geheimhaltungspflicht (inklusive Betriebs- und Geschäftsgeheimnissen) von Arbeitnehmern kann sich unmittelbar aus dem Arbeitsvertrag, als vertragsimmanente Pflicht zur Rücksichtnahme auf geschäftliche Interessen des Arbeitgebers, §§ 241 Abs. 2 und

---

12 §§ 383 Abs. 1 Nr. 6, 384 Nr. 3 ZPO; § 55 Abs. 1 StPO i.V.m. § 17 UWG oder § 404 AktG.

13 BGH, Urteil v. 16. 4. 2002 - X ZR 127/99, GRUR 2002, 801 (803) zur Abwägung bei dem Auskunftsanspruch eines Arbeitnehmers gegen den Konzern; Ahrens, Zur Aufklärungspflicht der nicht beweisbelasteten Partei, in: ZZP 96 (1983), 1 (14 f.) der den grundsätzlich weiten Inhalt bei der Aufklärungspflicht bei Unternehmensgeheimnissen einschränken will.

14 § 138 Abs. 2 ZPO.

242 BGB, ergeben.[15] Aufgrund „nachwirkender Treuepflichten" kann der Arbeitnehmer – auch ohne ausdrückliche vertragliche Vereinbarung – nach dem Ausscheiden aus dem Betrieb zur Geheimhaltung verpflichtet sein.[16] Eine Grenze der nachwirkenden Geheimhaltungspflicht ist die Beeinträchtigung der freien Entwicklung des Arbeitnehmers, d. h. die Abwägung mit den Interessen des Arbeitnehmers an seinem beruflichen Fortkommen (Art. 12 GG).[17] Betriebs- und Geschäftsgeheimnisse sind regelmäßig nicht als Informationsinhalt absolut, d. h. gegen schlechthin jede Offenbarung und Benutzung, geschützt. Sollte ein Dritter den Inhalt des Betriebs- und Geschäftsgeheimnisses aus eigener Leistung erlangt haben, so kann eine Offenlegung grundsätzlich nicht verboten werden.[18] Soweit die eigene Leistung allerdings in einem unbefugten Ausspähen des Betriebs- und Geschäftsgeheimnisses besteht, ist an einen Unterlassungsanspruch nach § 1004 BGB sowie an strafrechtliche Sanktionen nach § 202a StGB und § 17 Abs. 2 Nr. 1 lit. a) UWG zu denken.[19]

Im Folgenden soll das Spannungsverhältnis zwischen Informationsasymmetrie und dem, Interesse an Geheimhaltung exemplarisch mit Entscheidungen zur Beweisführung bei Geheimnissen (kryptographische Verfahren) bei der Nutzung von Geldautomaten dargelegt werden.

---

15 Vgl. in der Rechtsprechung statt vieler eine Entscheidung des BAG, Urteil v. 3.7.2003 - 2 AZR 235/02, NZA 2004, 427 (429); in der Literatur etwa: Richters/Wodtke, Schutz von Betriebsgeheimnissen aus Unternehmersicht, in: NZA-RR 2003, 281 (282f.); Palandt, 65. Aufl. 2006, § 611 Rd. 41.

16 BAG, Urteil v. 16.03.1982 - 3 AZR 83/79, NJW 1983, 134 (135); BAG, Urteil v. 15.12.1987 - 3 AZR 474/86, NJW 1988, 1686 (1687); für die Literatur, vgl. Wertheimer, Bezahlte Karenz, in BB 1999, 1600 (1603), der die nachwirkende Verschwiegenheitspflicht auf besonders treuwidriges Verhalten beschränken will. Teilweise soll die Verschwiegenheitspflicht mit dem Ausscheiden enden: BAG, Urteil v. 19. 5. 1998 - 9 AZR 394/97, NZA 1999, 200.

17 BGH, Urteil v. 3.5.2001 - I ZR 153/99, GRUR 2002, 91 (93); Richters/Wodtke, a.a.O., (Fn. 15), 281 (286). In diesem Fall überwiege das Recht des Arbeitnehmers - aus Art. 12 Abs. 1 GG - den Anspruch des Arbeitgebers auf dessen geschäftliche Interessen Rücksicht zu nehmen.

18 Wolff, Der verfassungsrechtliche Schutz der Betriebs- und Geschäftsgeheimnisse, in: NJW 1997, 98 (99 f.).

19 Ob im Einzellfall tatsächlich eine Strafbarkeit Dritter beim unbefugten sich Verschaffen vorliegt, ist zu prüfen. § 17 Abs. 2 Nr. 1 lit. a) UWG schränkt das unbefugte Sich-Veschaffen auf Fälle des Eigennutzes zugunsten eines Dritten oder der Absicht, dem Unternehmen zu schaden, ein. Ob diese Motivationen bei der Offenbarung von Sicherheitslücken ausschlaggebend sind oder mitschwingen, ist wohl im Einzelfall (Eigennutz: Ehre des Crackers?; Schadensabsicht: Offenbarung von Sicherheitslücken lediglich bestimmter Unternehmen?) zu prüfen. Tatsächlich ist jedoch die Zahl der Fälle einer Strafverfolgung eher gering. Als Gründe werden die Angst vor Rufschädigung und der Zwang zu bzw. die Notwendigkeit zur Offenbarung während des Strafverfahrens genannt, Fezer/Rengier UWG § 17 Rd. 5 und 84.

2. Geheimhaltung im Gerichtsprozess

a) Entscheidung zum „ec-Karten Missbrauch" I

Das Spannungsverhältnis von Geheimnisschutz und effektiven Rechtsschutz wird in seiner Bedeutung für die IT-Sicherheit in einer aktuellen Entscheidung des BGH aufgegriffen. In der Sache geht es um die Frage, ob der Kunde oder die Bank das Risiko der unbefugten Nutzung einer ec-Karte und der PIN an einem Geldautomaten trägt. Im Prozess spiegelt sich diese Frage an der Verteilung der Beweislast wieder. In einer Entscheidung zum ec-Karten-Missbrauch deutet der BGH an, dass eine Bank als Partei in einem Prozess verpflichtet sein könnte

> *„sich im Rahmen der ihr nach § 138 Abs. 2 ZPO obliegenden Erklärungspflicht zu den Behauptungen der beweispflichtigen Partei konkret zu äußern, wenn diese außerhalb des von ihr vorzutragenden Geschehensablaufs steht und keine nähere Kenntnis der maßgebenden Tatsachen besitzt (…).*"[20]

Dies gelte auch

> *„hinsichtlich der von ihm im – Rahmen des Zumutbaren und gegebenenfalls in verallgemeinernder Weise – darzulegenden Sicherheitsvorkehrungen."*[21]

Die Sicherheitsvorkehrungen wären hier zugunsten der Beweisführung der Gegenpartei offen zu legen, eine weitere – wohl differenziert zu betrachtende – Konstellation ist die Offenlegung für die eigene Beweisführung.[22] Mangels ausreichender substantiierter Darlegung hat der BGB die Beweisführung allerdings abgewiesen.[23]

Sollte eine solche Erklärungspflicht bestehen, scheint die betroffene Partei vor die Wahl gestellt, die Geheimhaltung bezüglich ihrer IT-Sicherheitsvorkehrungen auf-

---

[20] BGH, Entscheidung v. 05.10.2004 - XI ZR 210/03, NJW 2004, 3623 (3625). Grundlegend zur Frage des Missbrauchs von ec- und Kreditkarten: Lochter/Schindler, Missbrauch von PIN-gestützten Transaktionen, in: MMR 2006, 292 ff.

[21] BGH, Entscheidung v. 05.10.2004 - XI ZR 210/03, NJW 2004, 3623 (3625); zum Verhältnis von Geheimhaltungsinteressen bei technischen Vorrichtungen und dem Berichtungsanspruch bei Urheberrechtsverletzungen: BGH, Entscheidung v. 02.05.2002 - I ZR 45/01, NJW-RR 2002, 1617 (1619).

[22] Stadler, Der Schutz des Unternehmensgeheimnisses im Zivilprozess, in: NJW 1989, 1202 (1202).

[23] In der Entscheidung des BGH, Entscheidung v. 05.10.2004 - XI ZR 210/03, NJW 2004, 3623 (3625) las sich dies so: *„Diese hat lediglich unter Sachverständigenbeweis gestellt, daß die Maßnahmen in Bankrechenzentren und Bankverlagen zum Schutz der Software, zur Geheimhaltung der Institutsschlüssel und zur Vermeidung anderer interner Angriffe auf das PIN-System nicht ausreichend seien, um erfolgreiche Angriffe auszuschließen. Daß derartige - von der Klägerin damit nicht substantiiert behauptete - Sicherheits- und Softwaremängel als Ursachen für die Möglichkeit eines Mißbrauchs einer gestohlenen ec-Karte theoretisch in Betracht kommen, ergab sich aber bereits aus dem vom Berufungsgericht eingeholten Sachverständigengutachten."*

zugeben oder den Prozess zu verlieren. Diesem Dilemma kann man sich über das Prozessrecht annähern.

Die Geheimhaltung kann sich auf die Gegenpartei und/oder auf die Öffentlichkeit beziehen. Im Fall des wirtschaftlichen Konkurrenten bezieht sich das Geheimhaltungsinteresse in der Regel gleichmäßig auf beide.

Der Ausschluss der Öffentlichkeit nach § 172 Nr. 2 GVG bzw. die Verpflichtung zur Geheimhaltung über § 174 Abs. 3 GVG reichen in diesem Fall nicht aus, um dem Interesse an Geheimhaltung gerecht zu werden, da der Grundsatz der Parteiöffentlichkeit einer absoluten Geheimhaltung entgegensteht, § 357 Abs. 1 ZPO.

Lösungen über ein in-camera Verfahren analog § 99 Abs. 2 VwGO, in dem nur das Gericht Einsicht in bestimmte Akten erhält, sind wegen eines Verstoßes gegen das rechtliche Gehör nach Art. 103 Abs. 1 GG nicht rechtmäßig und zudem nicht für alle Entscheidungskonstellationen zweckmäßig. Ein substantiiertes Bestreiten wäre zumindest nicht möglich. Liegen die Dinge wie bei der ec-Karten Entscheidung des BGH und geht es um eine Darlegung der Partei selbst, ist eine Lösung entsprechend § 99 Abs. 2 VwGO nicht weiterführend. Als Ultima Ratio wird deshalb die Einführung eines Geheimverfahrens unter temporärem Ausschluss der Gegenpartei vorgeschlagen,[24] wobei hier ebenfalls Art. 103 Abs. 1 GG entgegenstehen dürfte.

Das Geheimhaltungsinteresse vor der Gegenpartei begründet grundsätzlich eine Interessenabwägung zwischen diesem und dem in Art. 19 Abs. 4 GG verankertem effektiven Rechtsschutz und dem Gebot des rechtlichen Gehörs. Eine vermittelnde Variante will deshalb die Geheimnisse nur den Anwälten der Parteien offenbaren (Anwaltslösung).[25] Mit dem Einsatz des Anwalts soll ein Verstoß gegen Art. 103 Abs. 1 GG als verhältnismäßig gerechtfertigt sein.[26]

---

[24] Stadler, Der Schutz des Unternehmensgeheimnisses im Zivilprozess, in: NJW 1989, 1202 (1203 ff.). Auf Verfassungsebene im Fall des Ausschlusses der beweisbelasteten Partei (etwa in der Konstellation des § 138 Abs. 2 ZPO) sei eine Güterabwägung zwischen Art. 103 Abs. 1 GG mit Art. 14 Abs. 1 GG zu treffen. Beim Ausschluss der nicht beweisbelasteten Partei bleibe es regelmäßig bei der Wahl zwischen Rechtsdurchsetzung und Geheimhaltung.

[25] Hausberg, Der Schutz von Betriebs- und Geschäftsgeheimnissen, 2004, S. 124 ff.; zur Anwaltslösung im US-amerikanischen Recht: Pagenberg, Betrieblicher Know-How-Schutz, in: CR 1991, 65 (69 f.). Grundsätzlich spricht gegen eine solche Anwaltslösung, dass der Anwalt lediglich Interessenvertreter seiner Mandanten ist. Er kann jedoch keine Interessen vertreten, wenn er sich mit seinen Mandanten über bestimmte Punkte nicht absprechen kann.

[26] Stadler, a.a.O., (Fn. 24), 1202 (1204); a. A. das BVerwG in einer neueren Entscheidung die stetige Rechtsprechung bestätigend: Die Verwertung eines Sachverständigengutachtens, das auf Unterlagen beruht, die nur einer Partei bekannt sind, verstoße gegen das rechtliche Ge-

Im Fall von ec-Karten gilt es wohl regelmäßig, die Sicherheitsvorkehrungen vor der Öffentlichkeit und nicht primär vor der konkreten Partei zu schützen. In diesem Fall könnte ein Schutz von IT-Sicherheitsvorkehrungen als Betriebs- oder Geschäftsgeheimnis über den Ausschluss der Öffentlichkeit nach § 172 Nr. 2 GVG ausreichend sein.[27] In jedem Fall können die in der nicht öffentlichen Sitzung anwesenden Personen über § 174 Abs. 3 GVG – strafbewehrt über § 353d Nr. 1, 2 StGB – zur Geheimhaltung verpflichtet werden.

Allerdings erscheint es tatsächlich unwahrscheinlich, dass sich ein Kreditinstitut auf ein wie auch immer geartetes Geheimverfahren einlassen wird, da im Fall der Entscheidung zugunsten des Kunden mit weiteren Klagen zu rechnen sein kann. Nichts desto trotz gibt es Fälle, in denen prozessual zu Geheimhaltung verpflichtet wird.

b) Entscheidung zum „ec-Karten Missbrauch" II

Der Prozess „Diners Club SA (PTY) LTD v. A. & V. Singh" vor dem High Court of South Africa (Durban and Coast Local Division) soll nur im Tatsächlichen dargestellt und kann rechtlich nicht abschließend bewertet werden.

In der Sache[28] geht es wie in der Entscheidung des BGH darum, wer – das Kreditinstitut oder der Kunde – finanziell den Missbrauch der Karte und der PIN zu vertreten hat. Während eines Aufenthalts des Kunden in Südafrika sollten in London mit der Karte in 190 Fällen Abbuchungen vom Konto des Kunden in einer Gesamthöhe von $ 80.000 getätigt worden sein. Das Kreditinstitut vertrat den Standpunkt, dass das Verfahren der Abbuchungen von Geldautomaten sicher sei – es müsse demnach ein (vom Kunden ermöglichter) Missbrauch der Karte und der PIN vorliegen. Der Kunde verneinte eigene Transaktionen oder fahrlässige Ermöglichung des Missbrauchs. Soweit liegt der Fall parallel zur Entscheidung des BGH.

---

hör, BVerwG, Beschluss v. 15.08.2003 – 20 F 8/03, http://www.bundesverwaltungsgericht.de/ (30.05.2006).

27 In den nächsten „Phasen" des Prozesses erfolgt der Schutz bei der grundsätzlich öffentlichen Urteilsverkündung nach § 172 Abs. 1 GVG über eine Ausnahme nach § 173 Abs. 2 GVG.

28 Informationen zu dem Fall: unter Punkt "Robustness of cryptographic protocols": http://www.cl.cam.ac.uk/users/rja14/ (30.05.2006); http://cryptome.org/citi-ban.htm (30.05.2006); in der Presse: News.Com vom 21.02.2003, McCallagh, Declan, Crypto research under fire in U.K. suit, http://news.com.com/2100-1023-985545.html (30.05.2006); ZDNet UK vom 21.02.2003, Loney, Matt, Banks seeking to gag crypto research, http://news.zdnet.co.uk/business/0,39020645,2130897,00.htm (30.05.2006).

Jedoch geht der Prozess mit der Beweisführung weiter, die der BGH im letzten Abschnitt grundsätzlich für möglich gehalten – mangels ausreichend substantiierter Darlegung des Kunden im konkreten Fall allerdings abgewiesen – hat.

Die Kunden wollten ihren Standpunkt mit Hilfe von Wissenschaftlern der Cambridge University vertreten, die veröffentlichten, Sicherheitslücken im kryptographischen Verfahren der Transaktion entdeckt zu haben. Konkret ging es bei diesem Prozess um den Nachweis, dass das kryptographische Verfahren zum Schutz der PIN von Geldkarten bei Geldautomaten – ATM (Automated Teller Machines)-Transaktionen – nicht ausreichen sollte.[29] Die Sicherheitslücken liefen letztendlich darauf hinaus, dass „Bank-Insider" leicht die PIN jedes Kunden in Erfahrung bringen konnten.

Im Laufe des Prozesses wurde die Vernehmung der Zeugen (Mitarbeiter des Kreditinstituts) und der Sachverständigen verfügt.[30] Zum Schutze des Kreditinstituts hat das Gericht in die Verfügung den Ausschluss der Öffentlichkeit, die inhaltliche Beschränkung der Beweisaufnahme und eine Geheimhaltungsverpflichtung aufgenommen: Die Mitarbeiter des Kreditinstituts wurden mit dieser Verfügung verpflichtet, keine Aussagen über Details über IT-Standards oder –Strategien, den physikalischen Ort des Sicherheitssystems, die Softwarearchitektur und die Art und Weise, wie das System angegriffen, missbraucht, umgangen oder sonst sich unberechtigter Zugang verschafft werden könnte, zu treffen.

Die Geheimhaltungsverpflichtung war gerichtet an die Parteien, ihre rechtliche Vertretung, die Sachverständigen und bezog sich sachlich auf die Geheimhaltung aller Informationen während der Vernehmung. Hiernach mussten die Mitarbeiter der Universität Cambridge ihre – bereits erfolgten[31] – Publikationen über die Sicherheitslücken einstellen.

---

29 Die Beschreibung einiger technischer Details findet sich in der eidesstattlichen Versicherung von Anderson vom November 2002, http://cryptome.org/gag/rja-affidavit.pdf (30.05.2006).

30 Da der Prozess selbst in Südafrika (High Court of South Africa (Durban and Coast Local Division)) stattfand, sollten einige Zeugen, unter anderem auch die Sachverständigen der Universität Cambridge, stellvertretend vor dem Royal Courts of Justice in London vernommen werden. Mittels einer Verfügung wurde eine Zeugenvernehmung vor Ort (London) und die sachliche und inhaltliche Beschränkung auf bestimmte Fragen angeordnet, http://cryptome.org/gag/gagging-order-X.pdf (30.05.2006).

31 Nach eigenen Angaben wurde der technische Report über 110,000 Mal über das Internet abgerufen. Die Publikation bis zum Termin der Vernehmung wurde nach der Ladung zur Zeugenvernehmung „erzwungen" und forciert, vgl. Anderson, Open and Closed Systems are Equivalent, 2003, http://www.cl.cam.ac.uk/ftp/users/rja14/toulousebook.pdf (30.05.2006).

Dieser Prozess offenbart einen zentralen Konflikt der Geheimhaltung. Selbst die „letztmöglichen Maßnahmen" des Rechtsstaats zum Schutz der Geheimhaltung sind in ihrer Wirksamkeit beschränkt. Soweit der Wille zur Veröffentlichung besteht, findet sich auch ein Weg. Sei es durch eine (unkontrollierbare) Vorabveröffentlichung im Internet oder (soweit rechtlich möglich[32]) durch Abstandnahme von einer Prozessbeteiligung als Gutachter.

B Technische Bewertung von Information zur Erhöhung der Sicherheit

Zunächst soll eine notwendige technische Betrachtung der Erforderlichkeit und Nützlichkeit der Offenbarung von Sicherheitslücken und Schwachstellen im IT-System vorangestellt werden, die als Basis für die rechtliche Beurteilung der Pflichten dienen soll. Die zunächst dargestellte Debatte um „Full-Disclosure" und „Nondisclosure" (1) berücksichtigt die Nützlichkeit der Offenbarung. Die anschließend vorgestellten „Guidelines for Security Vulnerability Reporting and Response" (2) und der Vorschlag für eine RFC (3) stellen Beispiele für die Regelung des Verfahrens der Offenbarung von Sicherheitslücken dar.

(1) Das Meinungsspektrum[33] reicht von Vertretern einer „*Nondisclosure*", die einer Veröffentlichung von Sicherheitslücken negative Auswirkungen auf die Sicherheit bescheinigen, bis zu Vertretern einer *„Full-Disclosure"*, die die sofortige und vollständige Information für die Öffentlichkeit fordern. Pointiert dargestellt: Für eine Nondisclosure wird angeführt, dass Sicherheit nur durch Geheimhaltung bis zur Schließung der Lücke garantiert werden kann (*„security by obscurity"*[34]). Dagegen spricht, dass die Geheimhaltung ein Gefühl der Sicherheit vermittelt, faktisch aber keineswegs sicher ist, da nie klar ist, wer bereits Kenntnis von der Sicherheitslücke hat (im Folgenden als sichere Unsicherheit bezeichnet). Eine Full-Disclosure dagegen zwingt Hersteller ein zeitnahes Patch herauszugeben und die Lücke zu schließen und gibt Administratoren das nötige Wissen, um reagieren zu können. Aller-

---

32 Soweit man als Zeuge geladen oder zum Sachverständigen ernannt ist, ist ein Abstandnehmen von der „Funktion" als Beweismittel nur in gesetzlichen Grenzen erlaubt. Vgl. §§ 51, 77 StPO; §§ 380 f., 407 ZPO.

33 Eine ausführliche Gegenüberstellung findet sich etwa bei Shephard, Stephen. A., Vulnerability Disclosure, http://www.giac.org/certified_professionals/practicals/gsec/2541.php (30.05.2006). Der Aspekt und die Relevanz des Verkehrsschutzes werden im weiteren Verlauf der Arbeit behandelt werden.

34 Schneier, Secrety & Lies, 2000, S. 371, mit einem Beitrag gegen *„security by obscurity"*.

dings werden auch Script Kiddies und Cracker[35] mit dem erforderlichen Wissen ausgestattet, um Dritten Schaden zufügen zu können.

Es scheint sich ein Mittelweg herausgebildet zu haben, der der – für die rechtliche Bewertung der Informationspflichten erforderlichen – Abschätzung der Gefahren durch veröffentlichte Sicherheitslücken zu Grunde gelegt werden kann.

Die Diskussion um *„Full-Disclosure"* oder *„Nondisclosure"* von Sicherheitslücken kann zugunsten einer *„unpredictable Full-Disclosure"*[36] entschieden werden. Das heißt, Informationen über Sicherheitslücken sind so zu veröffentlichen, dass sie für mögliche Cracker und Script Kiddies nicht ausnutzbar, sondern eben unberechenbar sind. Ziel sollte sein, durch die Veröffentlichung der Sicherheitslücke dem Nutzer Informationen für ein verantwortungsvolles Handeln zu geben. Hierbei müssen nicht zwingend technischen Details veröffentlicht werden, die der gemeine Nutzer nicht einzuordnen vermag. Der Nutzer sollte entscheiden können, ob er das Programm weiter nutzt, deinstalliert oder Schutzmaßnahmen installiert.

Andere Varianten der unberechenbaren Offenbarung zielen auf eine personell und inhaltlich eingeschränkte Offenbarung (*„limited disclosure"*[37]). Bei der „*responsible disclosure"*[38] wird ein 30-Tage-Zeitraum zur Geheimhaltung und Schließung der Lücke vorgesehen, in dem nur der Hersteller informiert wird.

Ohne die Debatte und den Nutzen von (Full-)Disclosure bzw. Nondisclosure für die Sicherheit technisch abschließend beurteilen zu können, können zwei Aspekte genannt werden, die bei der Beurteilung den Ausschlag für eine Pflicht des Herstellers zu informieren (disclosure) geben können. Zum einen besteht erst durch die Pflicht zu informieren ein Anreiz, Maßnahmen gegen Sicherheitslücken zu ergrei-

---

35 Die folgenden Begriffserklärungen sind http://www.bsi-fuer-buerger.de/abzocker/-05_03.htm (30.05.2006) entnommen: Script Kiddies (zumeist Jugendliche) sind diejenigen, die ohne wirkliches Expertenwissen mit vorgefundenen Programmen und Anleitungen in ein fremdes IT-System eindringen. Sie stehen im Ruf ziellos nach Schwächen zu suchen und diese dann auszunutzen. Da sie kein Verständnis davon haben sollen, was sie tun, gelten sie als besonders gefährlich. Cracker sind diejenigen, die mit Expertenwissen in ein fremdes IT-System eindringen, aber Schaden verursachen. Sie nutzen, verändern oder löschen vorhandene Daten.

36 Schneier, Secrety & Lies, 2000, S. 371.

37 Howard, John D., An Analysis Of Security Incidents On The Internet 1989 – 1995, 1997, http://www.cert.org/research/JHThesis/Start.html (30.05.2006).

38 Shephard, a.a.O., (Fn. 33), S. 8 f. Ein bestimmter Zeitraum der Geheimhaltung bis zur Veröffentlichungspflicht kann auch in Sicherheitspolicies empfohlen werden, CERT/CC Vulnerability Disclosure Policy (45 Tage), http://www.cert.org/kb/vul_disclosure.html (30.05.2006); Ntbugtraq Disclosure Policy (30 Tage), http://www.ntbugtraq.com/-default.aspx?sid=1&pid=47&aid=50 (30.05.2006).

fen.[39] Zum anderen ermöglicht nur eine Offenbarung dem Nutzer eine eigenverantwortliche Entscheidung über die (Weiter)Nutzung der Software.

(2) Mit den „Guidelines for Security Vulnerability Reporting and Response" hat die „Organization for Internet Safety" (OIS)[40] Sicherheitsrichtlinien veröffentlicht, die als entsprechende Empfehlungen für den Umgang mit der Offenbarung von Sicherheitslücken herausgegeben wurden.[41] Diese „Guidelines for Security Vulnerability Reporting and Response" werden im Folgenden als Draft bezeichnet. Für die Konturierung der Informationspflicht soll ein Überblick über den technischen Ablauf der Veröffentlichung exemplarisch mit diesem Draft der OIS gegeben werden.

Der Draft sieht ein mehrphasiges Verfahren bis zur Veröffentlichung vor, an dem neben dem Entdecker der Lücke und dem Hersteller auch ein Koordinator und Schlichter beteiligt sein kann (2.1 des Draftes). Allerdings ist einer Veröffentlichung ein langer Prozess vorgeschaltet, der einen unbestimmten Zeitrahmen für die Erforschung der Sicherheitslücke und Entwicklung von Gegenmaßnahmen vorsieht (2.3 des Draftes). Der üblicherweise in anderen Sicherheitsrichtlinien und Policies empfohlene Zeitrahmen von 30 Tagen bezieht sich in diesem Konzept auf die Zeit für die Veröffentlichung detaillierter Informationen nach der grundsätzlichen Offenbarung der Sicherheitslücke und des Patches (8.6 des Draftes). In der „Discovery" Phase wird die Sicherheitslücke entdeckt. Der „Finder" soll in einem „Vulnerability Summary Report" (VSR) u. a. einen reproduzierbaren Beweis der Sicherheitslücke darlegen. In der nächsten Phase, der „Notification", bestätigt der Hersteller des unsicheren Produkts den Eingang des Reports innerhalb von sieben Tagen (5). Soweit der Finder eine weitere Zusammenarbeit nicht ausschließt, soll die Kommunikation zwischen ihm und dem Hersteller grundsätzlich verschlüsselt erfolgen (2.4 des Draftes). Die nächste Phase („Investigation") gilt der Erforschung der Sicherheitslücke durch den Hersteller, deren Ergebnis er dem Finder mitzuteilen hat (6.5 des Draftes). Anschließend soll der Hersteller entsprechende Abhilfemaßnahmen entwickeln („Resolution"). In der Phase des „Release" soll schließlich über die Sicherheitslücke informiert und die Abhilfemaßnahme zur Verfügung gestellt wer-

---

39 Anderson, Open and Closed Systems are Equivalent (that is, in an ideal world), 2003, S. 10, http://www.cl.cam.ac.uk/ftp/users/rja14/toulousebook.pdf (30.05.2006).

40 Ein freiwilliger Zusammenschluss von Unternehmen, die die Zusammenarbeit zwischen Forschern und Herstellern zur Schließung von Sicherheitslücken erleichtern will, http://-www.oisafety.org/about.html (30.05.2006).

41 Guidelines for Security Vulnerability Reporting and Response Version 2.0, 01.09.2004 (Version 1.0., vom 28.07.2003 wurde nach der „public comment period" abgelehnt), http://-www.oisafety.com/guidelines/secresp.html (30.05.2006).

den. Der Hersteller soll diese Informationen für die Allgemeinheit einfach zugänglich und auffindbar bereitstellen. Zusätzlich kann der Finder die Informationen in entsprechenden Mailinglisten oder Ähnlichem veröffentlichen.

Das Verfahren belässt grundsätzlich die Entscheidung der Veröffentlichung bei dem Hersteller, ein davon unabhängiges Recht des Finders über die Veröffentlichung zu entscheiden, insbesondere bei Untätigkeit des Herstellers, sieht es nicht vor.

(3) In der Vergangenheit gab es Versuche, Informationspflichten über Sicherheitslücken in einem RFC zu regeln. Der Entwurf sieht einen abgestuften Informationsvorgang vor. Der Draft zur *„Responsible Vulnerability Disclosure Process"* wurde jedoch nicht als Standard veröffentlicht, da er menschliche und keine technischen Verhaltensweisen standardisiere,[42] und somit keine technisch fundierte Möglichkeit der Konkretisierung und Normierung rechtlicher Pflichten vorgeben könne.

Für die rechtliche Beurteilung kann demnach vorausgesetzt werden, dass, soweit eine Informationspflicht in Betracht kommt, eine differenzierte prozessorientierte Betrachtung und Gestaltung dieser Informationspflicht einer kategorischen Bejahung oder Verneinung vorzuziehen ist. Zudem können weitere differenzierende Aspekte wie möglicher Schadensumfang oder die Vorteilsziehung des Herstellers zur Konturierung der Informationspflicht beitragen.[43]

C Personelle Bewertung der Information zur Erhöhung der Sicherheit

Das Wissen um die Sicherheit und um die Sicherheitslücken – mithin der Informations(zu)stand – ist notwendigerweise Ausgangpunkt und beabsichtigtes Ziel der Information über IT-Sicherheitslücken. Mit der These *„je informationsbewusster die Parteien sind, desto geringer sind die implizierten Informationsansprüche"*[44], kann der Wissenstand des Nutzers zu der Pflicht oder dem Recht sich zu informieren (bzw. der Pflicht des Anbieters zu informieren) in eine rechtlich relevante Relation gesetzt werden.

---

42 Wie aus mehreren Quellen zu entnehmen ist, soll die IEFT die Verabschiedung eines solchen RFC nicht als ihre Aufgabe sehen, da sie nicht menschliche Verhaltensweisen, sondern Prozesse in der Technik standardisiere, http://www.oisafety.com/about.html (30.05.2006); heise news vom 19.03.2002, http://www.heise.de/newsticker/meldung/25866 (30.05.2006).

43 Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3147.).

44 Druey, Information als Gegenstand des Rechts, 1995, S. 343.

Deshalb soll im Folgenden dargestellt werden, welcher Wissensstand im Hinblick auf die Sicherheit vom Nutzer und Anbieter gefordert bzw. ihm unterstellt und welche Informationshandlungen von ihm gefordert werden können. Das Sicherheitsbewusstsein des Nutzers ist ein Indikator dafür, welchen Wissensstand der Nutzer selbst für erforderlich hält bzw. welcher ihm realistischerweise unterstellt werden kann.

Die Sicherheitserwartung des Nutzers kann Einfluss auf die Informationspflichten des Herstellers oder Anbieters haben. Im Einzelfall hängt es von dem Sicherheitsbewusstsein des Nutzers ab, ob Informationspflichten tatsächlich Einfluss auf die Sicherheit der Nutzung des Internets haben. Ohne Sicherheitsbewusstsein wird der Nutzer die Informationen kaum wahrnehmen und vor allem kaum umsetzen.

Als These soll formuliert werden: Je mehr durch Information Einfluss auf das Sicherheitsbewusstsein genommen wird, desto mehr muss Sicherheit in Eigenverantwortung geleistet werden und desto höher sind aber auch die Sicherheitserwartungen, die an ein sicheres Internet gestellt werden können. Je höher die Sicherheitserwartungen sind, desto eher kann etwa eine Verkehrssicherungspflicht und damit eine Haftung von Hersteller und Anbieter begründet werden.[45] Abzustellen ist hierbei grundsätzlich nicht auf den Einzelnen, sondern auf einen potenziellen Durchschnittsnutzer.

I. Sicherheitsbewusstsein und -erwartung

Das Sicherheitsbewusstsein des durchschnittlichen Nutzers reicht von Interesse bis hin zu Gleichgültigkeit und Resignation (Software ist eben nicht sicher).[46] Grundsätzlich wird dem Nutzer – zumindest noch im Jahre 1995 – in der Literatur kein wirkliches Sicherheitsbewusstsein attestiert. Das Bewusstsein sei entsprechend der Verantwortungsteilung von Herstellern und Entwicklern, Administratoren und

---

45 Eingehend dazu unter Kapitel 5 C II. und III.

46 Vgl. KES und KPMG Sicherheitsstudie 2002, http://www.kes.info/archiv/material/-studie2002/ (30.05.2006) nach dieser Studie gaben 65% der Befragten an, das fehlende Bewusstsein der Mitarbeiter behindere die Verbesserung der Informationssicherheit, 61% nannten das fehlende Bewusstsein im mittleren Management. 30% der Beeinträchtigungen für die IT-Sicherheit gingen nach dieser Studie von Irrtum und Nachlässigkeit eigener Mitarbeiter (25% von Malware) aus. 2004 gaben nur noch 51% an, das fehlende Bewusstsein bei den Mitarbeitern (45% bei Top-Management und 42% im mittleren Management) sei ein Hindernis für die Informationssicherheit. Rang 1 übernahm das mit 62% das fehlende Geld, KES und Microsoft Sicherheitsstudie 2004, S. 6, http://www.kes.info/archiv/material/-studie2004/kes-Microsoft-Studie2004-Sonderdruck.pdf (30.05.2006).

Nutzern auf ein minimales Niveau reduziert.[47] Zunehmend rückt jedoch das Bedürfnis nach einer *„security awareness"*[48] der Nutzer in den Vordergrund. Die Bedeutung des Sicherheitsbewusstseins des Nutzers wird auch im Bereich der technischen Normung nicht unterschätzt. So fordern auch internationale Standards wie die ISO/IEC 17799 die Förderung des Sicherheitsbewusstseins.[49]

Im Rahmen dieser Arbeit kann demnach festgehalten werden, dass der Nutzer für das Thema IT-Sicherheit (noch) nicht genügend sensibilisiert und daher zu sensibilisieren ist.

Die erforderliche Sensibilisierung soll durch Programme auf unterschiedlichen Ebenen erfolgen. Auf der hoheitlichen Ebene (Staat und Europa) gibt es etwa, konkret auf Inhalte aus dem Internet bezogen, ein *„Safer Internet Work Programme 2004 - Awareness"*[50]. Auf Ebene der Unternehmen beziehen sich Awareness-Kampagnen vor allem auf den „Faktor Mensch" als Sicherheitslücke.[51]

In die rechtlichen Kategorien von Sicherheit eingefügt, kann das Sicherheitsbewusstsein als Ausprägung der Eigenverantwortung des Nutzers betrachtet werden. Ohne Sicherheitsbewusstsein sind selbst Pflichten den Nutzer zu informieren fruchtlos, wenn dieser die Information nicht nutzt und umsetzt. Zudem erscheint es eher ungewöhnlich, ein Medium zu nutzen, ohne auch Interesse und ein gewisses Maß an Zeit für die Sicherheit aufbringen zu müssen. Dem individuellen, privaten Nutzer bieten sich im Internet zahlreiche Foren, auf denen er sich mit dem Thema IT-Sicherheit auseinander setzen kann (was allerdings ein entsprechendes Problembewusstsein, Interesse und nicht zuletzt Zeit voraussetzt).

---

47 Vossbein, Eigenverantwortung und Marktwirtschaft als Steuerungsimpulse der IT-Sicherheit, in: Pohl/Weck (Hrsg.), Beiträge zur Informationssicherheit, 1995, S. 43 (46).

48 Fox, Security Awareness, in: DuD 2003, 676 (676 f.): Dies läge nicht zuletzt daran, dass Sicherheitsverletzungen überwiegend durch Nutzer, respektive Mitarbeiter eines Unternehmens verursacht werden. Ursachen seien Unkenntnis oder Missachtung von Sicherheitsbestimmungen, Nachlässigkeit oder fehlende Übung im Umgang mit Sicherheitswerkzeugen.

49 ISO/IEC 1799 (BS 7799), Information technology – Code of practice for information security management, 01.12.2000, S. 11, 6.2. User training "*Objective: to ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.*"

50 Vorschlag für eine Entscheidung des Europäischen Parlaments und des Rates über ein mehrjähriges Gemeinschaftsprogramm zur Förderung der sichereren Nutzung des Internets und neuer Online-Technologien vom 12.03.2004, KOM(2004)91 endg.

51 Solche Kampagnen können in unterschiedlichen Phasen aufgebaut sein: Phase der Aufmerksamkeit, Phase der Wissensvermittlung, Phase der Verstärkung (hier wird die dauerhafte Veränderung der Einstellung und des Verhaltens angestrebt) und Phase der Öffentlichkeit (Vermittlung eines positiven Vertrauens-Image), vgl. Fox, Security Awareness, in: DuD 2003, 676 (678 f.); ISO/IEC 17799: 2000, S. 11.

Während das Sicherheitsbewusstsein als eine Beschäftigung mit den Gefahren und somit als Voraussetzung für die Sicherheitserwartung betrachtet werden kann, bezieht sich die Sicherheitserwartung auf das Fehlen von Gefahren.

Eine niedrige Sicherheitserwartung kann nicht zuletzt Einfluss auf die Haftung für Sicherheitslücken haben. Im Rahmen der deliktischen Haftung orientiert sich etwa die Verkehrssicherungspflicht an den Sicherheitserwartungen der betroffenen Verkehrskreise.[52] Im Rahmen der Verkehrssicherungspflichten bei der Nutzung des Internets ist demnach die Sicherheit zu gewährleisten, die von den Nutzern berechtigterweise erwartet werden darf.[53] Hierbei soll die Sicherheitserwartung an dem ordentlichen Durchschnittsmenschen zu orientieren sein.[54] Kriterien der Sicherheitserwartung sind hierbei u. a. das Ausmaß der Gefahr, die Möglichkeit und Zumutbarkeit der Gefahrvermeidung (Verkehrssicherungspflicht des Schädigers und Selbstschutz des Geschädigten) und Vertrauensschutz, welche in einer Interessenabwägung einzustellen sind.[55]

Soweit es um Fehler geht, die die IT-Sicherheit beeinträchtigen, ist fraglich, von welchen Produkten die Gewährleitung der IT-Sicherheit erwartet wird und werden kann. Nicht zuletzt ist dieses für den Nutzer die Software, die er nach seinen Kriterien aussuchen kann. Diese soll etwa die Datensicherheit oder Kommunikationssicherheit in der Regel entweder positiv gewährleisten (etwa Anti-Virensoftware) oder aber zumindest nicht beeinträchtigen.[56] In Betracht gezogen werden könnte etwa die Sicherheitserwartung, Virenangriffen auf einem gewissen aktuellen Niveau standhalten zu können. Teilweise wird die Sicherheitserwartung auch vom Preis abhängig gemacht. So könne bei kostenloser Software nicht erwartet werden, dass umfangreiche Tests durchgeführt werden.[57]

---

52 Vgl. Koch, Haftung für die Weiterverbreitung von Viren, in: NJW 2004, 801 (804).

53 In Anlehnung an die Rechtsprechung des BGH zu den Sicherheitserwartungen betroffener Verkehrskreise, vgl. etwa BGH, Urteil v. 08. 01. 2002 - VI ZR 364/00, NJW 2002, 1263 (1284); BGH, Urteil v. 20.09.1994 - VI ZR 162/93, NJW 1994, 3348 (3349); BGH, Urteil v. 11.12.1984 - VI ZR 218/83, NJW 1985, 1076 (1076).

54 MünchKommBGB/*Wagner,* § 823 Rd. 575 will die Sicherheitserwartungen an dem ordentlichen Durchschnittsmenschen orientieren.

55 Koch, a.a.O., (Fn. 52), 801 (804), mit weiteren Hinweisen auf die Kommentarliteratur.

56 Selbst bei Produkten, deren Gebrauch mit Risiken verbunden ist, soll eine „Basissicherheit" vorausgesetzt werden können, Taeger, Produkt- und Produzentenhaftung, in: CR 1996, 257 (263).

57 Spindler, Das Jahr 2000-Problem, in: NJW, 1999, 3737 (3739): Bei der Haftung für fehlerhafte Software bestimmen etwa Faktoren wie das projektierte Einsatzgebiet, die Nutzungsdauer und der Preis (bei Freeware können nicht vollumfängliche Sicherheitstests zur Verweidung

Ein Beispiel für den normativen Bezug auf die „Sicherheitserwartung" findet sich in § 3 Produkthaftungsgesetz. Die Produkthaftung nach § 3 Produkthaftungsgesetzes schützt das Integritätsinteresse, das an den berechtigten Sicherheitserwartungen des Käufers ausgerichtet ist.[58] Diese Sicherheitserwartung ist produktorientiert an der entsprechenden Hard- und Software ausgerichtet. Die Sicherheitserwartungen – so sie denn im Bereich der IT-Sicherheit vorhanden sind – erfahren zwei Einschränkungen. Die Erwartungen müssen sich zum einen im Rahmen des Anwendungsbereichs der Haftungsvorschrift bewegen, d. h., die Sicherheitserwartungen müssen sich etwa bei der Produzentenhaftung auf die Unterlassung von Konstruktions-, Fabrikations- und Instruktionsfehlern beziehen.[59] Zum anderen ist sie auf die *„berechtigterweise"*[60] erwartete Sicherheit zu reduzieren, wobei zum Ausgleich vor überzogenen Sicherheitserwartungen eine *„Berücksichtigung aller Umstände"*[61] stattfinden muss.

Soweit gesetzliche Vorschriften ex ante zur Gewährleistung von Sicherheit bestehen, kann sich die zu erwartende Sicherheitserwartung an dem Niveau der gesetzlichen Vorschrift orientieren. So kann etwa im Szenario 3 bei der Organisation von personenbezogenen Daten erwartet werden, dass die technisch-organisatorischen Maßnahmen des § 9 BDSG und seiner Anlage eingehalten werden und tatsächlich ein entsprechendes Maß an Sicherheit gewährt wird.

Die Sicherheitserwartung des Nutzers besitzt eine rechtliche Relevanz, wenn sie sich im Rahmen des technisch Machbaren[62] und ökonomisch Vernünftigen[63] be-

---

von Konstruktionsfehlern erwartet werden) die berechtigten Sicherheitserwartungen der Nutzer.

58 Das Integritätsinteresse ist die Erwartung, dass die Sache die Sicherheit bietet, die von der Allgemeinheit berechtigterweise erwartet werden kann, vgl. Marly, Softwareüberlassungsverträge, 4. Aufl. 2004, Rd. 1304; ebenso Rothe, Produkthaftung. Rechtliche Grundlagen und ihre Auswirkungen auf die Industrie, in: CR 1993, 310 (312): *„Als maßgebend (…) wird nach dem Produkthaftungsgesetz die Sicherheitserwartung der durchschnittlichen Anwender vorgegeben (…)."*

59 Marly, a.a.O., (Fn. 58), Rd. 1304 f.; Bartsch, Computerviren und Produkthaftung, in: CR 2000, 721 (722). Ob und welche IT-Sicherheitslücken unter diese Fehlerkategorien subsumiert werden können, soll hier nicht weiter ausgeführt werden.

60 Die berechtigte Sicherheitserwartung schließt in jedem Fall die „totale Sicherheit" aus, vgl. Palandt, 65. Aufl. 2006, ProdHaftG, § 3 Rd. 3. Auf der anderen Seite unterschreitet wohl das „Mantra" der Softwareindustrie, dass Software nicht fehlerfrei sein könne (vgl. Bartsch, a.a.O., (Fn. 59), 721 (721)), die Sicherheitserwartungen der Allgemeinheit, und kann letztendlich auch nur für Fehler gelten, die nicht in die von Rechtsprechung und Literatur entwickelten Kategorien der Konstruktions-, Fabrikations- und Instruktionsfehler fallen.

61 Vgl. Palandt, 65. Aufl. 2006, ProdHaftG, § 3 Rd. 3.

62 Das technisch Machbare (oder vertraglich Vereinbarte) ist grundsätzlich die Obergrenze für Sicherheitserwartungen.

wegt (vgl. etwa § 3 Produkthaftungsgesetz „berechtigterweise“ und § 9 BDSG „erforderlich“). In Haftungsszenarien ex post kann eine entsprechende Sicherheitserwartung, die an Hersteller und Anbieter gestellt werden kann, zusammen mit Maßnahmen der Eigenverantwortung zu Grunde gelegt werden bzw. korreliert mit der in Eigenverantwortung zu treffenden Maßnahmen. Welche Qualität Maßnahmen in Eigenverantwortung diesbezüglich haben sollten, hängt vom konkreten Einzelfall ab.

II. Wissen um die Sicherheit – Nutzerleitbild

Mit dem Sicherheitsbewusstsein und der Sicherheitserwartung wurden Kriterien dargestellt, welche in ein IT-Informationsrecht einbezogen werden können. Darüber hinaus soll im Folgenden geprüft werden, ob diese Kriterien an einem sicherheitsorientierten Durchschnittsnutzer angelegt werden können.

Diesbezüglich soll hier dargelegt werden, ob ein bestimmtes Sicherheitsniveau allen Nutzern unterstellt werden kann (Idee des sicherheitsorientierten Durchschnittsnutzers). Diese Idee soll mit einer Studie des BSI[64] dargestellt werden. Hierbei bewerteten die Nutzer ihre Fähigkeiten im Bereich der IT-Sicherheit.

So ist 90% der Nutzern bekannt, dass der PC/Laptop bei Sicherheitslücken durch Hacker ferngesteuert werden kann.[65] Legt man diese Einschätzung einem IT-Informationsrecht zu Grunde, so müsste der Durchschnittsnutzer Informationen über Sicherheitslücken benötigen und fordern. Da 76% der Durchschnittsnutzer privat einen Virenscanner benutzen,[66] dürften diese auch ein Interesse an Information über ihre Sicherheit haben.[67]

---

63 Von einem Produkt, das unterdurchschnittlich billig ist, kann realistischerweise erwartet werden, dass ein bestimmtes Minimum an Sicherheit garantiert wird, allerdings auch nicht mehr, da „optimale Sicherheit“ ihren Preis hat, Taeger, Produkt- und Produzentenhaftung, in: CR 1996, 257 (263).

64 BSI, IT-Awareness-Monitoring – Bevölkerung, Repräsentativumfrage in der bundesdeutschen Bevölkerung zu Themen der IT-Sicherheit, September 2004. Hinweise zu Fundstellen finden sich in den Pressemitteilungen des BSI vom 20.01.2005, http://www.bsi.bund.de/-presse/pressinf/270105ohn_Virensch.htm (30.05.2006).

65 BSI Studie, a.a.O., (Fn. 64), Tabelle 22.

66 BSI Studie, a.a.O., (Fn. 64), Tabelle 4.

67 Betrachtet man allerdings die Umsetzung von Information am Beispiel des Einspielens von Patches, so ist der Nutzen fraglich: Das Einspielen von Patches beschäftigte 14% der Nutzer einmal im Monat, 42% noch nie (BSI Studie, a.a.O., (Fn. 64), Tabelle 21).

Soweit es einen sicherheitsorientierten Durchschnittsnutzer gibt, ist der Informationsfluss und -inhalt an diesem zu messen.

Zunächst soll kurz das Kriterium der Medienkompetenz für den Durchschnittsnutzer angeführt werden, bevor geprüft wird, inwieweit Überlegungen zum Durchschnittsverbraucher auf den Durchschnittsnutzer übertragbar sind.

1. Medienkompetenz und IT-Sicherheitskompetenz

Inhaltlich ist die Medienkompetenz[68] die Fähigkeit, Inhalte und Informationen finden, einordnen, nutzen und bewerten zu können. Dies umfasst auch in einem bestimmten Maße die Aneignung von technischen (Grund)Kenntnissen.

Solange auf der politischen Agenda das Bemühen um die Chancen und Freiheiten der Bürger in der Informationsgesellschaft steht, scheint die Medienkompetenz noch keine Realität zu sein. So ist diese nach einem Beitrag auf der Medienkompetenztagung in Nordrhein-Westfalen:

> *„(…) eine der großen gesellschaftlichen Herausforderungen, die darauf abhebt, alles zu tun, damit am Ende ein medienmündiger Bürger steht. Das ist, in der kürzesten Formulierung, die ich dazu finde, einer, der macht und nicht einer, der immer nur gemacht wird. Einer der macht und dadurch die Macht der hauptberuflichen Macher ein bisschen durchschaut, entheiligt, ernüchtert."*[69]

Diese Vorstellung von einem medienmündigen Bürger kann auf die Einstellung zur Sicherheit übertragen werden. Gerade ohne Kenntnisse von IT-Sicherheit und des erforderlichen Sicherheitsniveaus wird man in der Informationsgesellschaft „gemacht". Zugespitzt auf die Sicherheit sollte das Kompetenzportfolio eines Nutzers neben den (Grund)Kenntnissen über technische Abläufe, etwa Kompetenz hinsichtlich der einzusetzenden IT-Sicherheitsinfrastruktur beinhalten, da es etwa nicht zuletzt manchmal die neuen Eigenschaften eines Gerätes sind, die zulasten der Sicherheit implementiert werden (Stichwort Feature-Overflow).[70]

---

[68] Medienkompetenz wird etwa in § 39 des Landesmediengesetzes Nordrhein-Westfalen definiert: So ist die *„(…) Medienkompetenz im Land zu fördern, Medienerziehung zu unterstützen und zum selbstverantwortlichen Umgang mit allen Formen analoger und digitaler Medienkommunikation sowie zur gleichberechtigten Teilhabe an ihr beizutragen."*

[69] So Schneider, Norbert, Direktor der Landesanstalt für Medien Nordhein-Westfalen (LfM) auf dem Tag der Medienkompetenz im Landtag Nordrhein-Westfalen am 9./10.11.2004 in seiner Ansprache zur Begrüßung, http://www.tagdermedienkompetenz.de/doku/rede_-schneider.html (30.05.2006).

[70] Dieser kann am Beispiel des Adobe Readers verdeutlicht werden. Dieser ist eine Software zum Öffnen von PDF-Dokumenten. Mit der Version 6 des Readers wurde eine Funktion eingeführt, um Macromedia-Flash-Dateien und Filme – also bewegte Bilder - in PDF-

Addiert man zu diesen Kenntnissen die Kenntnis um die eigene Verantwortlichkeit, *„kann von einer dezidierten IT-Sicherheitskompetenz gesprochen werden".*[71]

2. Vom Durchschnittsverbraucher zum Durchschnittsnutzer

Fraglich ist, ob im Bereich der IT-Sicherheit auf einen Durchschnittsnutzer ähnlich einem Durchschnittsverbraucher im (sonstigen) Verbraucherrecht abgestellt werden kann. Im Europarecht wurde das Bild eines „durchschnittlich informierten, aufmerksamen und verständigen Durchschnittsverbrauchers" entwickelt. Ausgehend von diesem Leitbild könnte der Inhalt und Umfang der Information, die der Nutzer hinsichtlich Sicherheitslücken erhalten oder haben muss, mit einem Leitbild des Durchschnittsnutzers bestimmt werden.[72]

Es wird demnach versucht ein Leitbild zu finden, das Aussagen für eine Verteilung von Information über Sicherheitslücken zulässt. Ein solches Leitbild muss ein bestimmtes Sicherheitsbewusstsein oder gewisse eigene Sicherheitsvorkehrungen beim Nutzer erwarten lassen und von den Herstellern und Anbietern zu Grunde legt werden können. Umgekehrt müssen die Hersteller und Anbieter den Sicherheitserwartungen der Nutzer mit einem bestimmten Niveau von Sicherheitsmaßnahmen – respektive Informationen – entsprechen. Die Kriterien des Sicherheitsbewusstseins und der Sicherheitserwartung konkretisierend könnte ein Leitbild Folgen für den Bereich der Haftung zeitigen.

Zunächst soll grundsätzlich dargelegt werden, was ein „durchschnittlich informierter" Verbraucher ist, bevor die Annahmen der Rechtsprechung zum Wissensstand

---

Dokumenten einbetten zu können. Eine Funktion, die über den ursprünglichen Zweck und Einsatzgebiet der Software hinausgeht. Diese Funktion ermöglicht allerdings nicht nur die Animation. Präparierte PDFs können beim Öffnen auf einem Rechner zugreifen, um beispielsweise Cookies von den Rechnern der Besucher zu kopieren, heise news vom 12.10.2004, http://www.heise.de/newsticker/meldung/52078 (30.05.2006). Ebenso finden sich Spiele statt Sicherheit bei den laufenden Aufrüstungen bei mobilen Endgeräten (Handy). Vgl. zu den Gefahren bei Java-Handys, Fey, Jürgen, Adam Gowdiak, der Entdecker der Sicherheitslücke in Java-Handys, in: pcwelt.de, vom 19.10.2004, http://www.pcwelt.de/know-how/sicherheit/104018/ (30.05.2006) und heise news vom 19.10.2004, http://www.-heise.de/newsticker/meldung/52321 (30.05.2006).

71 BSI, Die Lage der IT-Sicherheit in Deutschland 2005, 2005, S. 11, http://www.bsi.de/literat-/lagebericht/lagebericht2005.pdf (30.05.2006).

72 Der Durchschnitt kann selbstverständlich kein Maßstab für (IT-)Sicherheit sein, will man das Optimum an Sicherheit erreichen. Der Durchschnitt kann allerdings ein Maßstab für die Sicherheit sein, muss man die Förderungspflichten und –rechte mit anderen Interessen abwägen. So können etwa „Pflichten zu informieren" mit weiteren Geschäftsinteressen des Anbieters oder Herstellers abzuwägen sein.

des Nutzers dargelegt werden. Dies soll als Basis für die abschließende Diskussion des Durchschnittsnutzers dienen.

a) Rechtsprechung des EuGH zum Durchschnittsverbraucher

Zunächst ist der Durchschnittsverbraucher ein Leitbild, das – soll es nicht willkürlich durch den einzelnen Richter verwendet werden – für die Entscheidungsfindung nachweisbare und überprüfbare Kriterien aufweisen muss.[73] Der EuGH hat demnach das Bild und die Kriterien des *„durchschnittlich informierten, aufmerksamen und verständigen Durchschnittsverbrauchers“* [74] entwickelt. Die Rechtsprechung des EuGH zum Durchschnittsverbraucher ist in Deutschland vom BGH und der Rechtsprechung übernommen worden.[75]

Der Begriff des Durchschnittsverbrauchers wurde im Wettbewerbsrecht entwickelt. Sinn und Zweck des Wettbewerbsrechts ist der Schutz von Mitbewerbern und der Schutz der Verbraucherinnen und Verbraucher, § 1 UWG. Diese sollen nicht zuletzt durch Produktinformationen (§§ 5, 6 UWG) geschützt werden.[76] Geschützt ist

---

73 Rüthers, Rechtstheorie, 1999, S. 392 f., Rd. 696.

74 Vgl. EuGH, 16.07.1998, Rs. C-210/96 Gut Springenheide, Slg. 1998, I-4657, Rd. 31, GRUR Int 1998, 795 (797); EuGH, 28.01.1999, Rs. C-303/97 Sektkellerei Kessler, Rd. 36, GRUR Int 1999, 345 (348); EuGH, 13.01.2000, Rs. C-220/98, Lifting, Slg. 1998, I-117, Rd. 27, NJW 2000, 1173 (1174).

75 Stetige Rechtsprechung seit BGH, Urteil v. 20.10.1999 - I ZR 167/97 Orient-Teppichmuster, GRUR 2000, 619 (621); BGH, Urteil v. 25.04.2001 - 2 StR 374/00, NJW 2001, 2812 (2813); zuletzt in BGH, Urteil v. 22.07.2004 - I ZR 288/01, GRUR 2004, 1037 (1038). Nicht immer hat ein Durchschnittsverbraucher ein „Recht“ auf korrekte Informationen: OLG Nürnberg, Urteil v. Urteil v. 28.12.1999 - 3U 2355/99, GRUR 2000, 1105 (1106), zur Unterscheidung zwischen Saft und Nektar, da ein durchschnittlich informierter, aufmerksamer und verständiger Durchschnittsverbraucher keine Ahnung von der richtigen Bedeutung des Begriffes Saft hat, kann er von der „Falschinformation“ auch nicht getäuscht werden. Zum Durchschnittsverbraucher im Telekommunikationsrecht: OLG Köln, Urteil v. 06.02.2002 - 6 U 143/01, MMR 2002, 465; OLG Köln, Urteil v. 18.01.2002 - 6 U 136/01, MMR 2002, 469.

76 Nicht zuletzt ist im Bereich des Verbraucherschutzes im Entwurf der europäischen Verfassung vom 29.10.2004 in Artikel III-235 Abs. 1 das Recht des Verbrauchers auf Information festgehalten:
„(1) Zur Förderung der Interessen der Verbraucher und zur Gewährleistung eines hohen Verbraucherschutzniveaus leistet die Union einen Beitrag zum Schutz der Gesundheit, der Sicherheit und der wirtschaftlichen Interessen der Verbraucher sowie zur Förderung ihres Rechtes auf Information, Erziehung und Bildung von Vereinigungen zur Wahrung ihrer Interessen.“

hierbei die Informationsgrundlage des Verbrauchers als Basis der Entscheidungsfreiheit.[77]

Fraglich ist darüber hinaus, wie der „angemessen (normal) informierte" Verbraucher die Information erlangen kann. Normal ist der Kenntnisstand, den die maßgebliche Verbrauchergruppe im allgemeinen Leben[78] (Schule, Zeitung, Alltag, Internet) erwirbt. Dieser „normale Kenntnisstand" wird bei Verbrauchern, die Produkte zumindest gelegentlich kaufen, vorausgesetzt.[79] Das Merkmal des „informierten" Verbrauchers knüpft an den aktuellen Wissens(zu)stand an.

Die Frage nach der Erhöhung des Wissens(zu)standes betrifft die Aufmerksamkeit und Verständigkeit des Verbrauchers und ist abhängig von dem zu erwerbenden Produkt.[80] So müsse der Verbraucher bei Vertrauensgütern auf die Information des Anbieters vertrauen (können), da er selbst das Produkt („handgemacht") nicht oder nur unter erschwerten Bedingungen beurteilen könne. Ob der Verbraucher die vom Anbieter angebotene Information

> *„wahrnimmt und in sein Kalkül einbezieht, ist dann seine Sache. Ein gewisses Maß an Selbstverantwortung kann dem Verbraucher nicht abgenommen werden."*[81]

Das Verbraucherleitbild des EuGH basiert im Wesentlichen auf dem so genannten *„Informationsmodell"*[82] Der Konsument wird mittels (gesetzlich) erforderlicher Information der Anbieter in die Lage versetzt, rationale und marktgerechte Entschei-

---

77 Dieses Leitbild dient vor allem der Konkretisierung der unbestimmten Rechtsbegriffe der Irreführung des Verbrauchers und der Verwechslungsgefahr im Wettbewerbsrecht.

78 Lettl, Der Schutz des Verbrauchers nach der UWG-Reform, in: GRUR 2004, 449 (454).

79 Helm, Das Verbraucherleitbild im Vergleich, in: Keller/Plassmann/v. Falck (Hrsg.), Festschrift für Wilfried Tilmann, 2003, S. 142 (142).

80 EuGH 22.06.1999, Rs. C- 342/97 Lloyd Schuhfabrik Meyer & Co. GmbH, Rd.. 26, GRUR Int 1999, 734 (736); EuGH 20.03.2003, Rs. C-291/00 LTJ Diffusion SA, Rd.. 52, GRUR 2003, 422 (425); Lettl, Der Schutz des Verbrauchers nach der UWG-Reform, in: GRUR 2004, 449 (454). Es wird regelmäßig zwischen Erfahrungs-, Such- und Vertrauensgütern im Kontext von Informationsasymmetrien und Unsicherheiten unterschieden, vgl. Menke, Die moderne, informationsökonomische Theorie der Werbung und ihre Bedeutung für das Wettbewerbsrecht, in: GRUR 1993, 718 (719); Van den Bergh/Lehmann, Informationsökonomie und Verbraucherschutz im Wettbewerbs- und Warenzeichenrecht, in: GRUR Int 1992, 588 (591).

81 Köhler, Zum Anwendungsbereich der §§ 1 und 3 UWG, in: GRUR 2001, 1067 (1069).

82 Solche verbraucherschützenden Informationsmodelle basieren auf einer gesetzlichen Pflicht des Anbieters den Verbraucher zu informieren und sehen eine Sanktionsmöglichkeit vor (regelmäßig zeitlich befristetes Widerrufsrecht des Verbrauchers), vgl. Kind, Die Grenzen des Verbraucherschutzes durch Information, 1997, S. 34.

dungen zu treffen.[83] Gesetzliche Normierungen finden sich etwa in der BGB-Informationspflichten-Verordnung[84] und in gesundheitlich sensiblen Bereichen wie dem Arzneimittelrecht[85]. Das wettbewerbsrechtliche Leitbild des Durchschnittsverbrauchers dient allerdings der Steuerung des Informationsinhaltes und sagt grundsätzlich nichts über den Informationsvorgang (Irreführungsverbot und kein Informationsgebot[86]).

b) Auswertung der nationalen Rechtsprechung hinsichtlich Internet- und Computerkenntnisse

Im Hinblick auf das Sicherheitsbewusstsein soll im Folgenden untersucht werden, inwieweit die Rechtsprechung bereits auf (sicherheitsrelevante) Computer- und Internetkenntnisse rekurriert.

Im Hinblick auf die Kenntnisse, die dem „durchschnittlich informierten, aufmerksamen und verständigen Durchschnittsverbraucher" zugemutet oder unterstellt werden, sollen Entscheidungen der Rechtsprechung mit Bezug zum Internet oder Computern präsentiert werden.[87] Diese sollen Anzeichen für ein zu Grunde geleg-

---

83 Zu den Unlänglichkeiten des Informationsmodells etwa in Zwangslagen: Bydlinski, Die Suche nach der Mitte, in: AcP 204 (2004), 309 (364 ff.).

84 So erlauben etwa die den Reiseveranstalter verpflichtenden Prospektangaben nach § 4 BGB-InfoV eine Prognose über den Erholungswert des Urlaubs.

85 Vgl. Pflicht zur Packungsbeilage im Arzneimittelrecht nach § 11 AMG.

86 BGH, Urteil v. 14.12.1995 - I ZR 213/93 GRUR 1996, 367 (368). Das Irreführungsverbot kann sich allerdings zu einem Informationsgebot verdichten, vgl. Fezer, Das wettbewerbsrechtliche Irreführungsverbot, in: WRP 1995, 671 (676). Fezer will darüber hinaus dem Informationsgebot der Werbenden eine Informationspflicht des Verbrauchers gegenüberstellen. Diese entspräche keiner „sanktionierten Rechtspflicht", sondern mehr einem rechtlich zu erwartendem Marktverhalten, a.a.O., S. 676.
Das „allgemeine" Verbraucherbild ist zudem durchaus vom Informationsvorgang geprägt. So geht das europäische Verbraucherrecht von einem Recht des Verbrauchers auf Information aus. Vgl. Reich in: Reich/Micklitz (Hrsg.), Europäisches Verbraucherrecht, 4. Aufl. 2004, S. 23 ff., Rd. 1.10 f., der von einem Verbraucherrecht auf Information als einem *„Informationsparadigma des gemeinschaftsrechtlichen Verbraucherschutzes"* (a.a.O., S. 24, Rd. 1.10) spricht.

87 Diese Auswertung erfolgt in dem Bewusstsein, dass die Entscheidungen aufgrund des unterschiedlichen Entscheidungskontextes und –horizonts nur einen kursorischen Überblick geben kann. Soweit sie primär wettbewerbsrechtliche Entscheidungen sind und keinen Erkenntnisgewinn für die hier interessierenden Fragen bieten, sollen diese nicht einbezogen werden: Vgl. BGH, Urteil v. 13.11.2003 - I ZR 40/01, MMR 2004, 160 (161), zur „umgekehrten Versteigerung im Internet"; BGH, Urteil v. 20.03.2003 - I ZR 60/01, GRUR 2003, 963 (964), zur Markennutzung AntiVir/AntiVirus; BGH, Urteil v. 24.10.2002 - I ZR 50/00, NJW 2003 895 (896), zur Computerwerbung; OLG Köln Entscheidung v. 19.07.2002 - 6 U 17/02, in: MMR 2003, 188: zur Kennzeichnungskraft der Bezeichnung Explorer. Dies gilt ebenso für Entscheidungen, die sich mit der Ähnlichkeit und Kennzeichnungskraft

tes „Durchschnittsniveau“ hinsichtlich Internet- oder Computersachverstand liefern. Abzugrenzen ist dieses von dem – nicht zwingend durchschnittlichen – Maßstab, der durch die eigenen Kenntnisse des Richters vorgegeben wird. Teilweise kann vermutet werden, dass der Richter seine eigenen über-, durch- oder unterdurchschnittlichen Internet- oder Computersachkenntnisse zu Grunde legt.[88]

Explizit mit der Frage, ob das Internet ein anderes Verbraucherleitbild erfordere, beschäftigte sich der BGH in einem Urteil zum Verbraucherleitbild bei Werbung im Internet.[89] Gegenstand der Entscheidung war die Klage eines Mitbewerbers wegen irreführender Werbung für Tintenpatronen. Irreführend deshalb, da die Information auf den Webseiten der Beklagten ohne das Anklicken von Angaben den Eindruck erwecken würde, die Beklagte vertreibe Produkte der Klägerin. Das Berufungsgericht ging davon aus, dass dem Internet ein von dem europäischen Verbraucherleitbild abweichendes Leitbild zu Grunde gelegt werden könne, da der elektronische Geschäftsverkehr auf den aktiven Interessenten ausgerichtet sei, der Informationen nachfragen müsse.[90] Daher könne bei diesem mehr vorausgesetzt werden als beim Normalverbraucher. Dem trat der BGH entgegen. Die Tatsache, dass Informationen aktiv abgerufen werden müssen, *„rechtfertigt als solche nicht die Zugrundelegung eines anderen Verbraucherleitbildes.“*[91]

Mit dem OLG Köln darf festgehalten werden, dass die Bedeutung des Begriffs „Internet“ der Allgemeinheit – Nutzern und Nichtnutzern – bekannt ist.[92] Allein diese,

---

von Domainnamen auseinandersetzen: LG München I „bioland.de“, Urteil v. 13.08.2002 - 9 HK O 8263/02, MMR 2003, 832 (833); im österreichischen Recht: OGH„internetfactory.at", Entscheidung v. 27.11.2001 - 4 Ob 230/01d.

88 So etwa der OLG Köln, Entscheidung v. 19.07.2002 - 6 U 17/02 in: MMR 2003, 188 (190): *„Die elektronische Datenverarbeitung durch Computer hat eine Vielzahl von englischsprachigen Fachbegriffen mit sich gebracht, die jeweils einzelne Anwendungen bzw. Vorgänge des EDV-Systems beschreiben. Zu diesen Begriffen gehört – was der Senat, dessen Mitglieder (potenziell) zu den Nutzern der EDV gehören, selbst feststellen kann – auch der weit verbreitete Begriff des „EXPLORER“.“* Ebenso mit weiteren Hinweisen zum „Richter als Durchschnittsverbraucher“: Schweizer, Die "normative Verkehrsauffassung", in: GRUR 2000 923 (924).

89 BGH, Urteil v. 16.12.2004 – I ZR 222/02, K&R 2005, 227.

90 BGH, Urteil v. 16.12.2004 – I ZR 222/02, K&R 2005, 227 (229 f.).

91 BGH, Urteil v. 16.12.2004 – I ZR 222/02, K&R 2005, 227 (231).

92 OLG Köln, Urteil v. 19.01.2001 - 6 U 78/00, MMR 2001, 538 (539): *„Der Begriff „Internet“ und seine inhaltliche Bedeutung haben in sämtlichen Medien eine derart weite Verbreitung gefunden, dass sowohl der Ausdruck als solcher als auch der damit beschriebene Sachverhalt, jedenfalls in den Grundstrukturen, fest im Bewusstsein der Allgemeinheit verankert sind. Auch Personen, die nicht über einen Zugang zum Internet verfügen und auch nicht zu den Nutzern der Möglichkeiten des Internets gehören, ist doch zumindest annähernd bekannt, was es mit dieser Form der Datenbeschaffung und –präsentation auf sich hat (…)“*

wenn auch positive, Feststellung im Jahr 2001, lässt das Internet immer noch nicht als etwas Alltägliches erscheinen.[93]

Nach dem KG Berlin ist es nicht überwiegend wahrscheinlich, dass *„der Begriff "Gigabyte" dem Durchschnittsverbraucher in seiner Bedeutung bekannt"*[94] ist. Weiter führt das Gericht differenzierend aus:

> *„Es geht hier nicht nur um das Verständnis von Internet-Insidern, sondern es geht auch um den durchschnittlichen Internetnutzer, dessen Verständnis ebenso durch die Angebote der Konkurrenz beeinflusst ist. Wenn hier nun ein vom Üblichen abweichendes Preismodell in versteckter Form und im Widerspruch zu der Angabe „Festpreis" beworben wird, so kann keineswegs vorausgesetzt werden, dass der Durchschnittsverbraucher die Einzelheiten des Preismodells erkennt und die auf ihn zukommenden Kosten einigermaßen sicher kalkulieren kann."*[95]

Wenn bereits die Bedeutung von Gigabyte allein dem Verständnis von Internet-Insidern zuzurechnen ist, lässt dies erwarten, dass die Rechtsprechung für komplexere Sachverhalte wenig Kenntnis vorausgesetzt. Zumal diese Kenntnisse keine Informationen sind, die dem Anbieter vorbehalten sind, sondern sich leicht und ohne Aufwand erschließen lassen.

Im Bereich des sicheren Internetzugangs gibt es im Wettbewerbsrecht ein Urteil des OLG Hamburg[96]. Zu beurteilen war der Slogan:

> *„- eröffnet Ihnen den einfachen Weg ins Netz: Schnell, sicher, kostengünstig".*

Das Gericht war folgender Auffassung:

> *„Angesichts der Diskussionen über die Datensicherheit im Internet liegt es für den Verkehr nahe, die Angabe "sicher" für den Internetzugang der Ag. in einem Kontext, in dem die Ag. sie benutzt hat, nicht etwa (nur) auf die Stabilität der Übertragungswege, sondern (auch) auf die mit dem Internet verbundenen Sicherheitsgefahren, nämlich auf die Einschleusung von Computerviren und/oder den Mißbrauch von Daten zu beziehen, obwohl die Ag. - anders als die Ast. in ihrer Werbung - im Kontext nicht auf entsprechende Software hinweist."*[97]

Das OLG Hamburg legt im Vergleich zu den Ausführungen des KG Berlin zum Gigabyte einen umsichtigen Nutzer zu Grunde, der sich bereits Gedanken um die verschiedenen Kategorien der Sicherheit macht.

---

93 So hätte ein Fernseher wohl kaum solche Ausführungen in einer Urteilsbegründung erhalten.

94 KG Berlin, Urteil v. 6.4.2001 - 5 U 6/01, in: MMR 2001, 701 (701), zum Internet zum Festpreis. Zur gleichen Festpreisthematik: OLG Köln, Urteil v. 26.05.2000 - 6 U 191/99, MMR 2000, 700; OLG Hamburg, Urteil v. 11.05.2000 - 3 U 252/99, MMR 2000, 702.

95 KG Berlin, Urteil v. 6.4.2001 - 5 U 6/01, in: MMR 2001, 701 (701).

96 OLG Hamburg, Entscheidung v. 31. Oktober 2002 - 3 U 71/0, MMR 2003, 340 (340) Leitsatz der Redaktion: „*Die Angabe „T-Online eröffnet Ihnen den einfachen Weg ins Netz: Schnell, sicher, kostengünstig" in einer Multimedia-Präsentation auf einer CD-ROM ist im Hinblick auf den Begriff „sicher" irreführend. Denn es liegt für den Verkehr nahe, diese Angabe nicht nur auf die Stabilität der Übertragungswege, sondern auch auf die mit dem Internet verbundenen Sicherheitsgefahren zu beziehen."*

97 OLG Hamburg, Entscheidung v. 31. Oktober 2002 - 3 U 71/0, MMR 2003, 340 (340).

Über die Sicherheit von Passwörtern ging es vor dem LG Bonn. Zur Entscheidung stand das Zustandekommen eines Vertragsschlusses bei einer Internetauktion. Das Gericht stellte bei einem Gebot mittels E-Mail fest, dass die Verwendung der E-Mail und des Passwortes mangels ausreichender Sicherheitsstandards keinen Anscheinsbeweis für das Zustandekommen eines Vertrages begründen könne.

Das Gericht führte aus, dass ein online verwandtes Passwort Zugriffsmöglichkeiten Dritter ausgesetzt ist.

> *„Im Hinblick auf die derzeitigen Sicherheitsstandards der im Internet verwendeten Passwörter als solche und die Art ihrer Verwendung kann nicht der Schluss gezogen werden, dass der Verwender eines Passwortes nach der Lebenserfahrung auch derjenige ist, auf den das Passwort ursprünglich ausgestellt wurde (…).“*[98]

In dieser Entscheidung standen nicht primär die Kenntnisse der Nutzer im Vordergrund. Dennoch erlaubt sie einige Rückschlüsse auf (durchschnittliche) Anforderungen an Sicherheitsmaßnahmen. Das Gericht monierte nicht die Wahl des Passwortes (04xx) als zu kurz und einfach. Sogar die Verwendung des Geburtsdatums würde nach Ansicht des Gerichts keine Rechtsfolgen (Rechtsscheinhaftung) nach sich ziehen, da sich die Gefahren des Internets in der Entschlüsselung des Passwortes manifestieren würden, die Passwortwahl des Nutzers Einfluss aber keinen auf die Entschlüsselungsmöglichkeiten habe. [99]

Ein weiterer Fall, in dem dem Nutzer eine besondere Sachkunde des Internets unterstellt wird, beschäftigte sich mit der Frage, ob eine Variante einer Internet-Auktion als Versteigerungen gesehen werden kann. Das Gericht unterstellt, dass die Nutzer über besondere Sachkunde verfügen, weil *„die das Internet nutzenden Personen bereits über spezielle Kenntnisse verfügen müssen, um dieses Medium überhaupt zu gebrauchen und sinnvoll einzusetzen.“*[100] Diese Kenntnisse würden auch den Ablauf einer Internetversteigerung umfassen. Diese Erkenntnis überrascht grundsätzlich nicht, ist aber auch nicht wei-

---

98 LG Bonn, Urteil v. 07.08.2001 - 2 O 450/00, MMR 2002, 255 (256). Ebenso das AG Erfurt, Urteil v. 14.09.2001 - 28 C 2354/01, MMR 2002, 127 (128): Die E-Mail-Adresse i.V.m. einem Passwort sei kein ausreichendes Indiz dafür, dass der E-Mail-Inhaber an der Internetversteigerung teilgenommen hat. Das Internet selbst gewährleiste keine Sicherheit dergestalt, dass Dritte keinen Zugriff auf die entsprechenden Daten haben.

99 LG Bonn, Urteil v. 07.08.2001 - 2 O 450/00, MMR 2002, 255 (257).

100 LG Wiesbaden, Urteil v. 13.01.2000 - 13 O 132/99, JurPC Web-Dok. 57/2000 http://-www.jurpc.de/rechtspr/20000057.htm (30.05.2006). Ebenso OLG Hamburg, Urteil v. 5.11.1998 - 3 U 130/98, MMR 1999, 159 (160): *„Zu berücksichtigen ist auch der Umstand, daß niemand ohne gewisse Grundkenntnisse von den Strukturen das Internet benutzen kann.“* Wiebke, „Deep Links“, in: WRP 1999, 734 (738) bescheinigt dem durchschnittlichen Internetnutzer *„gewisse technische Kenntnisse“*. OLG Köln, Urteil v. 19.01.2001 - 6 U 78/00, MMR 2001, 538 (539), a.a.O., (Fn. 92). Verhalten: Freitag, Wettbewerbsrechtliche Probleme im Internet, in: Kröger/Gimmy (Hrsg.), Handbuch zum Internetrecht, 2000, S. 402, der hinsichtlich der Anforderungen an die Kenntnisse noch keinen Maßstab der Rechtsprechung ausmacht.

terführend. Da der Adressatenkreis des Produkts „Internet“ grundsätzlich nicht auf einen bestimmten Kreis zu reduzieren ist – dies kann allenfalls für die Nutzung bestimmter Webangebote gelten – sind diese speziellen Kenntnisse nicht geeignet, ein gesondertes Nutzerwissen für die Anwendung zu bestimmen.[101] Fokussiert auf die IT-Sicherheit kann zudem angemerkt werden, dass gewisse technische Kenntnisse für die Nutzung hinreichend sein mögen, für die sichere Nutzung aber noch nicht ausreichend sind.

Keine besonderen Kenntnisse voraussetzend, zumindest aber kein Sicherheitsbewusstsein verlangend, stellte der BGH in seiner „Dialer-Entscheidung“[102] fest, dass es dem Internetnutzer nicht oblag, ohne besondere Verdachtsmomente für einen Missbrauch ein Dialerschutzprogramm zu nutzen.

Im Rahmen einer wettbewerbsrechtlichen Entscheidung stellte das OLG Hamburg hinsichtlich der Anforderungen an die Dialerschutzsoftware fest, dass Verbraucher mündige Bürger seien, die sich ihre Programme gezielt selbst aussuchen und auf ihrem heimischen Computer installieren würden.[103] Dies gilt nicht nur für die Gruppe der sicherheitsbewussten Nutzer, sondern offensichtlich für jeglichen Nutzer, wenn das Gericht weiter ausführt, es habe keinen Zweifel daran,

> *„dass der durchschnittliche Nutzer eines Viren- und/oder Dialer-Schutzprogramms ohne weiteres in der Lage ist zu entscheiden, welche Schutzmechanismen ihm angemessen erscheinen und welche Konsequenzen er zu ziehen hat, wenn das Programm seinen Ansprüchen nicht genügt.“*[104]

Der Überblick bietet lediglich Einzelfallentscheidungen. Abgesehen von der Verallgemeinerbarkeit bleibt die Frage, auf welche Bereiche diese übertragen werden können. Soweit etwa in der letztgenannten „Dialer-Entscheidung“ keine Installation von Schutzprogrammen für (rechtlich) erforderlich erachtet wurde, könnte man dies auch auf Virenschutzprogramme ausdehnen wollen. Für und widerstreitende Kriterien für eine solche Übertragung könnten Gefahrenpotenzial, technische Raffinesse des Angriffs, Aktualität der Gefahr, tatsächliche Verbreitung von Schutzprogrammen, individuelles Gefahrenrisiko (Nutzungshäufigkeit, technische Voraussetzungen) und Kosten-Nutzen-Er- und Abwägungen sein.

---

101 In diesem Sinne auch Schrader, Die wettbewerbsrechtliche Beurteilung von neuen Vertriebsformen im Internet, 2004, S. 194, der konstatiert, dass es keinen besonderen Internet-Verbraucher gebe.

102 BGH, Urteil v. 04.03.2004 - III ZR 96/03, MMR 2004, 308.

103 OLG Hamburg, Beschluss v. 13.04.2004 – 5 W 52/04, CR 2005, 19 (20).

104 OLG Hamburg, Beschluss v. 13.04.2004 – 5 W 52/04, CR 2005, 19 (20).

Festzuhalten ist, dass sich die Rechtsprechung kaum mit dem Wissen der Nutzer um ein sicheres Internet befasst hat. Daher kann kein Wissensminimum vorausgesetzt werden, was die Bezeichnung „durchschnittlich" rechtfertigen würde. Soweit dennoch auf den Durchschnittsnutzer abgestellt wird,[105] wird dieser nicht beschrieben. Daher kann festgestellt werden, dass die Rechtsprechung (noch) keine einheitliche Vorstellung von den Kenntnissen eines „Durchschnittnutzers" entwickelt hat. Soweit kein Durchschnittsnutzer feststellbar ist, der ähnlich einem Durchschnittsverbraucher informiert und umsichtig ist, könnten dies erhöhte Anforderungen an die Informationspflichten der Anbieter zur Folge haben.

c) Vom Durchschnittsverbraucher zum Durchschnittsnutzer

Die Angleichung des Begriffs Durchschnittsverbraucher an einen Durchschnittsnutzer erfolgte etwa durch das LG Düsseldorf:

> *„Bei verständiger Betrachtung will der Nutzer, und zwar gerade der informierte, aufgeklärte Durchschnittsnutzer, der sich vom Internet einen schnellen Zugriff auf viel Information verspricht – denn darin liegt letztlich der Sinn des Internet (…)."*[106]

Fraglich ist, ob das Bild des Durchschnittsverbrauchers, das für das Wettbewerbsrecht entwickelt wurde, im Bereich der Information über Sicherheitslücken angewandt werden kann; quasi der verständige Internetnutzer als Durchschnittsnutzer oder „Durchschnittsgarant" für die Sicherheit betrachtet werden kann. Entsprechend des Leitbildes ließen sich Informationsrechte und –pflichten verteilen. Ein Leitbild des Durchschnittsnutzers könnte für die IT-Sicherheit und den damit verbundenen Gefahren zusätzlich der Zuweisung von Verantwortung und der Schutzsphärenverteilung bei der Haftung dienen. Die Haftung könnte durch die Sicherheitserwartungen der Nutzer und durch den sich daraus ergebenden Pflichten der Anbieter und Hersteller zu Schutzmaßnahmen bestimmt werden.[107] Soweit ein Si-

---

105 Vgl. OLG Hamburg, a.a.O., (Fn. 103).

106 LG Düsseldorf, Urteil v. 27.03.2002 - 12 O 48/02. In diesem wettbewerbsrechtlichen Urteil ging es um die Verwendung von Metatags ohne Bezug zum Inhalt der Seite.
Nach Ott, Urheber- und wettbewerbsrechtliche Probleme von Linking und Framing, 2004, S. 431, kann sogar ein einheitlicher Informationsstand bzw. ein Wissensminimum erwartet werden, wenn er im Rahmen einer wettbewerbsrechtlichen Diskussion den Nutzerkreis im Internet grundsätzlich für informiert hält: „*Es mag zwar einige weit unterdurchschnittlich informierte Internetbenutzer geben, insbesondere solche, die ihre ersten Schritte in dem neuen Medium machen (…).*"

107 Micklitz, Zur Notwendigkeit eines neuen Konzepts für die Fortentwicklung des Verbraucherrechts in der EU, in: VuR 2003, 2 (11 f.) sieht in Zukunft die Eigenverantwortung des Verbrauchers stärker im Vordergrund der Überlegungen: *„Die Kommission hat sich politisch-programmatisch mit der Eigenverantwortung des Verbrauchers (noch) nicht auseinandergesetzt.",* Micklitz, a.a.O., S. 11 f.

cherheitsbewusstsein unterstellt werden kann, haben die Nutzer darüber hinaus Maßnahmen in Eigenverantwortung zu treffen. Gerade im Bezug auf Informationspflichten wird die Abhängigkeit deutlich. Ohne ein gewisses Sicherheitsbewusstsein wird der Nutzer kaum die Informationen des Anbieters oder Nutzers wahrnehmen.

Eine Möglichkeit das Leitbild des Durchschnittsnutzers auf das Internet zu übertragen, ist die Gleichsetzung des Nutzers mit dem Verbraucher. Soweit dieser unter § 13 BGB subsumiert werden kann, fragt er als Verbraucher Produkte (Hard- und Software als Gegenstand des Kaufvertrages) genauso wie Dienst- oder Werkleistungen (Internetzugang, Webhosting, Webpräsenz, etc.) nach. In diesem Fall ist das Internet nur eine Modifikation der Art und Weise des Abschlusses des Rechtsgeschäfts, d. h. des „Konsumierens". Insoweit ist der Durchschnittsnutzer kongruent mit dem Durchschnittsverbraucher.

Jedoch ist festzuhalten, dass der Internetnutzer über den Durchschnittsverbraucher hinausgeht, da das Verbraucherleitbild keine b2b, g2g oder g2b Konstellationen erfasst.[108] Soll hier auch ein gewerblicher und staatlicher Durchschnittsnutzer zu Grunde gelegt werden können, muss der Durchschnittsnutzer unabhängig von der Dichotomie Verbraucher – Unternehmer gefunden werden. Entscheidend darf nicht die staatliche, gewerbliche oder private Verfasstheit des Nutzers sein, sondern die grundsätzliche Möglichkeit von einer Sicherheitslücke Kenntnis zu haben oder erlangen zu können. Allerdings wird in der Regel der Anbieter eines IT-Systems oder der Hersteller eines Produkts bessere Kenntnismöglichkeiten und damit Informationspflichten haben. Zudem könnte bei einem gewerblichen Anbieter oder Hersteller aus dem Aspekt der Vorteilsziehung ein erhöhtes Bemühen um die Kenntnis von Sicherheitslücken angenommen werden. Insoweit wird entsprechend der Dichotomie Verbraucher – Unternehmer die Gegenüberstellung von Nutzer und Hersteller bzw. Anbieter die Informationspflichten bestimmen.

Festzuhalten bleibt, dass zur Bestimmung eines Durchschnittsnutzers im Bereich der IT-Sicherheit nicht auf den Durchschnittsverbraucher abgestellt werden kann. Die Informationspflichten können grundsätzlich unabhängig von der gewerblichen

---

108 Zur Diskussion, ob der wettbewerbsrechtliche Schutz auf b2b oder b2c oder beide Konstellationen Anwendung finden sollte, Henning-Bodewig, Das Europäische Lauterkeitsrecht: B2C, B2B oder doch besser beide?, in Keller/Plassmann/Clemens/v. Falck (Hrsg.), Festschrift für Winfried Tilmann, 2003, S. 149 (157). Sie führt aus, dass der Schutz der Mitbewerber und der Schutz der Verbraucher zwei Seiten der Medaille und nicht immer trennscharf seien.

Absicht bestehen und unterscheiden sich somit von den Informationspflichten gegenüber dem Durchschnittsverbraucher.

III. Zusammenfassung

Es gibt keinen einheitlichen Maßstab zur Beurteilung des Wissens(zu)standes des Nutzers hinsichtlich der Sicherheit im Internet. Während die Rechtsprechung (noch) keine verwertbare Aussage getroffen hat, ist die Selbsteinschätzung eher positiv. Die Selbsteinschätzung unterscheidet sich von anderen Studien (von Unternehmensseite und der Politik) zur IT-Sicherheit, die den Nutzer regelmäßig als „Faktor Mensch" und damit als Gefahr für die Sicherheit bewerten.[109]

Demnach ergibt sich entgegen der Rechtsprechung aus eigener Einschätzung ein Bild eines Nutzers, der grundsätzlich bereits ein Wissen zu haben scheint.[110] Ein Wissen, das allerdings nicht immer konsequent in Maßnahmen umgesetzt wird. Das Problembewusstsein und die Anforderungen und Bedürfnisse des Durchschnitts können und sollten jedoch ein Maßstab für den Umfang der Informationspflichten der Anbieter und Hersteller sein. Ein Durchschnittsnutzer ist allerdings nicht entsprechend einem Durchschnittsverbraucher feststellbar.

D Handlungs- und Entwicklungsimplikationen – Reaktionspflichten

Im Folgenden sollen in einem Überblick die Handlungs- und Entwicklungsimplikationen der Hersteller zum Schließen bekannter Sicherheitslücken durch Updates oder Patches vorgestellt werden und die Reaktionspflichten der Nutzer angedeutet werden. Eine ausführliche Behandlung, inwieweit der Hersteller vertraglich oder deliktisch verpflichtet sind Updates oder Patches zur Verfügung zu stellen, geht über das Thema der Arbeit – ob der Fokussierung auf die Rechte und Pflichten im Hinblick auf die Offenbarung der Sicherheitslücken – hinaus.

---

109 Vgl. etwa KES und KPMG Sicherheitsstudie 2002, http://www.kes.info/archiv-/material/studie2002/ (30.05.2006), die den Mitarbeiter als relativ hohes Sicherheitsrisiko bewertet (30% der Gefahren sollen alleine durch Irrtum und Nachlässigkeit der Mitarbeiter verursacht werden). Der hohe Rang des Faktors Mensch wurde in der folgenden Studie bestätigt, KES und Microsoft Sicherheitsstudie 2004, http://www.kes.info/archiv/material/-studie2004/kes-Microsoft-Studie2004-Sonderdruck.pdf (30.05.2006).

110 So auch die Bewertung der Studie des BSI von heise news vom 27.01.2005: *„Überraschend hoch sei in der Bevölkerung dagegen das Wissen zu Angriffsmöglichkeiten über das Internet."*, http://-www.heise.de/newsticker/meldung/55632 (30.05.2006).

I. Update und Patch

Ein Patch dient der Schließung einer konkreten (kleinen) Lücke, während mit dem Update oder Service Pack mehrere Programmteile oder –funktionen überarbeitet werden können.[111]

1. Updates

> *„Ein Update in der Informatik ist eine Erweiterung, die installiert werden kann, um ein Programm oder ein ganzes System zu verbessern, auf eine höhere Version zu bringen und/oder um Fehler zu bereinigen. Ganz wichtig ist ein Update in Form von so genannten Sicherheitspatches, die dafür sorgen, dass Sicherheitslücken geschlossen werden.“*[112]

Schuldrechtlich können Updates oder Patches zur Schließung einer Sicherheitslücke eine Gewährleistung des Herstellers oder Entwicklers sein.[113] Eine vertragliche Gewährleistungspflicht – im Fall von Standardsoftware[114] – nach Kaufvertrags-

---

111 Vgl. Punkt 7.3 der Guidelines for Security Vulnerability Reporting and Response Version 2.0, 01.09.2004, http://www.oisafety.org/guidelines/secresp.html (30.05.2006); Man kann auch weiter differenzieren: Update ist der Oberbegriff für jegliche Aktualisierung der Software. Der Grund kann vielfältig sein, so etwa Fehlerbeseitigungen, neue Grafiken oder Funktionen (dann in der Regel als Upgrade bezeichnet). Soweit das Update eine Sicherheitslücke (nicht jeder Fehler eröffnet gleichzeitig eine Sicherheitslücke) schließen soll, kann dieses als Patch bezeichnet werden.

112 So die Definition von update im Internetlexikon Wikipedia, http://de.wikipedia.org/wiki/Update (30.05.2006).

113 Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3145) mit weiteren Hinweisen. Spindler spricht darüber hinaus das Problem der Sicherheitslücke und Verjährung an.

114 Bei Open Source Software wird versucht, die Gewährleistung durch die GPL (General Public License) definitionsgemäß auszuschließen. Die GPL ist nur eine unter vielen Open Source Lizenzmodellen. In der Entscheidung des LG München I, Entscheidung v. 15.05.2004 - 21 O 6123/03, wurde die GPL als AGB eines Softwareüberlassungsvertrages eingestuft. Zum Gewährleistungsausschluss, vgl. § 11 der GPL, http://www.fsf.org/licenses/gpl.html (30.05.2006): “11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.” Koch, Handbuch Software- und Datenbankrecht, 2003, S. 170, Rd. 3, geht auf die Rechtmäßigkeit des Gewährleistungsausschlusses im Fall eines Kaufs von OSS nicht ein, da er wohl die grundsätzliche Kostenfreiheit von OSS unterstellt, a.a.O., S. 729, Rd. 436.

recht[115] besteht, wenn mangelhafte Software geliefert wird. Bei Standardsoftware soll man dies regelmäßig annehmen können, wenn sie nicht für die erwartete gewöhnliche Art der Verwendung geeignet ist.[116] Konkret könnte das Update als Nacherfüllung qualifiziert werden, die jedoch keine Wandlung ausschließen soll.[117] Die schuldrechtliche Qualifizierung eines Updates lässt eine mögliche deliktische Pflicht zum Patch unberührt.[118]

In den AGB und Lizenzbedingungen wird nicht selten darauf hingewiesen, dass *„Software niemals völlig fehlerfrei"*[119] sein könne. Diese technische Unmöglichkeit, bei komplexen Programmen Fehlerfreiheit herzustellen, soll nur dann eine Haftung ausschließen können, wenn das Programm dem Stand von Wissenschaft und Technik entspricht.[120] In diesem Fall kann der Hersteller konsequenterweise nur dann eine Pflicht haben, ein Update oder Patch bereitzustellen, wenn die Technik neue Möglichkeiten bietet. Davon unberührt muss allerdings die Pflicht bleiben, den Nutzer über Sicherheitslücken zu informieren, da dieser nur dann eine eigenverantwortliche Abwägung zwischen Schadensmöglichkeit und Deinstallation treffen kann.

In welchem konkreten Zeitrahmen der Hersteller ein Patch bereitstellen oder zumindest bei Unmöglichkeit informieren muss, ist im Einzelfall zu bestimmen. Die Qualität der Rechtsgutgefährdung, der mögliche Schadensumfang sowie die Vorteilsziehung des Herstellers können in die Überlegungen einzubeziehen sein.[121]

---

115 Zur Frage, wie der Softwareüberlassungsvertrag zivilrechtlich einzuordnen ist, vgl. Koch, a.a.O., (Fn. 114), S. 169, Rd. 1, Kaufrecht bei Standardsoftware; Marly, Softwareüberlassungsverträge, 4. Aufl. 2004, Rd. 35 ff.

116 Koch, a.a.O., (Fn. 114), S. 313 Rd. 16.

117 Die Ansprüche auf Rücktritt und Minderung können nicht durch die Vereinbarung eines Updates abbedungen werden, LG Karlsruhe, Urteil v. 02.05.1995 3 O - 41/95, CR 1996, 290. Das Update als Nacherfüllung ist allerdings dem Vertriebshändler, mangels Zugriff auf den Quellcode, regelmäßig nicht möglich, Koch, a.a.O., (Fn. 114), S. 365, Rd.115. Der Händler ist dann nach § 275 Abs. 2 S. 1 BGB von der Pflicht zur mangelfreien Leistung befreit, er kann aber bei Vertretenmüssen ersatzpflichtig nach § 280 BGB sein.

118 Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3147). Hierzu vgl. Kapitel 5 C III. und IV. 1.

119 Für die Gewährleistung muss bedacht werden, dass (technische) Fehlerfreiheit nicht gleichbedeutend sein muss mit rechtlicher Mängelfreiheit (etwa bei technisch fehlerfreier Software, der eine zugesicherte Eigenschaft fehlt): Koch, a.a.O. (Fn. 114), S. 320, Rd. 27 f. Für die Frage eines Schadensersatzes nach § 280 BGB kommt es auf das Verschulden des Herstellers an. Dieser kann sich allerdings durch den Nachweis, dass die Software dem Stand der Technik entspricht, entlasten, vgl. Heussen, Unvermeidbare Softwarefehler, in: CR 2004, 1 (6).

120 Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3146).

121 Spindler, a.a.O., (Fn. 120), 3145 (3147).

Manche Hersteller veröffentlichen in zeitlich regelmäßigen Abständen Patches (Patchday) und schließen damit bekannte Sicherheitslücken.

2. Online-Updates

Die Eignung von Updates und Patches zur Behebung von Sicherheitslücken sind organisatorisch von der Distribution und der Information der Nutzer abhängig. Professionelles Patchen setzt ein institutionalisiertes Verfahren und die Information bzw. Instruktion des Nutzers voraus.[122] Unter diesen Aspekten ist ein Online-Update in Form eines automatischen Downloads einfach, da es dafür sorgt, dass Sicherheitslücken unbemerkt geschlossen werden. Eine so verstandene Handlungsimplikation macht bei einem zeitnahen Online-Update vielleicht den Aspekt der Distribution, nicht jedoch die Frage der Information selbst überflüssig. Unter dem Aspekt des Selbstschutzes sind unkontrollierbare und nicht steuerbare Updates jedenfalls abzulehnen.[123]

Gründe für ein solches automatisches Software-Update sind neben der Möglichkeit der zeitnahen Einspielung der Software, unabhängig vom Nutzer, der angebotene Patches häufig nicht oder nicht zeitnah einspielt, auch die Möglichkeit der Kostenersparnis (kein Datenträger und aufwendiger Vertrieb erforderlich)[124] und eine Chance der Hersteller von Betriebssystemen ihren guten Ruf zu erhalten, da Sicherheitslücken unbemerkt geschlossen werden können. Allerdings muss bei einem komplexen Netzwerk die Funktion und Wirkung zunächst getestet werden, um nicht neue Sicherheitslücken zu verursachen. In einem solchen Fall sind automatische Updates eher ein Sicherheitsrisiko denn risikominimierend.

Wie in der Vergangenheit einer Diskussion um Online-Updates zu entnehmen ist, kann ein Online-Update neben der sicherheitsbeeinträchtigenden Wirkung auch rechtliche Implikationen haben. Im Landesdatenschutzgesetz Schleswig-Holstein ist in § 6 Abs. 2 geregelt:

> *„Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. Die Zugriffe dieser Personen sind zu protokollieren und kontrollieren."*

---

122 Oppliger, Sicherheit von Open Source Software, in: DuD 2003, 669 (675).

123 *Hansen*, in: Rossnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, S. 311, Rd. 79.

124 Zum Zeitfaktor und Aufwand vgl. Punkt 18.3.1.des 32. Tätigkeitsberichts des Hessischen Datenschutzbeauftragten vom 31.12.2003, vgl. http://www.datenschutz.hessen.de/Tb32-/K18P03.htm (30.05.2006).

Im 26. Tätigkeitsbericht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein 2004 wird deshalb das automatische Online-Update für datenschutzrechtlich unzulässig erklärt.[125] Auch der hessische Datenschutzbeauftragte hat sich mit der datenschutzrechtlichen Zulässigkeit von Software-Updates beschäftigt und als „Fernwartung" dem § 4 Hessisches Datenschutzgesetz, der Regelung der Verarbeitung personenbezogener Daten im Auftrag, unterworfen.[126]

Im Ergebnis ist nach datenschutzrechtlichen Anforderungen und unter Berücksichtigung möglicher Sicherheitsrisiken ein Update wie folgt anzubieten: Das Online-Update ist vom Nutzer zu initiieren, ein Online-Datenaustausch mit dem Zielrechner ist nicht zwingend erforderlich (transparenter und revisionssicherer Update- und Installationsprozess), alternative datenträgerbasierte Updateverfahren sind an-

---

125 Dem Tätigkeitsbericht ist zu entnehmen, dass der Hersteller der Software mit dem automatischen Online-Update die Möglichkeit hat, unter anderem zu prüfen, welche Updates bereits installiert sind und die Versionsnummern von Softwarepaketen auslesen kann. Test hätten ergeben, dass beim ersten Scan eines Systems fast 10 MB Daten an den Server gehen, bevor nur eine Datei herunter geladen wird, vgl. 26. Tätigkeitsbericht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein 2004, Landtagsdrucksache vom 06.05.2004 15/3300, S. 87. Im Tätigkeitsbericht wurde zudem einen Auszug aus Lizenzbedingungen im Wortlaut (ohne Angabe des Gütigkeitsdatums) abgedruckt. Danach geben die Nutzer ihr Einverständnis zum Online-Update: *„Wenn Sie sich entscheiden, die Update-Funktionen innerhalb des Betriebssystems oder der Betriebssystemkomponenten zu verwenden, ist es zum Implementieren der Funktionen erforderlich, bestimmte Informationen zum Computersystem, zur Hardware und zur Software zu verwenden. Indem Sie diese Funktionen verwenden, ermächtigen Sie Microsoft oder deren bezeichneten Vertreter zum Zugriff auf die erforderlichen Informationen und zu deren Verwendungen für Updates. Microsoft ist berechtigt, diese Informationen nur zur Verbesserung ihrer Produkte oder zum Liefern von benutzerdefinierten Technologien an Sie zu verwenden. Microsoft erklärt sich einverstanden, solche Daten ausschließlich anonym offen zu legen. Das Betriebssystemprodukt oder die Betriebssystemkomponenten enthält bzw. enthalten Komponenten, die die Verwendung bestimmter internetbasierter Dienste ermöglichen und erleichtern. Sie erkennen und stimmen zu, dass Microsoft berechtigt ist, die von Ihnen verwendete Version des Betriebssystemprodukts und/oder seiner Komponenten automatisch zu überprüfen und Updates oder Fixes des Betriebssystems bereitzustellen, die automatisch auf Ihren Computer gedownloadet werden.*", a.a.O., S. 86.

126 Punkt 18.3.3. des 32. Tätigkeitsberichts des Hessischen Datenschutzbeauftragten, vom 31.12.2003, a.a.O., (Fn. 124). Im BDSG ist an § 10 zu denken. Nach Simitis u. a., BDSG/*Ehmann,* § 10 Rd. 19 soll jedoch selbst dann keine Übermittlung von Daten bei einer Fernwartung vorliegen, wenn die Daten bekannt werden, *„da weder Gegenstand noch Zweck der Fernwartung ist, Daten mit ihrem Informationsgehalt der Wartungsfirma zu überlassen. Mangels Übermittlung ist somit auch kein Raum für die Anwendung von § 10."* Dem ist nicht zuzustimmen, da bereits die Möglichkeit der Wartungsfirma Kenntnis von den personenbezogenen Daten zu erlagen, das Risiko der unberechtigten Nutzung erhöht. Demnach müssen die Regelungen des § 10 für (Online-)Software-Updates herangezogen werden, insbesondere müssen die nach § 9 erforderlichen technischen und organisatorischen Maßnahmen festgelegt werden, vgl. § 10 Abs. 2 S. 2 Nr. 4 BDSG, d. h. insbesondere ist der Umfang der Zugriffsrechte zu bestimmen und zu begrenzen.

zubieten und es darf keine Abhängigkeit von einem praktisch unkontrollierten Zugriff auf den Zielrechner bestehen.[127]

II. Reaktionspflichten des Nutzers

Ist der Nutzer über Sicherheitslücken, insbesondere über die Möglichkeiten der Wiederherstellung der Sicherheit informiert, so könnte ihn die Obliegenheit treffen, die Informationen zugunsten der Sicherheit auch zu verwerten. Versäumt er dies, so hat er unter Umständen seiner Schadensminderungspflicht nach § 254 Abs. 2 S. 1 BGB nicht genüge getan.

Bei Beschädigungen einer Sache erfordert die Schadensminderungspflicht des Nutzers, die Schäden möglichst gering zu halten.[128] Gedanklich kann eine Schadensabwendungs- oder -minderungspflicht bei Softwarefehlern von der Deinstallation des Programms bis zum Bezug eines Updates reichen.[129]

Dieser kursorische Ausblick mag an dieser Stelle der Arbeit genügen. Ausführlicher zu den Obliegenheiten des Nutzers im Sinne einer Reaktionspflicht unter Kapitel 5 C IV.

E Ergebnis

Es wurde festgestellt, dass Information durch die Elemente Vorgang, Zustand und Inhalt gekennzeichnet werden können. Die Relevanz dieser Elemente für die Frage nach den Informationsrechten und –pflichten bei Sicherheitslücken spiegelt sich in folgenden Punkten wieder.

Das Ziel eines IT-Informationsrechts ist der Ausgleich von ungleichen Informations(zu)ständen (Informationsasymmetrien). Dieser ist durch das Spannungsverhältnis zwischen der Informationsasymmetrie und den Interessen an Geheimhaltung geprägt. Insoweit erfordern Informationsrechte und –pflichten eine Abwä-

---

127 Vgl. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07.08.2003 zum automatischen Software-Update, http://www.datenschutz-berlin.de-/doc/de/konf/65-66/update.htm (30.05.2006). Eine ähnliche Erklärung ist auf internationaler Ebene abgegeben worden: „Resolution on Automatic Software Updates", 25th International Conference of Data Protection & Privacy Commissioners Sydney, 12.09.2003, http://www.privacy.gov.au/news/ressof_print.html (30.05.2006).

128 Erman-*Kuckuk* § 254 Rd. 68.

129 Spindler, Das Jahr 2000-Problem, in: NJW 1999, 3737 (3744) der eine Pflicht zum Erwerb eines Updates zur Schadensabwendung zu recht ablehnt.

gung. In diese Abwägung sind insbesondere die Aspekte des Non oder Full-Disclosure und das Sicherheitsbewusstsein und die Sicherheitserwartung der Nutzer einzustellen.

Die Debatte um Non oder Full-Disclosure steht für einen Informationsvorgang, in dem die Ambivalenz von Information für die Sicherheit Berücksichtigung findet.

Der Informations(zu)stand der Akteure besitzt in der Ausprägung als Sicherheitsbewusstsein und Sicherheitserwartung Relevanz für die Haftung. Während das Sicherheitsbewusstsein als Voraussetzung für die Sicherheitserwartung betrachtet werden kann, kann eine niedrige Sicherheitserwartung nicht zuletzt Einfluss auf die Haftung für Sicherheitslücken haben. Im Rahmen der deliktischen Haftung orientiert sich etwa die Verkehrssicherungspflicht an den Sicherheitserwartungen der betroffenen Verkehrskreise. Ein Leitbild des Durchschnittsnutzers, das zusätzlich der Zuweisung von Verantwortung und der Schutzsphärenverteilung bei der Haftung dienen könnte, ist für das Internet nicht feststellbar.

Eine besondere Form des Informationsinhaltes – und letztendlich Ziel von Informationsrechten und –pflichten bei Sicherheitslücken – ist das Schließen der Lücke mittels Updates und Patches.

KAPITEL 4 ZUM BEITRAG VON RECHT UND INFORMATION ZUR STEUERUNG DER SICHERHEIT IM INTERNET

Die Qualität und Reichweite des Beitrags von Recht und Information zur tatsächlichen Förderung und Erhöhung der Sicherheit im Internet wird zum einen durch die Möglichkeit und Grenzen der rechtlichen Steuerung im Allgemeinen bestimmt und ist zum anderen den Spezifikationen des Gegenstandes Internet und der Sicherheit im Besonderen geschuldet.

Zunächst soll die Qualität eines Beitrags des Rechts zur Sicherheit im Allgemeinen unter den Aspekten der Steuerungswirkung und –instrumenten dargelegt werden, bevor die Reichweite dieses Beitrags im Internet diskutiert werden kann.

A Zur Steuerung durch Recht und Information

Warum überhaupt die Frage nach und Diskussion der „Steuerung der Sicherheit im Internet"? Das Internet ist, wie gezeigt, aus vielen Elementen zusammengesetzt und variiert zusätzlich durch Entscheidungen der Akteure über die Rahmenbedingungen und Komponenten der Nutzung[1]. Das Internet ist demnach keine einzelne „Technologie", die monokausal ergründbar ist, sondern ein Konglomerat aus „Technologien", die unterschiedliche Aufgaben zu erfüllen haben.[2] Demnach könnte für das Internet gelten:

> *„Was nicht mehr beherrscht, was nicht länger determiniert werden kann, soll beeinflusst und gelenkt, gesteuert werden."*[3]

Während Beherrschung der erreichte Zustand einer zielgerichteten und linearen Einwirkung ist, ist Steuerung ein Prozess, der auch ermöglicht, indirekt auf das zu erreichende Ziel einzuwirken.

---

1 Diese Entscheidungen beginnen mit der Zusammensetzung der Soft- und Hardwarekomponenten beim Nutzer, die Modalitäten der Nutzung, LAN oder WAN/GAN, Einsatz einer Firewall und enden etwa mit der Wahl von Übertragungsweg und –technologie.

2 Diese Feststellung ist nicht nur für die Frage der Steuerung relevant. Vor der Steuerung stellt sich die Frage der Technikfolgenabschätzung, die mit dieser Bewertung des Internets allenfalls auf einem sehr abstrakten Niveau möglich ist, vgl. Roßnagel, Rechtswissenschaftliche Technikfolgenforschung, 1993, S. 84 f.

3 Di Fabio, Technikrecht – Entwicklung und kritische Analyse, in: Vieweg (Hrsg.), Techniksteuerung und Recht, 2000, S. 9 (12), der das Zitat auf primär auf die Wirtschaft in der Weltgesellschaft bezieht.

I. Steuerungswirkung

1. Begriff

Um der Antwort auf die Frage, wer oder was das Internet (durch Recht) beeinflusst oder beeinflussen könnte, näher zu kommen, können begrifflich neben der Steuerung die Aspekte der Verwaltung, Regierung, Regulierung oder in Betracht gezogen werden. Die Arbeit zieht den Begriff der Steuerung vor, da die Aspekte der Verwaltung, Regierung und Regulierung nicht die vergleichbare Reichweite und Nuancen besitzen.

Die *„Verwaltung des Internets"*[4] wird auf die ICANN[5] und ihre Aufgaben konzentriert. Als rein technisches Mandat betrifft dies die Domainvergabe, die Domaingenerierung und die Standardisierung im DNS. Regierung ist mit der Idee der Nationalstaaten verbunden. Eine Regierung des „grenzenlosen" Internets mutet daher vermessen an. Regulierung ist fokussiert auf den gegenständlichen Teilaspekt der Förderung und Sicherstellung des Marktes.[6]

Steuerung ist die Beeinflussung eines so nicht gewünschten Zustand (Ist-Zustand). Sie zielt – so die Ausgangsthese – auf die Herstellung eines bestimmten Regelzustandes (Soll-Zustandes)[7] und kann als Gestaltung eines Prozesses verstanden werden.[8] Dieser Aspekt wird auch im alltäglichen Sprachgebrauch deutlich. Man kann

---

4 Etwa: Proksch, Internet Governance – Die Verwaltung des Internet, 2001, http://www.it-law.at/papers/proksch-internet-governance.pdf (30.05.2006); Mitteilung der Kommission, Organisation und Verwaltung des Internet Internationale und europäische Grundsatzfragen 1998 – 2000, vom 11.04.2000, KOM(2000) 202; so etwa auch die Ausrichtung bei: Reinermann (Hrsg.), Regieren und Verwalten im Informationszeitalter, 2000. International wird die „Internet Governance" diskutiert und - zumeist fokussiert auf den Aspekt der technischen Verwaltung des Internets - auf das DNS, das IP und die Root Server reduziert, vgl. Kleinwächter, Wolfgang, How WSIS tries to enter new territory of Internet Governance, vom 11.03.2004, http://www.unicttaskforce.org/perl/documents.pl?id=1294 (30.05.2006). Diese Bereiche entsprechen dem technischen Mandat der ICANN.

5 Internet Cooperation for Assigned Names and Numbers.

6 Im Gesetz wird der Begriff der Regulierung etwa in § 2 TKG verwandt. Regulierung im Sinn des § 2 Abs. 2 TKG will den Wettbewerb fördern, sicherstellen und Interessen wahren. Regulierung kann somit pointiert als Verbesserung und Eingriff in den Markt bezeichnet werden.

7 Diesen Prozess als Differenzminderung der Steuerung bezeichnend, Schulte, Techniksteuerung durch Technikrecht, in: Vieweg (Hrsg.), Techniksteuerung und Recht, 2000, S. 23 (28).

8 So auch: Schulz, Regulierte Selbstregulierung im Telekommunikationsrecht, in: Berg/Fisch/Schmitt Glaeser/Schoch/Schulze-Fielitz (Hrsg.), Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, in: Die Verwaltung, Beiheft 4, 2001, S. 101 (101).

auf ein bestimmtes Ziel hin steuern, aber man regelt eine Sache. Dieser prozessorientierte Charakter der Steuerung entspricht dem Kontext des dynamischen Internets und dem schwer fass- und erreichbaren Ziel der Sicherheit und ist demnach den weniger aussagekräftigen Begriffen vorzuziehen.

Die Fragen der staatlichen Steuerung versuchen verschiedene Disziplinen wie Politikwissenschaft, Wirtschaftswissenschaften, Sozialwissenschaft, Staats- und Verwaltungswissenschaft und die Rechtswissenschaft zu beantworten.[9]

Die Sozialwissenschaft hält verschiedene Aspekte der Steuerung bereit. Dies sind Aspekte, die auch in einer rechtlichen Betrachtung der Systematisierung zu Grunde gelegt werden können, ohne eine Vorstellung eines Steuerungsbegriffs abschließend zu konturieren und vorwegzunehmen.[10] Sie dienen der sprachlichen Darstellung und Vermeidung von Unklarheiten. Eine Auseinandersetzung mit der Vielfalt und Differenziertheit der sozialwissenschaftlichen Diskussion, insbesondere mit dem Einfluss der Systemtheorie auf die Steuerungsdebatte, soll hier nicht stattfinden. Vielmehr sollen, was für diesen Kontext ausreichend erscheint, lediglich einige Aspekte zu Grunde gelegt werden.

Bausteine einer Architektur des Steuerungsbegriffs sind das Steuerungssubjekt, -objekt, -ziel und -wissen.[11] Diese begriffliche Klärung von Mayntz kann durch die Steuerungsfähigkeit, -medien und -instrumente ergänzt werden und erscheint daher für den weiteren Verlauf der Arbeit am zweckmäßigsten. Weitere Bausteine ergeben sich aus den Fragen, die man mit der Steuerung eines Systems verbindet, etwa der Steuerungsfähigkeit oder Steuerbarkeit.

Die Steuerung bedarf zunächst eines Steuerungssubjekts (oder –akteurs), das ein Steuerungsobjekt lenken will. Steuerungssubjekt ist der Staat. Mit dem Recht befasst und das Recht formend sind Gesetzgebung, Rechtsprechung und Verwaltung.

---

9 In der sozialwissenschaftlichen Diskussion wurde der Begriff Steuerung erst Beginn der siebziger Jahre vermutlich zur Übersetzung des angelsächsischen „control“ eingeführt. Vgl. Mayntz, Politische Steuerung, in: Ellewein/Hesse/Mayntz/Scharpf (Hrsg.), Jahrbuch zur Staats- und Verwaltungswissenschaft, 1987, S. 89 (91 f.).

10 Im rechtlichen Kontext gibt es zwar auch Begriffe, wie etwa in der Gesetzgebung Gesetzgeber, Gesetz, Kompetenz, Rechtsgrundlage oder in der Rechtsprechung das streitige Rechtsverhältnis des Klägers und der Beklagten, das mittels Urteil geregelt wird. Diese Begriffe bestimmen jedoch Details und erlauben keinen Blick auf das Ganze. Durch die Verwendung disziplinfremder Strukturierungsangebote kann eine Adlerperspektive vielleicht gelingen.

11 Mayntz, a.a.O., (Fn. 9), S. 89 (93 f.), die einen handlungs- und keinen systemtheoretisch orientierten Steuerungsbegriff vertritt.

Als Steuerungssubjekt kommen demnach nicht nur die Gesetzgeber[12], sondern auch die Verwaltung und Gerichte in Betracht.[13]

Steuerungsobjekt können die Gesellschaft, der Einzelne und Organisationen sein.[14] Teilweise wird vertreten, dass sich Organisationen als Steuerungsobjekte besser durch Recht steuern lassen als Individuen.[15] Organisationen seien

> *„wegen der sie kennzeichnenden strukturellen und prozeduralen Gegebenheiten tendenziell rationaler in ihren Handlungsweisen und deshalb berechenbarer und steuerbarer als Individuen."*[16]

Steuerungsziel ist hier die Sicherheit im Internet. Zur Erreichung seines Ziels bedient sich das Steuerungssubjekt eines oder mehrerer Steuerungsmedien. Staatliche Steuerungsmedien sind etwa Macht, Geld, Wissen oder Information und Recht. Der Einsatz dieser Medien kann durch seine wechselseitigen Bezüge gekennzeichnet sein und kann mit unterschiedlichen Steuerungsinstrumenten realisiert werden.

Welche Aspekte die Steuerung im Kontext des Rechts charakterisieren und welches die Herausforderungen an die Steuerung durch Recht sind, wird im Folgenden dargelegt.

2. Aspekte der Steuerung

a) Aspekt Steuerungsprozess

Ausgangspunkt der weiteren Überlegungen ist das Verständnis von Steuerung als Lenkung, Eingreifen oder Setzen von Grenzen.[17] Dieses Hinwirken auf Wirkungen

---

12 Der Plural ist den verschiedenen Rechtsordnungen geschuldet, auf internationaler Ebene, im Europa-, Bundes und Landesrecht.

13 Anders Schuppert, der bei der Betrachtung der Steuerung des Verwaltungshandelns durch Verwaltungsrecht den Gesetzgeber als einziges Steuerungssubjekt benennt und etwa die steuernde Wirkung von Urteilen des Verwaltungsrechts nicht erwähnt. Schuppert, Verwaltungswissenschaft als Steuerungswissenschaft, in: Hoffmann-Riehm (Hrsg.), Reform des allgemeinen Verwaltungsrechts, 1993, S. 65 (69).

14 Ein Bezug von Steuerungssubjekt und Steuerungsobjekt unterbindet den Gebrauch des Begriffes der Selbststeuerung oder -regulierung. Demnach scheint das Internet als Beispiel der *„Selbstregulierung"* (so: Holznagel, Regulierte Selbstregulierung im Medienrecht, in: Berg/Fisch/Schmitt Glaeser/Schoch/Schulze-Fielitz (Hrsg.), Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, in: Die Verwaltung, Beiheft 4, 2001, S. 81 (82)) nicht mit diesem Ansatz fassbar.

15 Derlien, Staatliche Steuerung in Perspektive, in: König/Dose (Hrsg.), Instrumente und Formen staatlichen Handelns, 1993, S. 503 (508 f.).

16 König/Dose, Referenzen staatlicher Steuerung, in: dies. (Hrsg.), Instrumente und Formen staatlichen Handelns, 1993, S. 517 (524).

kann in einer komplexen Gesellschaft nicht als lineare Kausalkette gedacht werden. Deshalb ist Steuerung häufig ein Handeln unter und mit Ungewissheit.[18] Ungewiss nicht zuletzt deshalb, weil die Steuerung sich durch verschiedene über eine Zeit erstreckende Handlungszusammenhänge realisiert (Steuerungsprozess).[19] Zur Erlangung von Sicherheit mag ein Handeln mit Ungewissheiten/Unsicherheiten paradox bis kontraproduktiv gelten. Solange aber kein „Patentrezept" im Sinne einer Regelung im engeren Sinn existiert, wird Sicherheit nur unter dem Primat des (selbstlernenden) Steuerungsprozesses zu erreichen sein.

Ein Prozess kann in personeller Hinsicht ein zufälliges oder gewolltes und bewusstes Zusammen- oder Entgegenwirken von Akteuren bedeuten. Solche möglichen Interaktionen oder Konflikte sind in der Wirkung der Steuerung abzuschätzen. Nichts desto trotz kann eine Zielführung des Steuerungsprozesses durch die Implementierung von Einfluss- und Kontrollmechanismen optimiert werden.

Das primäre Kriterium des Prozesses impliziert die weiteren Kriterien wie Anreiz, Autorität und Verantwortung, welche in dieser Arbeit dem Begriff der Steuerung zu Grunde gelegt werden sollen.

b) Aspekte Anreiz, Autorität und Verantwortung

Die lateinische Wurzel des „gubernare"[20] (ein Schiff steuern, lenken) bietet die Chance zur Bildung einer weiter führenden Diversifizierung. Diese Wurzel zeigt die Notwendigkeit der Interaktion zweier Akteure, des Schiffsführers und der Mannschaft und erschließt weitere Aspekte der Steuerung. Steuerung beinhaltet einen Anreiz (zur Umsetzung der Befehle des Schiffsführers). Anreize können zur Motivation durch Regelungen verbindlich gesetzt und unterstützt werden oder etwa durch ein *„Informations- oder Überzeugungsprogramm"*[21] empfohlen werden (Anreiz im engeren Sinn). Grenzen des verbindlichen Anreizes sind intendierte Verhalten, bei denen es auf Eigeninitiative, Innovation oder persönliches Engagement ankommt.

---

17 Diese Bedeutungen sind kontextgerecht der alltagssprachlichen Verwendung des Begriffes extrahiert. In der alltagssprachlichen Verwendung nimmt zudem der technische Zusammenhang (etwa ein Auto steuern) einen Platz ein.

18 Hoffmann-Riehm, Verwaltungsrecht in der Informationsgesellschaft, in: Hoffmann-Riehm/Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 9 (13).

19 Mayntz, a.a.O., (Fn. 9), S. 89 (93).

20 Gubernare hat mit kybernan eine griechische Wurzel und ist damit ein griechisches Lehnwort im Lateinischen.

21 Mayntz, a.a.O., (Fn. 9), S. 89 (98).

Steuerung ist ein Anreiz und bleibt lediglich ein Anreiz, wenn die Autorität und Verantwortung des Schiffsführers fehlt. Autorität und Verantwortung sind Motivation und Mittel zur Durchsetzung des Steuerungswillens. Der fremde Steuerungsanreiz kann zu einer eigenen Motivation werden, wenn Autorität und Verantwortung geteilt werden. Oben genannte Grenzen des Anreizes könnten so eventuell überwunden werden. Übertragen auf gesellschaftliche Vorgänge finden diese Überlegungen etwa Eingang bei der Privatisierung, der (regulierten) Selbstregulierung, Public-Private-Partnerships oder – im angelsächsischen Raum – Private Ordering[22].

c) Aspekt Information/Wissen

Der Aspekt sei an dieser Stelle nur der Vollständigkeit halber erwähnt, im weiteren Verlauf der Arbeit[23] wird er ausführlich diskutiert.

Der Erfolg des Steuerungsprozesses hängt zum einen von der normativen oder faktischen Durchsetzungskraft des Anreizes und zum anderen vom Steuerungswissen des Akteurs ab. Unzureichendes Wissen oder Information kann das (gezielte) Einsetzen von Steuerungsinstrumenten verhindern. So kann etwa im Bereich der Sicherheit erst das Wissen um die (technischen) Gefahren für das Rechtsgut eine Regelung evozieren. So wie das Wissen des Steuerungssubjekts für den Erlass der Regelung, ist das Wissen des Objektes um die Regelung unerlässlich. In welchem zeitlichen Abstand das Steuerungsobjekt mit diesem Wissen um das Steuerungsinstrument zur Realisierung der Steuerungswirkung vertraut wird, ist abhängig vom Inhalt der Regelung. So ist es bei staatlichen Warnungen vor einer Gefahr für die Wirkung zwingend erforderlich, dass das Steuerungsobjekt vor Realisierung der Gefahr ex ante von der Warnung „weiß". Bei einem einschränkenden Verbot etwa kann das Steuerungsziel auch mit ex post-„Wissen" erreicht werden, solange die Autorität zur Durchsetzung besteht.

Wissen ist eine Variable des Steuerungsmediums Recht und kann, wie folgt, als Information auch ein eigenständiges Steuerungsmedium sein. Im Folgenden sollen die Steuerungsmedien Recht und Information als Medien der Techniksteuerung betrachtet werden.

---

22 Schwarcz, Private Ordering, Northwestern University Law Review Vol. 97, No. 1 S. 319-349.

23 Vgl. Kapitel 4 A II. 3.

II. Recht und Information als Medien der Techniksteuerung

1. Steuerungsmedien

Es lassen sich neben dem Recht im Wesentlichen drei staatliche Steuerungsmedien ausmachen: Macht, Geld und Wissen.[24] Die Arbeit bleibt ob des gewählten Themas auf die Medien Recht und Wissen fokussiert.

Dem Einwand, dass Recht logisch nicht in die Reihe der Steuerungsmedien passt, da das staatliche Handeln in der Regel rechtsförmig verläuft,[25] kann entgegen gehalten werden: Zum einen wird die Entscheidung des legislativen „Ob" nicht erfasst, zum anderen wird eine lediglich mittelbare Steuerung betrachtet, wenn die steuernde Regelung nicht einbezogen wird. Letzterer Aspekt beruht auf der Vorstellung, dass letztendlich alles staatliche Handeln auf Recht zurückzuführen ist. *„Überspitzt kann man von einer verrechtlichten Welt sprechen."*[26] Das Steuerungsmedium Recht soll in dieser Phase der Arbeit auf abstrakter Ebene diskutiert werden, ohne bereits hier den spezifischen Beitrag des Rechts darlegen zu müssen.[27] Der Zusammenhang von Steuerung und Recht wird zunächst auf der Ebene des Staates gesehen. Dem Staat, der selbst durch das Recht konturiert und reglementiert ist und der das Recht konturiert und anwendet, kann eine Steuerung durch Recht zugestanden werden. Dies

---

24 Vgl. Grothe, Restriktionen politischer Steuerung des Rundfunks, 2000, S. 137 mit weiteren Hinweisen. Vgl. auch König/Dose, Klassifikationsansätze zum staatlichen Handeln, in: dies. (Hrsg.), Instrumente und Formen staatlichen Handelns, 1993, S. 3 (118 f.), mit einer anderen Terminologie (Steuerungsmedium und –instrument sind begrifflich „vertauscht") werden als externe Steuerungsinstrumente Macht, Geld und Information genannt. Des Weiteren Voigt, Staatliche Steuerung aus interdisziplinärer Perspektive, in: König/Dose (Hrsg.), Instrumente und Formen staatlichen Handels, 1993, S. 298 (309), der zudem Moral als Steuerungsmedium bezeichnet, dem Recht in westlichen Industriestaaten aber eine herausragende Rolle einräumt.

25 Grothe, a.a.O., (Fn. 24), S. 138.

26 Vieweg, Technik und Recht, in: Vieweg/Haarmann (Hrsg.), Beiträge zum Wirtschafts-, Europa- und Technikrecht, S. 199 (199).

27 So auch Schuppert mit den einleitenden Worten der zur immensen Fülle der Literatur in der Steuerungsdebatte und der darauffolgenden theoretischen Abhandlung zum Steuerungsbegriff und Steuerungstypologien, um den Vorwurf der Theorielosigkeit zu entgehen. Vgl. Schuppert, Verwaltungswissenschaft als Steuerungswissenschaft, in Hoffmann-Riehm (Hrsg.), Reform des allgemeinen Verwaltungshandelns, 1993, S. 65 (67).

entspricht dem Leitbild des „starken Staates“, der die Quelle der Steuerung durch Recht ist.[28]

Dem Verhältnis des Steuerungsmediums Wissen und Recht ist eine wechselseitige Beziehung immanent. Entsprechend dem oben dargelegten Verständnis von Information kann das Medium im Weiteren als Information bezeichnet werden. So kann eine Gesetzgebung ohne vorherige Sach- und Detailinformation über das zu regelnde Gebiet vernünftigerweise nicht erfolgen. Mangelndes Wissen ist eine Sperre für jedes rationale staatliche Handeln. Durch diese ambivalente Beziehung zum Recht erhalten Wissen und Information eine eigene Qualität, die es rechtfertigt, von einem Steuerungsmedium zu sprechen, auch wenn diese teilweise nur Mittel zum Zweck sind und vorbereitende Handlungen auf die rechtliche Steuerung darstellen.

Die Generierung und Akzelerierung von Wissen durch den Staat kann zum einen durch die Einstellung entsprechenden Personals und zum anderen durch ein entsprechendes Wissensmanagement erfolgen. Das Steuerungsmedium Information erhält seine Qualität durch die staatliche Generierung einerseits und die staatliche Zuteilung und Verbreitung von Wissen andererseits. Die Faktoren Wissen und Information könnten letztlich sogar die staatliche Steuerungskompetenz in Frage stellen. Diese läge dann dort, wo das jeweils relevante Entscheidungswissen für ein Problem gegeben ist.[29] Im Rahmen der Gesetzgebung kann dies zu einer Divergenz von Steuerungskompetenz und Rechtssetzungskompetenz führen.

Neben den staatlichen Steuerungsmedien besteht der Markt[30] als Steuerungsmedium. Dieser „agiert“, wenn die staatlichen Steuerungsmedien nicht oder nur teilweise (Regulierung) eingesetzt werden. Im Falle der Sicherheit zeigt sich die Steuerungskraft des Marktes etwa in der Nachfrage der Nutzer und Verbraucher nach Sicherheitsaspekten der Produkte. Teilweise wird eine Steuerungswirkung des Marktes abgelehnt, da dieser ein Abstimmungsprozess zwischen Angebot und Nachfrage sei und somit mehr koordiniere, als eine eigenständige gerichtete Wir-

---

28 So auch Kaufmann, der differenziert zwischen den Staaten des Common Law und Kontinentaleuropa. Durch den Anspruch an ein widerspruchsfreies Rechtssystem ist in den Rechtssystemen Kontinentaleuropas eine Infrastruktur geschaffen worden, die eine vergleichsweise höhere staatliche Steuerungskapazität vermuten lässt. Kaufmann, Steuerung wohlfahrtsstaatlicher Abläufe durch Recht, in: Grimm/Maihofer (Hrsg.), Gesetzgebungstheorie und Rechtspolitik, 1988, S. 65 (72).

29 So Grothe, a.a.O., (Fn. 24), S. 142. Dies wäre der Fall, wenn man diese als nicht originär beim Staat begreife, sondern dort, wo das jeweils relevante Entscheidungswissen liegt.

30 Vgl. Mayntz, die eine Akteurqualität des Marktes ablehnt, Mayntz, a.a.O., (Fn. 9), S. 89 (91).

kung zu besitzen.[31] Auf eine eigenständige Steuerungswirkung des Marktes zielen aber letztendlich die Regulierungsversuche durch Recht ab, Wettbewerb zu schaffen. Ist dieser Zustand erreicht, bedarf es idealiter keine Steuerung durch Recht mehr.

Vorab sollen zunächst die Steuerungsmedien Recht und Information im Hinblick auf ihren Einsatz im Bereich der Technik im Allgemeinen konturiert werden. Bevor die Chancen der Information zur Steuerung der Sicherheit des Internets im nächsten Kapitel im Konkreten entwickelt werden, soll im nächsten Schritt die Steuerung des Internets als Teil der Technik im Besonderen betrachtet werden.

2. Steuerung durch Recht

a) Aspekte der Steuerung durch Recht

Ausgehend von den Aspekten, unter denen die Steuerung des Internets untersucht werden kann, kann zwischen staatlichem und nicht-staatlichem Akteur der Steuerung unterschieden werden. Das Schrifttum zur Steuerung durch Recht befasst sich hauptsächlich mit der Steuerung durch den Staat. Auf den ersten Blick drängt sich eine Steuerung durch Recht durch nicht-staatliche Akteure nicht unbedingt auf. Unvoreingenommen erscheint dies nicht möglich, da nicht-staatliche Akteure keine Entscheidungsgewalt über das Recht als Steuerungsmedium haben. Dem kann mit Schuppert entgegengehalten werden, dass das Recht auch eine Bereitstellungsfunktion besitzt.[32] Hiervon ausgehend müsse es möglich sein, dass eine Steuerung durch Recht von Akteuren erfolgt, die zwar selbst keine Rechtsetzungsgewalt haben, denen eine Steuerung durch das Recht durch die Elemente des Rechtsgerüstes aber ermöglicht werde. Voraussetzung sei, dass der Akteur selbst Rechtsubjektqualität besitzt, damit er vom Recht erfasst werden kann.

Eine notwendige, differenzierte Betrachtung zwischen staatlichen und nicht-staatlichen Akteuren indiziert die Wirklichkeit des Internets, die auch von nicht-

---

31 König/Dose, Referenzen staatlicher Steuerung, in: Dies. (Hrsg.), Instrumente und Formen staatlichen Handelns, 1993, S. 519 (520).

32 Schuppert kommt hierzu, nachdem er Beiträge von Kaufmann und Ritter zur Steuerung durch Recht rezipierte. Von Kaufmann listete er Normierungstypen des Rechts auf, und beschäftigte sich im Anschluss mit Ritters Rechtsgerüst. Aufgrund der Voraussetzungen, die das Recht für eine Steuerung zu bieten hat, folgert er eine Bereitstellungsfunktion des Rechts: Schuppert, Verwaltungsrechtswissenschaft als Steuerungswissenschaft, in: Hoffmann-Riem (Hrsg.) Reform des allgemeinen Verwaltungsrechts, 1993, S. 65 (93 ff., 96 f.).

staatlichen Akteuren gestaltet wird. Für staatliche und nicht-staatliche Akteure gelten jedoch unterschiedliche Machtbegrenzungen und Legitimationsprinzipien.[33]

Der Erfolg anderer staatlicher Steuerungsmedien hängt zum einen von der Verfasstheit der Steuerungsobjekte ab, zum anderen wird die Wirksamkeit von einem vielfach vorstrukturierten Handlungsfeld beeinträchtigt.[34] Für eine staatliche Steuerung durch Recht kann dies nur bedingt gelten, da durch das Recht die Handlungsfelder selbst strukturiert werden und so der Boden für den Erfolg der Steuerung vorbereitet werden kann. Teilweise vermag jedoch auch das nationale Recht das Handlungsfeld – etwa bei multinationalen Konzernen – nicht abzustecken und zu konturieren.

aa) Recht als staatliches Steuerungsmedium

Im Kontext von Recht und Technik zielt die Steuerung auf den Schutz von Rechtsgütern und hat dabei das Ziel, *„die Rechtsverträglichkeit technischer Systeme sicherzustellen“*[35] – Recht zum Schutz vor Technik. Daneben soll das Recht die Technik auch unterstützen und ermöglichen – Recht zum Schutz der Technik.

Ein Beispiel für die Schwierigkeit der Verwirklichung dieser ambivalenten Ziele kann der Kommentierung zu Art. 12 der Bremer Verfassung entnommen werden. Dieser Artikel ist ein Beispiel einer „verfassungsrechtlich garantierten Sicherheit“ vor Technikfolgen;[36] vgl. Art. 12 der Verfassung der Freien Hansestadt Bremen vom 21.10.1947:

„Der Mensch steht höher als Technik und Maschine.

---

33 Brohm, in Isensee/Kirchhof (Hrsg.) HbdStR II, § 36, Rn. 36.

34 Voigt, Staatliche Steuerung aus interdisziplinärer Perspektive, in: König/Dose (Hrsg.), Instrumente und Formen staatlichen Handels, Köln, 1993, S. 289 (297).

35 Roßnagel, Rechtswissenschaftliche Technikfolgenforschung, 1993, S. 241. Die zentrale These ist, dass die Technik die Gesellschaft ungeplant beeinflusse. Um negativen Entwicklungen vorzubeugen, solle unerwünschte Technik schon relativ frühzeitig von der Gesellschaft getrennt werden. Weitere Ansätze sollen die Technikfolgenabschätzung (in einer zunächst abwartenden Haltung können die Folgen der Technik für die Gesellschaft analysiert werden.) und der Bottom-up Ansatz sein (die „beste“ Technik setzte sich durch Annahme und Verbreitung in der Gesellschaft durch.), vgl. Müller, Enthält die Informatik Sprengkraft für Regulierungssysteme?, in: Bizer/Lutterbeck/Rieß (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft, 2002, S. 93 (99). Diese können durch einen Top-down Ansatz (jeder Technikentwicklung geht die Erstellung von Anforderungen voraus) ergänzt werden.

36 Neumann, Die Verfassung der Freien Hansestadt Bremen, Kommentar, 1996: Art. 12 Rd. 2 und 6: Art. 12 Abs. 1 LV sei eine verfassungsrechtliche Wertentscheidung und konkretisiere die Menschenwürde. Art. 12 Abs. 2 LV normiere verfassungsrechtlich garantierte Ingerenzrechte.

Zum Schutz der menschlichen Persönlichkeit und des menschlichen Zusammenlebens kann durch Gesetz die Benutzung wissenschaftlicher Erfindungen und technischer Einrichtungen unter staatlicher Aufsicht und Lenkung gestellt sowie beschränkt und untersagt werden."

Diesem *„Primat des Menschen gegenüber der Technik (…) bei der Gesetzgebung praktische Gestalt zu geben"*[37] falle schwer, da es regelmäßig nicht möglich sei, bei technischen Sachverhalten Anforderungen an die Sicherheit detailliert festzulegen.[38] Zudem könne die Rechtmäßigkeit des Weges, Sicherheit durch staatliche Aufsicht nach Art. 12 Abs. 2 herzustellen, bezweifelt werden.[39]

Inspiriert von den Grundrechten kann an die freiheitsgewährende, die schützende und die abwehrende Funktion von Recht gedacht werden. Die Relation dieser Funktionen mit der Regelungsdichte kann folgendermaßen vereinfacht und thesenartig gedacht werden: Je eher Recht zum Schutz vor Technik eingesetzt werden soll, desto höher ist grundsätzlich die Regelungsdichte, da der Schutz von Rechtsgütern vielfältig ausgestaltet sein sollte, um überhaupt eine Regelungswirkung zu entfalten. Je eher eine Technik abgewehrt werden soll (Verbot), desto geringer ist die Regelungsdichte. Soweit Recht zum Schutz der Technik eingesetzt wird, erfordert es modifizierte Überlegungen, um die Technikentwicklung und Innovationen nicht grundsätzlich zu behindern oder zu unterbinden.

Dies macht deutlich, dass das Recht als Medium zur Steuerung einer Technik verschiedene Zielrichtungen besitzen kann. Darauf aufbauend kann das Recht näher konturiert werden, die Art des Rechts als zwingendes oder dispositives Recht, formelle und materielle Regelungen, Zweck des Rechts, etc.

bb) Technische Normung als (nicht)-staatliches Steuerungsmedium

Anders als bei den anderen Aspekten ist bei der technischen Normung die rechtliche Qualität zu hinterfragen. Dazu verurteilt *„Normzwischenschicht"*[40] zu sein, entsprechen technische Normen nicht der klassischen Gesetzesform.[41]

---

37 Neumann, a.a.O., (Fn. 36), Art. 12 Rd. 4.

38 BVerfG, Beschluss v. 08.08.1978 - 2 BvL 8/77, BVerfGE 49, 89 (134).

39 Neumann, a.a.O., (Fn. 36), Art. 12 Rd. 6: Art. 12 Abs. 2 LV könne die in Art. 5 Abs. 3 S. 1 GG garantierte Wissenschaftsfreiheit verletzten. Zum eine könne diese nur durch andere verfassungsrechtlich geschützten Rechtsgütern beschränkt werden, Art. 5 Abs. 3 S. 2 GG. Zum anderen gelte: *„Da der Gesetzesvorbehalt des Art. 12 Abs. 2 LV zu weit ist, ist die Vorschrift ungültig."*

40 Di Fabio, Verlust der Steuerungskraft klassischer Rechtsquellen, in: NZS 1998, 449, (452).

41 Die klassische Gesetzesform oder Rechtsquelle zeichnet sich nach Di Fabio durch legitimierte Subjekte, durch nachvollziehbare Verfahrensregeln beim Entstehen und durch Regeln über Anwendungs- und Geltungsvorrang aus. Di Fabio, Verlust der Steuerungskraft klassi-

Trotzdem kann an Formung von Recht gedacht werden, da ebenso wie der Rechtsprechung der Verwaltung die Anwendung und Konkretisierung[42] des Rechts mittels Heranziehung technischer Normung obliegt. Diese Konkretisierung wird als *„staatsentlastende Rezeption privaten, externen Sachverstandes"*[43] bezeichnet. Ob im Bereich der technischen Normung von einer Steuerung durch Recht (durch die inhaltliche Übernahme von und der Bezug im Recht auf technische Normen) gesprochen werden kann,[44] oder gar das Recht selbst gesteuert wird, ist fraglich und ist im Hinblick auf den Einfluss auf Individualinteressen wohl abzulehnen. Für den Bereich der technischen Normung kann festgestellt werden, vieles können Gesellschaft und Wirtschaft selbst erreichen und regeln. Um aber über Individualinteressen hinweg verbindliche Regeln erzwingen zu können, bedarf es des Machtmonopols und der Autorität der öffentlichen Gewalt.[45] Für den Bereich der Sicherheit, zugunsten derer nicht selten Individualinteressen eingeschränkt werden müssen, gilt dies umso mehr, als wichtige Bereiche der Infrastruktur betroffen sind.

In einem Verständnis von technischer Normung als *„halbstaatlichen Form der Regelsetzung und selbstregulativen Überwachung"*[46] findet sich die Überschneidung von privater und staatlicher Tätigkeit ausgedrückt.

Im amerikanischen Recht hat sich für das Internet, dem „Cyberspace", eine Lex Informatica[47] herausgebildet. Oder wie der amerikanische Rechtsprofessor Lessig es

---

scher Rechtsquellen, in: NZS 1998, 449, (450). Im Fall der technischen Normung fehlen (demokratisch) legitimierte Subjekte als Normgeber. Dies ergibt sich bereits aus der mangelnden Gesetzgebungskompetenz der Normungsgeber als privatrechtliche Vereinigungen. In diesem Sinne, Hess/Werk, Qualitätsmanagement, Risk Management, Produkthaftung, 1995, S. 140. Demnach sollen technische Nomen auch nicht wie demokratisch legitimierte Normen Allgemeinverbindlichkeit beanspruchen können, Kilian, Datensicherheit in Computernetzen, in: CR 1990, 73 (76).

42 Tatsächlich konkretisieren technische Normen die Sorgfaltspflichten des Herstellers, ohne allerdings eine abschließende Feststellung seiner Verantwortung zu treffen, Katzenmeier, Entwicklungen des Produkthaftungsrechts, in: JuS 2003, 943 (946); vgl. auch Leitsatz im BGH, Urteil v. 07.10.1986 - VI ZR 187/85, NJW 1987, 372 (372).

43 Vieweg, Technik und Recht, in: Vieweg/Haarmann (Hrsg.), Beiträge zum Wirtschafts- Europa- und Technikrecht, 2000, S. 199 (210).

44 So übernimmt in Österreich das Recht eine weitergehende Rahmenfunktion für die Gewährleistung der technischen Normung. In dem Bundesgesetz über das Normenwesen wird das Österreichische Normungsinstitut institutionell als Verein verankert, vgl. Bundesgesetz über das Normenwesen (Normengesetz) von 1971, BGBl. Nr. 240, S.1971.

45 Di Fabio, Technikrecht – Entwicklung und kritische Analyse, in: Vieweg (Hrsg.), Technik-steuerung und Recht, 2000, S. 9 (12).

46 Di Fabio, Risikosteuerung im öffentlichen Recht, in: Hoffmann-Riehm/Schmidt-Aßmann (Hrsg.), Öffentliches Recht und Privatrecht, 1996, S. 143 (162).

formuliert hat, *„Code is Law"*[48]. Der „Code" des Internets beruhe auf den die Auswirkungen der physikalischen und (techno)logischen Infrastruktur des Internets. Er könne demnach als bereichsspezifische faktische Normierung und Normung des Verhaltens der Nutzer angesehen werden.

cc) Rechtliche Aspekte anderer (nicht-)staatlicher Steuerungsmedien

Schließlich kann – unter der Prämisse, dass das Recht keinen, keinen abschließenden oder einen ungenügenden Beitrag zur Steuerung des Internets leistet (leisten kann) – die rechtliche Beurteilung anderer staatlicher Steuerungsmedien oder einer nicht-staatlichen Steuerung entwickelt werden. Diese Arbeit konzentriert sich exemplarisch auf Information.

Information ist zum einen, wie bereits dargestellt, ein Medium staatlicher Steuerung. Zum anderen kann Information als Informationspflicht eine rechtliche Steuerung sein. Die Frage ist, wie der rechtliche Rahmen für eine solche im Internet gesetzt werden kann. Allein einem Unternehmen Informationspflichten aufzuerlegen, kann im Bereich der Sicherheit im Internet als kontraproduktiv sein, wenn Sicherheitslücken offenbart werden, die somit auch eine Anleitung oder gar Aufforderung zum Ausnutzen derselben bieten. Eine Informationspflicht könnte daher, soweit möglich, mit der Pflicht zu verknüpfen sein, eine Abhilfemöglichkeit oder Patches[49] zu veröffentlichen. Fraglich ist allerdings, ob eine solche Informationspflicht nicht zu weit gehend bzw. überhaupt möglich ist.

Insoweit kann diese Betrachtung nicht trennscharf vom Recht als Steuerungsmedium an sich abgegrenzt werden. Mit dem Medium Information wird die Bedeutung des Rechts als Handlungsmaßstab des Staates und als „Handlungsaufforderung" an das Steuerungsobjekt betrachtet. Insoweit setzt das Recht einen Handlungsrahmen für den Staat als Steuerungsakteur und dem Steuerungsobjekt. Unter dem Ge-

---

47 In Anlehnung an die Lex Mercatoria, die entstanden im Mittelalter, heute die Funktion besitzen soll, aus Gründen der Rechtssicherheit und –klarheit und zur Vereinfachung des internationalen Handels internationale Handelsbräuche und vorherrschende Praktiken des internationalen Handels als Rechtsgrundsätzen oder Rechtsanschauungen aufzufassen. Die Rechtsnatur der Lex Mercatoria ist umstritten, MünchKomm/*Martiny,* EGBGB Art. 27 Rd. 31 ff. Teilweise wird die Lex Mercatoria als „autonomes Recht des Welthandels" begriffen, Pfeiffer, Welches Recht gilt für elektronische Rechtsgeschäfte, in: Jus 2004, 282 (283).

48 Lessig, Code and other Laws, 1999, S. 3ff., 6. Als „code" bezeichnet Lessig die Auswirkungen der Hard- und Software (inklusive Protokolle und Standards) auf das Verhalten der Nutzer im Cyberspace.

49 Patch (engl.) Flicken, im technischen Kontext kleine Programme, die Fehler in der Software beheben.

sichtspunkt der Initiative ist der Handlungsmaßstab initiativ-aktiv vom Staat gesetzt und fordert reaktives-aktives oder -passives Handeln des Staates (Pflicht und Recht zur Verbreitung und Sammlung von Information – oder bloße „Annahmestelle"). Die Handlungsaufforderung ist initiativ-aktiv vom Staat gesetzt und fordert reaktiv-aktives Handeln des Objektes (Pflicht und Recht zur Verbreitung und Sammlung von Information). Der Handlungsrahmen soll nicht als Initiierung, sondern als situativ-aktive Handlungsvorgabe für das Objekt begriffen werden.

b) Steuerungsinstrumente

Steuerungsinstrumente des Rechts können in „schwarz-weiß Manier" skizziert und in ex ante- und ex post-Instrumente eingeteilt werden. Weiter unterteilt finden sich etwa Auflagen, Verfahrensvorgaben oder Vorgaben für die inhaltliche Gestaltung von Rechtsgeschäften.[50] Diese Instrumente erfordern den Rückhalt von Autorität und die Durchsetzung der Verantwortung (Haftung). Setzen Instrumente durch Rechtsunverbindlichkeit oder Belohnungen Anreize, so sind sie dennoch nicht rechtsunerheblich, da sie in der Wirkung einem regulativen Instrument gleichstehen können.

Die Einteilung in ex ante und ex post ist für ein IT-Sicherheitsrecht jedoch nicht ausreichend. Diese Dichometrie lässt den prozesshaften Charakter der IT-Sicherheit außer Betracht. Dies soll an einem Beispiel verdeutlicht werden:

Ex ante kann das Recht – etwa in vertraglichen Vereinbarungen wie Allgemeine Geschäftsbedingungen – die Verwendung von Passwörtern vorgeben. Im Hinblick auf die Kommunikationssicherheit und Datensicherheit wird der Umgang mit Passwörtern regelmäßig mit dem Provider vertraglich geregelt. So schreiben etwa AGB häufig vor, dass Passwörter benutzt und zur Sicherheit in regelmäßigen Abständen geändert werden müssen.[51] Sollte der Kunde diese Vorgabe ex ante nicht einhalten, kann das Haftungsrecht ex post greifen, wenn das Passwort nicht geändert wurde oder von ungenügender Qualität ist.

---

50 Vgl. etwa Schuppert, Verwaltungswissenschaft als Steuerungswissenschaft, in: Hoffmann-Riem (Hrsg.), Reform des Allgemeinen Verwaltungsrechts, 1993, S. 65 (71 f.).

51 Dieses sinnvolle und aus Sicherheitsgründen notwendige Erfordernis wurde erst mit einer Revision der AGB (A. VI. 2.2.) der T-Online als Neuerung in diese aufgenommen und ist gültig ab dem 01.10.2004, ftp://software.t-online.de/pub/service/pdf/agbdiens.pdf (30.05.2006). Dies macht zugleich deutlich, dass die Umsetzung der technischen Sicherheit im Alltag schwierig ist.

Systeme sind jedoch nicht entweder sicher oder unsicher. Die Sicherheitslücke kann eine Realisierung und Ausprägung von Unsicherheit sein, muss es aber nicht. Solange eine Sicherheitslücke unentdeckt bleibt, kann ein System weiterhin als sicher gelten. Dementsprechend müssen Mechanismen zur Aufdeckung von Unsicherheiten etabliert werden,[52] die ein Ausnützen der „sicheren Unsicherheit“ [53] durch Dritte verhindern, damit die Sicherheit in der Anwendung (wieder)hergestellt werden kann. Im Hinblick auf die „sichere Unsicherheit“ stößt der Umgang mit der Information über Sicherheitslücken an die Grenzen des technisch Machbaren.

Konkret für das Beispiel heißt dies: Der Nutzer hat die Anforderungen ex ante hinsichtlich des Passwortes eingehalten. Ex post kann ihm im Fall eines Schadens kein Vorwurf gemacht werden. Ein Schaden, verursacht durch eine Sicherheitslücke, kann dann auftreten, wenn etwa das im Sinne der AGB als sicher geltende Passwort entschlüsselt werden kann. Im Fall des Szenarios 3 konnte das Passwort etwa durch eine Modifikation der URL erraten werden. Ex post können sich Haftungsregelungen mit den Folgen der Ausnutzung der Sicherheitslücke beschäftigen. Im Rahmen der Arbeit interessiert jedoch, welche Steuerungsinstrumente das Recht für die Zwischenzeit vorsieht, für den Zustand der schwebenden „sicheren Unsicherheit“ (diese ist gegeben, wenn die Sicherheitslücke offensichtlich noch nicht ausgenützt wird). Es bedarf Regelungen, die ein Ergebnis des Interessenausgleichs zwischen den Interessen des Anbieters und der Kunden vorgeben. Dem Anbieter droht ein Reputationsverlust bei Bekanntgabe der Sicherheitslücke, das Recht des Kunden auf informationelle Selbstbestimmung ist tangiert, wenn seine Daten eingesehen werden können.

Die Einteilung der Steuerungsinstrumente eines Sicherheitsrechts kann dementsprechend in zeitlicher Hinsicht konkretisiert werden durch eine Betrachtung „in operatione“. „In operatione“ kann als zentrale Phase im Umgang mit bestehenden Sicherheitslücken verstanden werden. In dieser Phase dient der Beitrag des Rechts dem Umgang mit der „sicheren Unsicherheit“ und somit nur mittelbar der Sicherheit, da er Handlungsoptionen für Dritte im Umgang mit den Sicherheitslücken eröffnet.

---

52 Solche Mechanismen müssen vor allem auf eine rasche Aufdeckung von Sicherheitslücken zielen. Idealiter sollten sie greifen, und die Sicherheitslücke behoben werden, bevor sie ausgenutzt werden kann. In diesem Sinne auch Schneier, *„Detection is much more important than prevention.“*, Schneier, Secrets & Lies, 2000, S. 374. Der wenig später allerdings einräumt: *„On the Internet, detection can be a lot of work.”*, a.a.O., S. 375.

53 Vgl. Kapitel 3 B.

Auf diese Betrachtung konzentrieren sich auch die Ausführungen der Arbeit. Soweit die Betrachtung sich auf ein so verstandenes Sicherheits-Informationsrecht konzentriert, finden sich kaum normierte Regelungen.[54] Im europäischen Recht ist als ein Beispiel Art. 4 Abs. 2 der elektronischen Datenschutzrichtlinie[55] zu nennen. Soweit danach ein besonderes Risiko der Verletzung der Netzsicherheit besteht, muss der Betreiber die Teilnehmer über dieses Risiko unterrichten.

Ein weiterer sicherheitsrelevanter Aspekt eines geeigneten Steuerungsinstruments ist die Frage des Anstoßes des Informationsvorgangs. Ein solcher muss im Bereich der Informationen über Sicherheitslücken situativ-initiativ von demjenigen erfolgen, der sich im „Erfahrensbereich" der Sicherheitslücke befindet. Damit scheidet etwa eine Auskunftspflicht des Herstellers oder Anbieters gegenüber dem – zur Antragstellung verpflichteten – Nutzer aus. Eine effektive Regelung findet sich vielmehr als Benachrichtigungs- oder Anzeigepflicht.

3. Steuerung durch Information

Steuerung durch Information ist systematisch auch eine Betrachtung des Verhältnisses von Recht und Information. Wie oben bereits dargelegt, ist Information eine Voraussetzung für Recht und könnte idealiter das Recht teilweise substituieren. Wo Information als Wissen in geeigneter Form rezipiert wird, könnten rechtlichen Regelungen überflüssig sein. Relevant wird dies etwa in der Informationstätigkeit des Staates, die als schlicht-hoheitliches Verwaltungshandeln zwar grundsätzlich rechtsunverbindlich ist, in seiner Wirkung aber rechtserheblich und rechtsersetzend sein kann.[56]

Die Rezeption und Verwendung von Information ist tatsächlich vielfältig. So ist Information letztlich nicht nur ein „nice to have", sondern in einer Informationsgesellschaft ein geldwertes Gut, was eine staatliche Generierung von Information bei Privaten nicht ohne weiteres möglich macht.

---

54 Gegenstand der Informationsrechte- und pflichten sind folglich system- und nutzungsbedingte und nicht nutzerbedingte Sicherheitslücken und Schwachstellen, vgl. Kapitel 2 B III. 3.

55 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 132. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. Nr. L 201, vom 31.07. 2002, S. 37.

56 Fett, Rechtsschutz gegen schlicht-hoheitliches Verwaltungshandeln, in: WM 1999, 613 (613 f.).

Soweit die Informationstätigkeit des Staates als Steuerung durch Information verstanden wird, ist zu differenzieren. Diese kann im weiteren Sinne als die Verteilung von Information an Bürger mit intendierter verhaltenssteuernder Wirkung betrachtet werden *(„informationelle Steuerung“*[57]). In der Erzielung der intendierten Wirkung kann Information vielleicht als *„relativ weiches Steuerungsmedium“*[58] gelten, tatsächlich mit der Verursachung von „Kollateralschäden“ allerdings eine wesentlich weitere Wirkung besitzen.[59] Im engeren Sinn und offensichtlich rechtlich kann die Informationstätigkeit des Staates als Steuerung durch Informationsrechte und –pflichten begriffen werden und betrifft damit das Steuerungsmedium Recht.

Mit der Informationstätigkeit ist zumindest die Organisation von Information beim Staat selbst zu betrachten (Information als Handlungsvoraussetzung des Staates[60]). Zudem kann der Staat die Beziehungen und den Umgang Dritter mit Information regeln (Information als Steuerungsmedium des Staates). Als staatliche Informationstätigkeit können demnach (vorbereitende) Informationsbeschaffung (die Grundlage der Steuerung durch Information und Recht) und -sammlung, Informationsweitergabe (etwa Warnungen) und die Verpflichtung Dritter zur Informationsbeschaffung, –sammlung und –weitergabe betrachtet werden. Mit den bereits dargelegten Begrifflichkeiten sind Beschaffung, Sammlung und Weitergabe Steuerungsinstrumente des Mediums Information.

---

57 Der Begriff der „informationellen Steuerung“ ist mit dieser Bedeutung Kloepfer zu entnehmen, vgl. Kloepfer, Staatliche Informationen, 1998, S. 14. Kloepfer beschreibt diese wie folgt: *„Bei der informationellen Steuerung geht es primär darum, etwas zu tun, obwohl es nicht geboten ist bzw. etwas zu unterlassen, obwohl es nicht verboten ist (z. B. Energieeinsparappelle).“* Davon zu unterscheiden ist die verhaltenssteuernde Information als schlichtes Verwaltungshandeln („informelles Verwaltungshandeln“). Dieses erschließt sich in Abgrenzung zum formalisierten Verwaltungshandeln und ist traditionell gesetzlich nicht geregelt. Diese Rechtsfreiheit lässt zuweilen befürchten, konkrete „rechtsstaatliche Errungenschaften“ zu verlieren, vgl. Gusy, Verwaltung durch Information, in: NJW 2000, 977 (979).

58 König/Dose, Referenzen staatlicher Steuerung, in: dies. (Hrsg.), Instrumente und Formen staatlichen Handelns, 1993, S. 519 (555), die für den Fall der Nichtbefolgung von gesundheitsbedenklichen Warnungen keine rechtliche Konsequenzen annehmen wollen, a.a.O., S. 555 f. Dies mag für das Objekt der Warnung gelten, kann jedoch nicht für Dritte angenommen werden.

59 Als solche „Kollateralschäden“ sind etwa Grundrechtsverletzungen Dritter, im Fall staatlicher Warnungen vor Produkten der betroffenen Hersteller zu bezeichnen.

60 In diesem Sinne auch Kugelmann, Die Informatorische Rechtsstellung des Bürgers, 2001, S. 21, der auf die Informationssammlung als Entscheidungsvorbereitung der Verwaltung hinweist.

Informationsphasen sind Generierung und Sammlung sowie Verbreitung bzw. Geheimhaltung. Im Hinblick auf den Aufwand in den einzelnen Phasen lässt sich festhalten:

> *„Während die Generierung von Informationen typischerweise einen Aufwand macht, ist ihre Verbreitung und Nutzung nahezu kostenlos."*[61]

Im Verhältnis von Staat und Technik sind hinsichtlich der Informationsphasen zum einen die zeitlichen Komponenten „legal lag" und „legal age", zum anderen eine grundsätzliche „information gap" des Staates charakterisierend.

Charakteristika und Herausforderung der Gesetzgebung im Bereich der Technik ist der Umgang mit dem temporären Aspekt von technischen Innovationen. Dies ist zum einen der zeitliche Abstand zwischen Entwicklung der Technik (innovative Information) und ihrer rechtlichen Regelung (fehlende Information) – der *„legal lag"*[62] des Technikrechts, zum anderen eine rasche inhaltliche Divergenz zwischen der Technik (überholte Information) und der rechtlichen Regelung (überholtes Recht) – das *„legal age"*[63].

Der Rechtsprechung mag die Möglichkeit, sie zur Technikssteuerung instrumentalisieren zu können, abgesprochen werden. Es bleibt jedoch eine zumindest faktisch steuernde Wirkung der Rechtsprechung.[64] Darüber hinaus kann die Rechtsprechung eine fehlende gesetzliche Regelung – etwa den „legal lag" des Technikrechts – steuernd ausgleichen oder mittels der Ausfüllung unbestimmter Rechtsbegriffe konkretisierend steuern. Hier kann auf einen möglichen Kontrollverzicht hingewiesen werden. Durch die faktische Anerkennung technischer Regelwerke verzichte die Rechtsprechung auf eine weitergehende Kontrolle.[65]

---

61 Wagner, Haftung und Versicherung als Instrumente der Technikssteuerung, in: Vieweg (Hrsg.), Technikssteuerung und Recht, 2000, S. 87 (114).

62 Vieweg, Technik und Recht, in: Vieweg/Haarmann (Hrsg.), Beiträge zum Wirtschafts- Europa- und Technikrecht, 2000, S. 199 (209).

63 Ausgeglichen werden kann diese rechtliche Überalterung durch die Verwendung von unbestimmten Rechtsbegriffen, die eine laufende Anpassung entbehrlich machen. Zum anderen können Normen mit einem „Verfallsdatum" versehen werden, d. h. sie treten zu einem vorgegebenen Zeitpunkt außer Kraft oder müssen zumindest einer Relevanzprüfung unterzogen werden, vgl. Burkert, Internet und Recht, in: Drossou/v. Harren/ u. a. (Hrsg.), Machtfragen der Informationsgesellschaft, 1999, S. 385 (392).

64 So Sendler, der die Technikssteuerung lediglich als ein „Neben- oder gar Abfallprodukt" der Rechtsprechung ansieht: *„Indem Recht gesprochen wird, wird halt auch Technik gesteuert"*, Sendler, Technikssteuerung und verwaltungsgerichtliche Rechtsprechung, in: Vieweg (Hrsg.), Technikssteuerung und Recht, 2000, S. 307 (312).

65 Schuppert, Verwaltungswissenschaft als Steuerungswissenschaft, in: Hoffmann-Riehm (Hrsg.), Reform des allgemeinen Verwaltungsrechts, 1993, S. 65 (79).

Eine Behebung der „information gap“ des Staates mit Instrumenten des Rechts erscheint schwierig. Während dem „legal lag“ und dem „legal age“ durch die unbestimmten Rechtsbegriffe begegnet werden kann, sind zum Ausgleich der „information gap“ des Staates bzw. des Wissensvorsprungs der Wissenschaft und Forschung als rechtliche Instrumente die Pflicht zur Informationsweitergabe und eine Steuerung der Wissensverteilung durch Anreize[66] denkbar. Die Steuerung durch Informationsweitergabe kann auf vielfältige Art realisiert werden, um Motivationen und Handlungen beim Bürger zu evozieren. So ist etwa auch die Bibliothek eine Form und Anreiz für den Bürger, Information aufzunehmen.

Die Steuerung durch Information kann unterschiedliche Wirkungen besitzen. Kloepfer[67] nennt die „kompensatorische“ und die „stabilisierende“ Funktion. Mit der „kompensatorischen“ Funktion schreibt Kloepfer der Information eine kompensierende Wirkung für fehlende Zwangs- und Erwirkungsmittel zu.[68] Diese „enforcement gap“ ist ein Kennzeichen der globalen Reichweite des Internets, weshalb eine Steuerung durch Information grundsätzlich angestrebt werden kann. Hierbei ist allerdings zu berücksichtigen, dass rechtlich normierte Informationsrechte und –pflichten ihrerseits der „enforcement gap“ ausgesetzt sein können. Mit „können“ soll angedeutet werden, dass national vollzieh- und durchsetzbare Rechte und Pflichten bereits zur Erhöhung der Sicherheit beitragen und die Relevanz der „enforcement gap“ reduzieren können.

Mit der „stabilisierenden“ Funktion beschreibt Kloepfer die Information als notwendige Voraussetzung für die individuelle Eigenverantwortung und Selbstbeherrschung.[69] Je geringer die „kompensatorische“ Funktion einer Steuerung durch In-

---

66 Anreize sind etwa auch die finanzielle Unterstützung des Staates von Forschungsprogrammen, die den Staat durch verpflichtende Berichte über den Forschungsgegenstand Informationen beschaffen. Eine personelle Alternative zur Verminderung der „information gap“ ist die direkte staatliche Beteiligung etwa an Forschungszentren.

67 Kloepfer, Staatliche Informationen, 1998, S. 9 f.

68 Kloepfer, Staatliche Informationen, 1998, S. 9. Kloepfer begründet dies mit der entstandenen Lücke zwischen den heute nahezu unbegrenzten Aufgaben des Staates und die begrenzten Zwangsmittel zu ihrer Bewältigung. Als Beispiel führt er die staatliche Risikovorsorge im Umweltrecht an, die die Grenzen der zwangsweisen Durchsetzung staatlicher Aufgaben deutlich werden lasse.

69 Kloepfer, Staatliche Informationen, 1998, S. 10: Wo die Prinzipien der Vorsicht und Vorsorge sowie die stärkere Eigenverantwortung und Selbstbeherrschung das Verhalten bestimmen sollen, erwüchsen Entscheidungsspielräume jenseits von Rechtmäßigkeit und Rechtswidrigkeit. Ein in diesem Sinne verstandenes verantwortungsbewusstes Handeln erfordere eine ausreichende Versorgung mit Informationen. Informationen würden so nicht nur Handlungsspielräume erweitern, sondern vermittelten, „*wenn sie das „Siegel“* staatlicher Autorität tragen“, eine Gewissheit einer vernünftigen Entscheidung und damit eine letztlich system-

formation im engeren Sinne sei, desto höher könne die „stabilisierende" Funktion der Steuerung durch Information bei fehlenden Informationsrechten und -pflichten eingeschätzt werden. Ist auch die Sicherheit vorwiegend der rechtlichen Kategorie der Verantwortung übertragen, so sind die Grenzen zu der Kategorie der Rechtmäßigkeit und Rechtswidrigkeit fließend (vgl. oben). Je fließender die Grenzen, desto mehr ist der Staat gefordert, die Handlungsgewissheit und –sicherheit des Einzelnen für sein Handeln herzustellen. Die staatliche Steuerung durch Information dient in diesem Fall letztendlich der Rechtssicherheit.

Die Grenze einer Steuerung durch Information ist die „*information overload*"[70]. Ist dieser Zustand erreicht, verliert die Information ihre stabilisierende Wirkung.

Zusammenfassend soll als Steuerung durch Information sowohl die informationelle Steuerung als auch die Steuerung durch Informationsrechte und –pflichten verstanden werden.

B Grenzen des Beitrags des Rechts zur Sicherheit im Internet

Aufbauend auf den Betrachtungen zur Techniksteuerung im Allgemeinen soll nun im Besonderen der Beitrag des Rechts zur Steuerung der Sicherheit im Internet konturiert werden. Da ein positiver Beitrag in Form der Darlegung eines IT-Sicherheitsrechts in dieser Arbeit den Ausführungen zu den Informationsrechten und –pflichten vorbehalten sein und sich auf diese konzentrieren soll, wird der Beitrag des Rechts hier nur durch seine Grenzen konturiert. Hierbei sollen zunächst die Grenzen der Steuerung des Internets im Allgemeinen aufgezeigt, bevor diese in „internetspezifische" Aspekte gegliedert werden.

I. Steuerungsbedürftigkeit, Steuerungsfähigkeit und Steuerbarkeit

Nachdem die Steuerung als Prozess, Anreiz, Autorität und Verantwortung zu begreifen ist und durch Information bestimmt sein kann, stellen sich im Anschluss die

---

stabilisierende Sicherheit. Vgl. auch Pitschas, Staatliches Management für Risikoinformation, in: Hart (Hrsg.), Privatrecht im Risikostaat, S. 215 (243): Die Informationsfreiheit umfasse auch das Recht des Bürgers auf *„Informationen über Sicherheit vor Risiken wie seinen Anspruch auf Unterrichtung und Kommunikation zur persönlichen Risikoabwehr, schließlich auch als Verbraucher das recht auf selbstbestimmte Entscheidung über Risikoakzeptanz auf der Grundlage entsprechender Informationen."*

70 Eidenmüller, Der homo oeconomicus, in: JZ 2005, 216 (221).

Fragen: Warum und mit welchem Ziel soll eine Steuerung des Internets erfolgen? Gibt es nicht Bereiche und/oder Ziele, deren authentische Entwicklung – ohne Eingriffe durch den Staat – die förderlichste Option für das Gemeinwohl darstellt? Gibt es darüber hinaus Bereiche, die sich a priori einer Steuerung entziehen? Diese Aspekte sollen im Folgenden mit den Begriffen Steuerungsbedürftigkeit, -fähigkeit und Steuerbarkeit erörtert werden.

1. Steuerungsbedürftigkeit

Hinsichtlich der Steuerungsbedürftigkeit stellt sich die Frage, ob die bestehenden Zustände und Prozesse in einem System nicht bereits akzeptable Ergebnisse sind und damit ein (staatlicher) Eingriff nicht erforderlich ist.

Es gibt immer wieder Stimmen, die eine Steuerungsbedürftigkeit des Internets verneinen. Die Steuerungsbedürftigkeit könnte zu verneinen sein, wo der bisherige Zustand etwa durch die Selbststeuerung zu akzeptablen Ergebnissen führt.[71] Im Bereich der „Internetverwaltung" haben staatliche Stellen in Deutschland und der EU bisher beteuert, dass diese zur Zufriedenheit ausgeführt wird und ein Eingreifen nicht für notwendig erachtet wird.[72] Dennoch legte das Ministerium für Wirtschaft und Arbeit im Sommer 2003 im Rahmen der Telekommunikationsgesetznovelle einen Referentenentwurf zur Telekommunikations-Nummerierungsverordnung vor. Danach sollte die DeNIC durch die RegTP, die Vorgängerin der Bundesnetzagentur, ersetzt werden.[73] Die Beteuerung und der Entwurf stehen jedoch nicht zwangsläufig im Widerspruch zueinander. Im Fall der Internetverwaltung drängt sich der Gedanke eines eventuell notwendigen „Eingriffsvorbehalts" des Staates zur Schaffung von Rahmenbedingungen auf. So sind etwa die wachsende Anzahl der Urteile im Falle von Domainstreitigkeiten Indiz dafür, dass zumindest die Vergabe der

---

71 Voigt, Staatliche Steuerung aus interdisziplinärer Perspektive, in: König/Dose (Hrsg.), Instrumente und Formen staatlichen Handelns, 1993, S. 289 (300).

72 Antwort der Bundesregierung auf eine Kleine Anfrage zum Schutz von Internetadressen, vom 28.07.2000, BT-Drs. 14/3956, S. 3: „*Die Bundesregierung hält deshalb an ihrer Unterstützung der internationalen Selbstregulierung aller Beteiligten im Bereich der Internet-Adressenverwaltung fest.*"

73 § 2 Abs. 2 Nr. 10 des Referentenentwurfs vom 30.04.2003 sah vor:
„(2) Zu den Nummern, die in ihrer Gesamtheit jeweils einen Nummernraum bilden und nach § 58 Abs. 1 des Telekommunikationsgesetzes strukturiert und ausgestaltet sind, gehören (…)
10. Internet Domain Namen mit deutscher Landeskennung, (…)"
Dies hätte zur Folge gehabt, dass die RegTP und nicht die DeNIC nach dem Gesetz für die Strukturierung und Verteilung des Nummernraums zuständig wäre. Im weiteren Verlauf der Novellierung wurde dieser Vorschlag nicht mehr aufgegriffen.

Domainnamen in vielen Fällen nicht zur Zufriedenheit läuft und daher das „System“ nicht funktioniert. Es bleibt die Frage, was ein funktionierendes System ist, welches keiner Korrektur zur Vermeidung von Fehlentwicklungen bedarf.[74]

Die Steuerungsbedürftigkeit lässt sich anhand der Entwicklung des Internets konkretisieren: Die Grenze der Steuerung wird zum einen durch die globale Reichweite indiziert, zum anderen zeigt die bisherige Entwicklung, dass diese auf der freiwilligen und privaten Gestaltung des Internets durch den technischen Sachverstand basiert. Fraglich ist, ob mit einer „Verrechtlichung“ dieser Sachverstand weiterhin gewährleistet bleibt.

Gerade beim Auffinden von Sicherheitslücken scheint weniger die Expertise der Unternehmen als die Experimentierfreudigkeit der Hacker[75] erfolgsversprechend. In zahlreichen Fällen sind es die Hacker, die an Unternehmen herantreten[76] und auf Lücken aufmerksam machen, bzw. im Internet auf entsprechenden Seiten oder in Newsgroups Informationen zu Sicherheitslücken veröffentlichen.

2. Steuerungsfähigkeit und Steuerbarkeit

Die Steuerungsfähigkeit hängt von der Verfasstheit des Steuerungsakteurs und -objektes ab. Relevant sind diesbezüglich das Wissen des Akteurs und des Objekts sowie die Fähigkeit zur Diagnose und Prognose des Handelns.[77]

---

74 Voigt, Staatliche Steuerung aus interdisziplinärer Perspektive, in: König/Dose (Hrsg.), Instrumente und Formen staatlichen Handelns, 1993, S. 289 (301).

75 Dringen Unbekannte in ein Computersystem ein, ist meist von dem „Hacker“ die Rede. Das so mit „Hacken“ bezeichnete Verhalten ist durch das unterschiedliche Selbstverständnis der „Hacker“ zu differenzieren. Vgl. http://www.bsi-fuer-buerger.de/abzocker/05_03.htm (30.05.2006): Hacker sind diejenigen, die mit Expertenwissen in ein fremdes IT-System eindringen, um es zu verstehen, oder eben um Sicherheitslücken in einem System zu finden. Hierbei werden regelmäßig keine Daten verändert. Solange nicht explizit der Aspekt der Rechtsfolgen diskutiert wird, wird dem Hacker hier grundsätzlich keine schädigende Absicht unterstellt.

76 So geschehen etwa im Fall von ebay, heise news vom 27.09.2004, http://www.heise.de-/newsticker/meldung/51511 (30.05.2006); oder bei den Sicherheitsmängeln bei der T-Com Datenbank, durch den ccc (Chaos Computer Club) aufgedeckt, vgl. heise news vom 26.07.2004, http://www.heise.de/newsticker/meldung/49424 (30.05.2006). Allerdings gibt es kein statistisches Material von unternehmensintern aufgedeckten Sicherheitslücken, die man in Relation mit den öffentlich bekannten externen Entdeckungen setzen kann.

77 Voigt, Staatliche Steuerung aus interdisziplinärer Perspektive, in: König/Dose (Hrsg.), Instrumente und Formen staatlichen Handelns, 1993, S. 289 (302).

Die Steuerbarkeit lässt sich als die Möglichkeit bzw. Unmöglichkeit des Akteurs definieren, mit seinen Steuerungsinstrumenten einen bestimmten Systemprozess lenken zu können. Steuerbarkeit ist mithin eine Frage nach den Grenzen der Steuerung. Da die Begriffe Steuerungsfähigkeit und Steuerbarkeit in ihrer Anwendung nicht immer trennscharf sind, werden sie zusammengefasst dargestellt.

Bezüge zur Steuerungsfähigkeit und Steuerbarkeit des Internets finden sich in der globalen Reichweite des Internets und der Technik.

Eine Grenze könnte sich aus der globalen Reichweite des Internets ergeben. Die Macht des Rechts beruht primär auf seiner Durchsetz- und Vollziehbarkeit. So verstanden ist das Verhältnis von Sicherheit und Recht nicht eine Frage der Rechtsetzung, *„sondern auch, und gar vornehmlich, eine Frage der Rechtsdurchsetzung."*[78] Dieser sind in einer internationalen Umgebung Grenzen gesetzt („enforcement gap"). Allerdings kann Recht auch akzeptiert werden. Die Akzeptanz gewährt dem Recht Vollzugssicherheit. Auf eine Durchsetzungsmöglichkeit des Vollzugs kommt es dann nicht mehr an.

Die Chance, rechtlich formulierten Interessen im internationalen Kontext Durchsetzbarkeit zu verleihen, kann darüber hinaus durch die Ermöglichung der Wahrnehmung von Eigenverantwortung erhöht werden.[79] Basis dieser ist wiederum Information, die grundsätzlich ungeachtet der Reichweite des Rechts, wirken kann, die aber als Informationspflicht auch an die Reichweite des Rechts gebunden ist.

Zudem kann Technik eine bereichsspezifische Grenze[80] des Rechts darstellen. Die Technik indiziert ein rechtliches Dilemma zwischen Offenheit gegenüber technischen Neuerungen – durch unbestimmte Rechtsbegriffe und deren Ausfüllung durch technische Regelwerke – und Rechtsklarheit.[81] Im Ergebnis wird teilweise festgestellt, dass *„wenig Hoffnung auf eine inhaltliche Steuerbarkeit der Technik durch materielle Rechtmäßigkeitskriterien"*[82] bestehe. Schlussendlich ist festzuhalten, dass rechtlich gewünschte Regelungen stets durch das technisch Machbare begrenzt sind.

---

78 Isensee, Das Grundrecht auf Sicherheit, 1983, S. 40 f.

79 So als Konzept des Selbstdatenschutzes u. a. zur Überwindung der Globalität des Internets für die Wahrung des Datenschutzes entwickelt von: *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, S. 328, Rd. 3.

80 Vgl. Schuppert, Grenzen und Alternativen von Steuerung durch Recht, in: Grimm (Hrsg.), Wachsende Staatsaufgaben – sinkende Steuerungsfähigkeit des Rechts, 1990, S. 217 (217 ff.), der bereichsspezifische Grenzen im Bereich der Technik, Wirtschaft und Moral ausmacht.

81 BVerfG „Kalkar", Beschluss v. 08.08.1978 – 2 BvL 8/77, BVerfGE, 49, 89 (135 ff.).

82 Wolf, Das Recht im Schatten der Technik, in: Kritische Justiz, 1986, 241 (250).

Im Folgenden sollen Thesen dargestellt werden, die die Technik Internet aus unterschiedlichen Aspekten von vorneherein einer Steuerung entzogen wissen wollen.

II. Rechtliche Steuerung des Internets?

Teilweise werden Thesen vertreten, wonach der Beitrag des Rechts zur Steuerung des Internets bestimmten Annahmen unterliegt. Alle Thesen lassen sich auf die Annahme reduzieren, dass das Internet nicht durch Recht steuerbar ist. Die Thesen werden im Folgenden aufgrund der Fokussierung auf die Steuerung der Sicherheit auf ihre Relevanz für die IT-Sicherheit überprüft.

1. Cyberlaw These I: Anarchie

Die These vom Cyberspace als „rechtsfreier Raum" ist schon lange verbreitet. Diese *„staatsfeindliche Grundhaltung"*[83] wird regelmäßig der Internet-Gemeinde zugesprochen, während die Juristen *„naiv die Fortexistenz des Status quo"*[84] voraussetzen. Naiv oder nicht, so ist nicht von der Hand zu weisen, dass das Vertrauen in das Recht allgemein von der Ausdehnung des Rechts auch auf das Internet abhängt.[85] Der entscheidende Punkt dabei ist, nicht allein auf die abstrakte Geltung des Rechts, sondern auf seine konkrete Durchsetzbarkeit zu setzen und diese zu prüfen. Dies setzt etwa im informationellen Bereich staatliche Maßnahmen der Überwachung und Kontrolle voraus.[86]

Für eine Steuerung des Internets bedeutet dies nicht zwangsläufig eine Nichtsteuerbarkeit. Dort wo es an der Durchsetzbarkeit fehlt, kann auf den Anreiz und auf die freiwillige Akzeptanz von Recht und Information, sowie auf eine Steuerung durch Informationsverteilung und damit auf Eigenverantwortung gesetzt werden.

---

83 Vgl. etwa Borsook, Schöne neue Cyberwelt, 2000, S. 258; a.A. etwa Schneier, ein führender Sicherheitsexperte: *„Prosecution opens a can of worms that is completely foreign to most computer people: the legal system. Identifying an attacker isn't enough; you also need to be able to prove it in court."*, Schneier, Secrets & Lies, 2000, S. 377. Schneier sieht die Verfolgung als letzte Maßnahme in einem Sicherheitsprozess von detection, analysis, respond (prosecution). Die Vorbeugung (prevention) erwähnt er, schreibt ihr allerdings einen geringen Beitrag zur Erhöhung der Sicherheit zu, vgl. a.a.O., S. 374.

84 Fiedler, Der Staat im Cyberspace, in: Informatik Spektrum, Band 24 Nr. 5 2001, 309 (309).

85 Kalir/Maxwell, Rethinking Boundaries in Cyberspace, 2002, S. 22: Recht, das nur partielle Geltung und Durchsetzung besitzt, verliere langfristig seine Legitimität.

86 So Fiedler, a.a.O., (Fn. 83), 309 (310).

2. Cyberlaw These II: Lex Informatica/Code

Das „Wie" der rechtlichen Steuerung des Internets wird im US-amerikanischen Recht durch Lessigs Auseinandersetzung mit dem „Code" und Reidenbergs „Lex Informatica" als Alternativen zum Recht diskutiert. Im Folgenden soll nur ein kursorischer Überblick über diese Diskussion gegeben werden.[87]

Der Begriff *„Lex Informatica"*[88] wurde im amerikanischen Recht von Reidenberg als quasi-rechtliche Verfassung des Internets durch die Softwareprogrammierung und technischen Festlegungen des Kommunikationstransfers verstanden und formuliert.[89]

Ähnlich vermittelt Lessig für das US-amerikanische Recht das Konzept des „Code".[90] Der „Code" entspricht den durch die Infrastruktur aufgestellten Regeln. Durch die faktische Durchsetzung von (rechtlichen) Interessen durch die Technik werden diese durch die Technik determiniert und gestaltet. Das Verhältnis von Lex Informatica und Recht wird von einer parallelen Geltung bis hin zur Überlappung und Substitution angenommen.[91]

Der Annahme von der Vorherrschaft des „Code" oder einer „Lex Informatica" im Internet entspricht letztlich der Annahme einer Steuerung durch die Technik mithin von bereichspezifischen Grenzen durch die Technik.

Die rechtliche Verfassung des Cyberspace durch den Code reicht etwa von Gestattung der Meinungsäußerung bis zur Gewährleistung von Privatsphäre und Anonymität. Diese Freiheiten werden durch die Implementierung neuer Codes etwa in Form von Cookies und Authentifizierung, insbesondere durch die technische strikte Reglementierung und den technischen Schutz des Urheberrechts eingeschränkt[92] – eingeschränkter als es bei Printmedien je möglich gewesen wäre.

---

87 Eine ausführliche Auseinandersetzung findet sich bei Leube, Die Rolle des Staates im Internet, 2004, S. 226 ff.

88 Reidenberg, Lex Informatica, 76 TEXAS L. REV. 553 (1998), S. 553.

89 Reidenberg ist kein Informatiker, sondern Professor of Law at Fordham University School of Law. In Lex Informatica, 76 TEXAS L. REV. 553 (1998), S. 553 (566) stellt Reidenberg, das Rechtssystem dem System "Lex Informatica" u.a. in den Elementen territorialer Geltungsbereich, Steuerungsinstrumenten, Rechtsquelle und Durchsetzung gegenüber.

90 Im deutschen Recht finden sich Verweise auf und eine Rezeption von Lex Informatica und Lessigs Code etwa bei, Lutterbeck, vgl. Lutterbeck/Ishii, Open Code and Open Societies, http://ig.cs.tu-berlin.de/oldstatic/bl/042/index_html#fn0 (30.05.2006).

91 Reidenberg, Lex Informatica, 76 TEXAS L. REV. 553 (1998), S. 578.

92 Gutmair, Die Politik des Codes, 2000, telepolis vom 17.04.2000, http://www.heise.de-/tp/r4/html/result.xhtml?url=/tp/r4/artikel/6/6747/1.html&words=Gutmair

Am Beispiel des Urheberrechts kann das Verhältnis des Codes zum Recht dargestellt werden. Das Recht im traditionellen Sinne fungiert als Unterstützung der technischen Restriktionen für den Nutzer, konstituiert aber auch parallel erst ein Urheberrecht. Das Recht vermag nicht die erforderliche Balance zwischen den Interessen des Urhebers und der Meinungs- und Informationsfreiheit und letztendlich dem Allgemeinwohl (wieder)herzustellen. Deshalb kann der Code auch den quasi rechtlichen Status einer Einschränkung der Meinungs- und Informationsfreiheit erlangen.

Die Technik kann unter diesen Prämissen demnach als autonomer Bereich verstanden werden, in dem Recht keinen effektiven Beitrag leisten kann.[93]

3. Cyberlaw These III: Internationalisierung

Die Prämissen des grenzenlosen Internets und die territoriale Begrenztheit des Rechts werden im Grundsatz unterstellt und nicht weiter ausgeführt.[94] Diese Gegenüberstellung soll jedoch im Hinblick auf die IT-Sicherheit kurz differenziert werden.

Für rechtliche Regelungen der IT-Sicherheit lässt sich Folgendes ausführen. Soweit es um die Interessensicherung, d. h. unter anderem die Kontrolle von Inhalten geht, erlaubt das grenzenlose Internet nur begrenzt effiziente Regelungen, da unzulässige Inhalte von exterritorialen Servern gesendet und territorialen Clients abgerufen werden können. Soweit es um Daten-, Kommunikations- und Netzsicherheit geht, können bereits nationale Regelungen ex ante einen Beitrag zur IT-Sicherheit leisten. So etwa durch lokal vorgegebene und installierte Schutzmaßnahmen. Die Antithese vom grenzenlosen Raum und der begrenzten Reichweite des Rechts trifft jedoch auf ex post-Regelungen zu, soweit Sanktionen etwa für die Verbreitung von Spam oder das unbefugte Ausspähen von Daten durchgesetzt werden sollen. Effiziente Regelungen verlangen in diesem Bereich einen Beitrag des Rechts auf internationaler Ebene.

(30.05.2006); eine Auseinandersetzung mit dem Urheberrecht bei Lessig, Code and other Laws, 1999, S. 127 ff.

93 Leube, Die Rolle des Staates im Internet, 2004, S. 233.

94 Zu den Auswirkungen von Globalisierung auf Staat, Steuerung und Recht: Lutterbeck, Globalisierung des Rechts, in: CR 2000, 52 (52 ff.)

Die Analyse wird durch den ersten Ansatz eines internationalen Cyberlaw im ex post-Bereich des Strafrechts, die Convention on Cybercrime,[95] bestätigt.

4. Zusammenfassung

Die Thesen, die für die mangelnde rechtliche Steuerbarkeit des Internets grundsätzlich angeführt werden, haben nur bedingte Relevanz für Regelungen im Bereich der IT-Sicherheit. So steht insbesondere die territoriale Begrenztheit des Internets der IT-Sicherheit nicht unbedingt entgegen. IT-Sicherheit ist regelmäßig eine Herausforderung, der auch mit lokalen technischen, organisatorischen, personellen und rechtlichen Strategien effektiv und effizient begegnet werden kann; auch wenn die Gefahren für die IT-Sicherheit sicherlich virulent und international verbreitet sind. Eine Steuerung der IT-Sicherheit steht regelmäßig vor der Herausforderung, effiziente und effektive ex ante- und in operatione-Strategien entwickeln zu müssen. Unter diesen Gesichtspunkten kann der Verweis auf territorial begrenzte ex post-Sanktionen lediglich ein zweitrangiger Aspekt sein.

Soweit die Technik als autonomer Bereich verstanden werden kann, in dem Recht keinen effektiven Beitrag zu leisten vermag, kann zumindest das Recht die Eigenverantwortung des Einzelnen für die IT-Sicherheit betonen. Die Eigenverantwortung kann somit über eine „Herrschaft" von Soft- und Hardware gestellt werden.

Es bleibt festzuhalten, der „Anarchie" des Internets kann mit einem IT-Sicherheitsrecht begegnet werden, das effiziente und effektive lokale Maßnahmen und die Eigenverantwortung des Einzelnen voraussetzt.

C Sicherheit durch staatliche Steuerung des Informationsvorgangs

Hier sollen die Möglichkeiten des steuernden Einflusses des Staates auf die IT-Sicherheit mittels Information dargestellt werden.

Wie in diesem Kapitel ausgeführt, zielt die Informationstätigkeit des Staates auf Informationsbeschaffung[96] zur Optimierung der Handlungsvoraussetzung des Staates

---

[95] Convention on Cybercrime vom 23.10.2001, http://conventions.coe.int/Treaty/-EN/Treaties/Html/185.htm (30.05.2006).

[96] Zu den Begriffen Informationsbeschaffung und –verwertung siehe auch Kapitel 4 A II. 3.

und auf Informationsverwertung als Steuerungsmedium des Staates.[97] Die Informationstätigkeit lässt sich nicht immer trennscharf dem einen oder anderen Zweck zuordnen. Für eine Beurteilung der Zweck- und Rechtmäßigkeit kommt es auf die Bewertung des Umfangs der Staatsaufgaben[98] und die Grundrechtsrelevanz der Informationstätigkeit an. Die Informationsbeschaffung betrifft Grundrechte, etwa wenn der Bürger die Pflicht hat, den Staat zu informieren.[99] Die Grundrechtsrelevanz der Informationsverwertung kann bei Warnungen vorliegen. Am Beispiel der staatlichen Warnung sollen die Möglichkeiten der staatlichen Steuerung der Sicherheit im Internet konkret dargestellt werden.

I. Informationsbeschaffung und -verwertung

Die staatliche Informationsbeschaffung kann einerseits aus dem Recht des Staates sich zu informieren (korrespondierend mit der Pflicht des Bürgers zu informieren) und andererseits als Pflicht des Staates sich zu informieren gedacht werden.[100] Die Informationsverwertung entspricht primär einer Pflicht des Staates zu informieren.[101] Allerdings kann durch Informationszugangsrechte (Recht sich zu informieren) auch eine Steuerung des mündigen Bürgers (bzw. zum mündigen Bürger) erfolgen. Im Hinblick auf die Sicherheit soll jedoch die staatliche Informationstätigkeit im Vordergrund stehen, die nicht lediglich Anreize setzt, sondern sich aktiv um Informationen und ihre Verwertung bemüht und den Bürger verpflichtet. Die aktive staatliche Informationsbeschaffung und -verwertung entspricht letztendlich der Pflicht des Staates, den so erreichten Informations(zu)stand zum Wohl der Allgemeinheit zu nutzen.[102]

---

97 Die Informationsbeschaffung –sammlung und -verwertung sind Steuerungsinstrumente des Mediums Information. Sie realisieren sich in der Pflicht (den Staat) zu informieren, der Pflicht (des Staates) sich zu informieren und in dem Recht (die Allgemeinheit) zu informieren.

98 Grundlegend zu Staatsaufgaben: Bull, Die Staatsaufgaben, 1973.

99 Eine „versteckte" Informationsbeschaffung liegt etwa in der Auskunftspflicht bei Genehmigungsverfahren,

100 Teilweise wird die Pflicht des Staates sich zu informieren auch als *„Informationsverantwortung"* des Staates, die die Basis der Existenz des Staates in einer Informationsgesellschaft sei, bezeichnet, vgl. Pitschas, Verwaltungsverantwortung, 1990, S. 371.

101 Für die staatliche Öffentlichkeitsarbeit hat das BVerfG schon relativ früh festgestellt, dass es diese nicht nur für zulässig, sondern sogar für verfassungsrechtlich notwendig und somit geboten hält, BVerfG, Urteil v. 02.03.2977 - 2 BvE 1/76, BVerfGE 44, 125 (147).

102 Aufgrund des behördlichen Informationsvorsprungs soll eine staatliche Pflicht, die Öffentlichkeit zu informieren aus dem Rechtsstaatsgebot, dem Demokratieprinzip und der Trans-

Staatliche Informationsbeschaffung dient abstrakt zur Füllung der *„information gap"* des Staates und ist damit Grundlage für seine Aufgabenerfüllung, insbesondere der Erfüllung grundrechtlichen Schutzpflichten.[103] Konkret kann staatliche Informationsbeschaffung der Gefahrenabwehr dienen, so etwa wenn der Staat über Sicherheitslücken zu informieren ist. Ausgestaltet werden könnte dies als Recht des Staates sich zu informieren (mit entsprechender Auskunftspflicht des Bürgers oder Unternehmen – etwa im Fall des § 8 Abs. 9 S. 2 GPSG[104]) oder als Pflicht den Staat zu informieren (Anzeigepflicht des Bürgers oder Unternehmen – etwa im Fall des § 5 Abs. 2 GPSG). Im Gegenzug müsste der Staat entsprechende Annahmestellen – etwa durch Computer Emergency Response Teams (CERTs) – gewährleisten.

Eine effiziente (wirtschaftliche) und effektive (zielgerichtete) Regelung zur Informationsbeschaffung muss im Bereich der Informationen über Sicherheitslücken situativ-initiativ die Informationspflicht demjenigen, der sich im „Erfahrensbereich" der Sicherheitslücke befindet, auferlegen. Damit scheidet eine Auskunftspflicht des Bürgers oder des Unternehmens im oben beschriebenen Sinne aus. Eine Regelung ist nur über eine Ad-hoc-Anzeigepflicht möglich. Eine solche findet sich beispielgebend im Kapitalmarktrecht.[105] Flankierend können präventive Auskunftspflichten bei Realisierung der Gefahr bestehen. Der Bericht über die Gefahr hängt jedoch von der Initiative (Anzeige oder Meldung) desjenigen ab, der die Realisierung der Gefahr entdeckt.

Anzeigepflichten können als mögliche Eingriffe in die (negative) Meinungsäußerungsfreiheit, Berufs- oder allgemeine Handlungsfreiheit unter einem Gesetzesvorbehalt stehen.[106] Als solche treffen sie einen individualisierten Adressaten (vgl. etwa

---

parenz sowie sozialstaatlichen Überlegungen hergeleitet werden können, vgl. Barthe, Zur Informationstätigkeit der Verwaltung, 1993, S. 19 ff. Nicht erwähnt ist der Bereich des Schutzes der Öffentlichkeit. Allerdings kann angezweifelt werden, ob der Staat im Bereich der IT-Sicherheit tatsächlich einen Informationsvorsprung besitzt. In dieser Arbeit wird teilweise zugrundgelegt, der Staat müsse sich im Bereich der IT-Sicherheit die Informationen erst beschaffen, um der Pflicht, den Bürger zu schützen, nachkommen zu können.

103 Scherzberg, Risikosteuerung durch Verwaltungsrecht, in: VVDStRL 63 (2004), S. 214 (241).

104 Geräte- und Produktsicherheitsgesetz.

105 Unter Kapitel 5 C I. 3 wird die Relevanz dieser Anzeigepflicht nach § 15 Abs. 1 S. 1 WpHG für die IT-Sicherheit erörtert.

106 Vgl. Art. 5 Abs. 2, 12 Abs. 1 S. 2, 2 Abs. 1 GG und, S. 145; *Dreier*, in: Dreier (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 2. Aufl. 2004, Art. 5 I, II Rd. 74; Wendt in v. Münch/Kunig (Hrsg.) Grundgesetz-Kommentar, Bd. 1, 5. Aufl. 2000, Art. 5 Rd. 18, der unter anderen auch die gesetzlich verpflichtenden Produktwarnungen nennt; grundlegend Fenchel, Negative Informationsfreiheit, 1997.

die Anzeigepflicht in § 5 Abs. 2 GPSG), der nicht unbedingt ein Eigeninteresse an einer Anzeige oder gar entgegenstehende Interessen haben muss.[107]

Unabhängig von der Ausgestaltung als Auskunfts- oder Anzeigepflicht ist festzuhalten, dass die staatliche Informationsbeschaffung, soll sie durchsetzbar und sanktionierbar sein, einer Rechtsgrundlage bedarf. Die Normierung und Durchsetzbarkeit der Anzeigepflichten muss zunächst die Hürde der asymmetrischen Informationsverteilung nehmen.[108] Eine freiwillige Auskunft des Bürgers oder des Unternehmens ist allerdings theoretisch denkbar, wenn vom Staat Hilfe erhofft werden kann (Mobilisierung staatlicher Ressourcen und Sanktionen).[109] Die Basis dieser Informationsbeschaffung sind danach steuernde Anreize, die auf eine freiwillige Auskunftserteilung durch Bürger und Unternehmen setzen.[110]

Die präventive Informationsbeschaffung kann etwa über Genehmigungsvorbehalte, Evaluation, Zertifizierungen und Lizenzierung erfolgen. Diese Instrumente können als verwaltungsrechtliches Genehmigungsverfahren ein (normativ[111]) geregeltes Instrument der Informationsbeschaffung und der Qualitätssicherung sein. Was bei Genehmigungsvorbehalten augenfällig auch (neben der Qualitätssicherung) einer Informationsbeschaffung dient, ist bei den übrigen Modi primär eine Frage der Qualitätssicherung und des Anreizes. Als Informationsangebot ist die Qualitätsbewertung durch Evaluation, Zertifizierungen und Lizenzierung ein (kostenpflichtiger) Anreiz, sich eine Information über den Stand des eigenen Systems oder Systemteil einzuholen. In Kooperation mit privaten Akteuren stehen diese Informationsanbote zwischen staatlicher Informationstätigkeit und gesellschaftlicher Selbstregulierung.[112]

---

107 Weitere Anzeigepflichten: § 63b Abs. 2 und 3 AMG; im Zivilrecht: § 16 VVG.

108 Mit der asymmetrischen Informationsverteilung ist der Wissensvorsprung des Entwicklers und Herstellers gemeint. Wo über das Ausmaß der Gefahrenquelle keine Information vorhanden ist, kann keine Anzeigepflicht durchgesetzt werden. Ohne das Wissen um die Gefahren, d. h. das Wissen, welche Anzeigepflichten geeignet und erforderlich sein könnten, können diese nicht normiert werden.

109 Pohl, Informationsbeschaffung beim Mitbürger, 2002, S. 119 ff.

110 Pohl, a.a.O., (F. 109), S. 92 f. Durch Anreize in der Informationsbeschaffung solle der Informierende grundsätzlich nicht in seinen Grundrechten verletzt werden, da der Anreiz keine Zwangswirkung und somit keine Beschwer habe, a.a.O., S.195 ff. Dies ist allerdings zu überdenken, wenn die Qualität des Anreizes die Grenzen zwischen freiwilligen und unfreiwilligen Hinweisen verschiebt.

111 Durch private Lizenzierung und Zertifizierungsangebote können dem Staat Informationen verloren gehen. Allerdings kann die Informationsbeschaffung mit staatlichen Akkreditierungsstellen „durch die Hintertür" erfolgen.

112 Holznagel, Recht der IT-Sicherheit, 2003, S. 38 Rd. 29.

„Informationsbeschaffung“ (ohne Informationsanreize des Staates) sind spontane situativ-initiative Hinweise der Bürger, die nicht zuletzt auch das Ziel haben können, über die Information ein Verfahren der Behörde gegen Dritte zu initiieren.[113]

Diese Informationen kann der Staat auf vielfältige Weise verwenden. Je nach Informationsquelle und „behördlichem Informationsbesitzer“ können die Informationen in unterschiedlichen Verfahren (Gesetzgebungs-, Verwaltungs- oder Gerichtsverfahren) eingebunden sein. Soweit sie bereits zweckgebunden generiert wurden, betreibt der Staat diverse Informationssammlungen.[114]

Diese Aspekte der Informationsverwertung sollen hier nur angedeutet bleiben und der Fokus auf die Informationsverteilung durch Aufklärung, Warnungen und Empfehlungen im Bereich der IT-Sicherheit gerichtet werden, die im Folgenden als mögliche Instrumente der staatlichen Informationsverwertung beschrieben werden sollen. Damit konzentriert sich dieser Teil der Arbeit auf Informationen, die fallbezogen verwertet werden, den Stempel staatlicher Autorität tragen und damit Steuerungspotenzial besitzen (vgl. Aspekte der Steuerung Kapitel 4 A I. 2.). Fallbezogen meint indes nicht einzelfallbezogen. Das Augenmerk ist auf eine Informationsverwertung gerichtet, die sich an die Allgemeinheit richtet, da bei IT-Sicherheitslücken ein *„individualbezogenes Informationshandeln“*[115] des Staates unergiebig erscheint.

Bevor auf die Instrumente der Informationstätigkeit eingegangen wird, wird ein Überblick über die Organisationsstrukturen der Informationstätigkeit einschließlich der organisierten Informationssubjekte im Bereich der IT-Sicherheit gegeben.

1. Organisierte Informationsbeschaffung und -verwertung – „Informationszentren“

Die Verwaltung von Wissen könnte organisatorisch in Informationszentren erfolgen. Bei diesen Zentren steht das Informationsangebot als Initiierung eines Infor-

---

113 Pohl, a.a.O., (Fn. 109), S. 105 f., der insbesondere auf Anzeigen zur Strafverfolgung abstellt. Diese Form der „Informationsbeschaffung“ habe keine Grundrechtsrelevanz. Allerdings sollen alle entgegengenommenen Hinweise dem Zweckbindungsgrundsatz unterliegen, d. h., die Informationen sollen nur in dem Zusammenhang verwendet werden dürfen, in dem sie entgegengenommen wurden, a.a.O., S. 208.

114 Kloepfer, Informationsrecht, 2002, S. 433 Rd. 89, mit weiteren Ausführungen etwa zum Bundeszentral-, Pass- und Melderegister, Verkehrs- und Ausländerzentralregister sowie Bundesarchiv.

115 Kloepfer, Informationsrecht, 2002, S. 429 Rd. 79: individualbezogene Informationstätigkeit sind etwa Auskunftsrechte und -pflichten. Dem gegenüber stehe eine auf eine breite Öffentlichkeit zielende staatliche öffentlichkeitsbezogene Informationstätigkeit.

mationsvorgangs im Vordergrund. Als „*Informationsintermediäre*“[116] können sie eine Ausgleichs- und Selektionsfunktion haben, den Nutzer vor einer Fülle an technischen Sicherheitsdetailinformationen zu bewahren. Die folgenden hoheitlichen (der Begriff staatlich kann im Hinblick auf die ENISA hier nicht verwendet werden) Zentren wurden entsprechend ihrem Angebot als Informationszentrum für Sicherheitslücken und Schwachstellen in IT-Systemen ausgewählt.

a) ENISA

Mit der Verordnung vom 10.03.2004 wurde die Europäische Agentur für Netz- und Informationssicherheit (ENISA) mit Sitz in Heraklion errichtet.[117] Die ENISA soll als Fachzentrum[118] den Behörden der EU und den Mitgliedstaaten in Fragen der Netz- und Informationssicherheit zur Seite stehen. Unter Netz- und Informationssicherheit ist nach Art. 4 lit. b) der Verordnung die Fähigkeit des Netzes Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten und Dienste beeinträchtigen, zu verstehen.

Kein Teil der Netz- und Informationssicherheit im Sinn der Verordnung soll die hier bezeichnete Interessensicherung sein, da der Schutz der Nutzer vor schädlichen und illegalen Inhalten nicht Teil der Informationssicherheit sein soll.[119] Diese Ansicht bestätigt letztendlich die in dieser Arbeit vorgenommene technische Kategorisierung von Sicherheit.[120]

Nach Art. 3 lit. d) der Verordnung hat die ENISA unter anderem die Aufgabe einen Beitrag zur *„frühzeitigen, objektiven und umfassenden Informationsvermittlung in Fragen der Netz- und Informationssicherheit für alle Nutzer (…) einschließlich der Verfahren zur Warnung der Nutzer“* zu leisten. Inwieweit die ENISA diesem Auftrag durch an die Allgemeinheit gerichtete Warnungen über Sicherheitslücken selbst nachkommt, oder diese über geeignete mitgliedstaatliche Stellen oder die Wirtschaft erfüllt, bleibt in der Praxis zum momentanen Zeitpunkt noch abzuwarten.

---

116 Eidenmüller, Der homo oeconomicus, in: JZ 2005, 216 (221).

117 Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz und Informationssicherheit, ABl. Nr. L 077, vom 13.03.2004, S. 1.

118 Vgl. Kurzbeschreibung der ENISA http://europa.eu.int/agencies/enisa/index_de.htm (30.05.2006).

119 Vgl. heise news vom 09.10.2004, http://www.heise.de/newsticker/meldung/51994 (30.05.2006).

120 Vgl. Kapitel 2 A II. 2.

Das Arbeitsprogramm der ENISA wird derzeit von folgenden Aufgaben vorgegeben:[121] Beratung, Analyse von Sicherheitsunfällen, Unterstützen von Risikomanagement und Förderung von Sicherheitsbewusstsein.

b) BSI

Das BSI wurde zum 01.01.1991 als Bundesoberbehörde mit Sitz in Bonn durch das BSIG[122] errichtet. Ursprünglich als Zentralstelle im Bereich des staatlichen Geheimschutzes (Zentralstelle für Sicherheit in der Informationstechnik) dem Bundesnachrichtendienst zugeordnet, sind seit der Umwandlung in das BSI die Aufgaben auf die Sicherheitsaspekte der zivilen Anwendungen der Informationstechnik ausgedehnt worden.[123]

Mit der Förderung der Sicherheit in der Informationstechnik legt das BSI den Fokus auf den Schutz durch *„Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen"* in oder bei der Anwendung informationstechnischer Systeme, § 2 Abs. 2 BSIG.

In erster Linie wendet sich das BSI an *„öffentliche Verwaltungen in Bund, Ländern und Kommunen, aber auch Unternehmen und Privatanwender"*[124]. Für den Bürger als Anwender bedeutet dies konkret das Angebot der Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen, § 3 Abs. 1 Nr. 3 BSIG, und die Beratung in Fragen der Sicherheit in der Informationstechnik. Für die private Zielgruppe stellt das

---

121 http://www.enisa.eu.int/about/activities/index_en.htm (30.05.2006): *"In order to ensure the fulfilment of its objectives, the Agency's tasks will be focused on:*
- Firstly, advising and assisting the Commission and the Member States on information security and in their dialogue with industry to address security-related problems in hardware and software products.
- Secondly, collecting and analysing data on security incidents in Europe and emerging risks;
- Thirdly, promoting risk assessment and risk management methods to enhance our capability to deal with information security threats.
- Finally, awareness-raising and co-operation between different actors in the information security field, notably by developing public / private partnerships with industry in this field."

122 Gesetz zur Errichtung des Bundesamtes für Sicherheit in der Informationstechnik.

123 http://www.bsi.bund.de/bsi/historie.htm (30.05.2006); Bizer/Hammer/Pordesch/Roßnagel, Ein Bundesamt für die Sicherheit in der Informationstechnik, in: DuD 1990, 178 (178). Entsprechend der historischen Entwicklung dehnen sich die Aufgaben des BSI von der Unterstützung des Verfassungsschutzes (§ 3 Abs. 1 Nr. 6 BSIG) bis zu der Beratung der Anwender der Informationstechnik (§ 3 Abs. 1 Nr. 7 BSIG).

124 http://www.bsi.bund.de/bsi/leitbild.htm (30.05.2006).

BSI über die primäre Webpräsenz hinaus ein eigenes Informationsportal[125] zur Verfügung und seit März 2006 mit dem Bürger-CERT ein *„Warn- und Informationsdienst zur IT-Sicherheit für Bürgerinnern und Bürgern sowie kleine Unternehmen"*[126].

c) CERT

Die Erkenntnis, dass der erste Internet-Wurm durch Kenntnis und Korrektur der sicherheitsrelevanten Lücken hätte vermieden werden können, führte Ende 1988 zur Gründung des ersten CERT[127] an der Carnegie Mellon University in Pittsburgh.[128] Heute gehören CERTs zu den wichtigsten Informationsquellen über Sicherheitslücken für IT-Verantwortliche.[129]

CERTs sind Anlaufstellen für die präventive Sammlung von und Warnung vor Sicherheitslücken und damit Quelle reaktiver Maßnahmen zur Schadensbegrenzung. Solche CERTs finden sich vor allem in größeren Unternehmen und staatlichen Bereichen und werden demnach staatlich, privat oder in staatlich-privater Kooperation (Public-Private-Partnership) geführt. Einen Überblick über CERTs in Deutschland bietet das BSI.[130] Seit März 2006 wird mit dem Bürger-CERT direkt der private Nutzer angesprochen.[131] Ein staatliches CERT ist etwa das CERT-Bund, das unter anderem die Warnung vor Bedrohungen und die Empfehlungen von Maßnahmen zur Aufgabe hat. Dieses CERT ist als ein Referat des BSI organisiert, dessen Dienstleistungen in erster Linie den Bundesbehörden zur Verfügung stehen.[132]

---

125 http://www.buerger-cert.de/ (30.05.2006). Hier kann ein Newsletter mit aktuellen Sicherheitsinformationen (kostenlos) abonniert werden, https://www.buerger-cert.de/-abonnieren.aspx (30.05.2006).

126 Pressemitteilung vom 02.03.2006, http://www.bsi.de/presse/pressinf/020306_buerger-cert.htm (30.05.2006).

127 Computer Emergency Response Team.

128 Fox, Computer Emergency Response Team, in: DuD 2002, 493.

129 Fox, a.a.O., (Fn. 128).

130 Vgl. http://www.bsi.de/certbund/teaminfo/certlink.htm (30.05.2006).

131 http://www.buerger-cert.de/default.aspx (30.05.2006); vgl. Pressemitteilung vom 02.03.2006 zur Freischaltung, http://www.bsi.de/presse/pressinf/020306_buergercert.htm (30.05.2006): *„Das Bürger-CERT ist ein verlässliches und neutrales Angebot, das Informationen über aktuelle Gefährdungen, Schwachstellen und Angriffe auf Computer und Netzwerke für jedermann in verständlicher Form kostenlos zur Verfügung stellt. Staat und Wirtschaft haben sich zusammengeschlossen, um den Bürgerinnen und Bürgern eine effektive Hilfestellung bei der Sicherung ihrer PCs und ihrer Netze zu bieten."*

132 http://www.bsi.bund.de/certbund/aufgaben.htm (30.05.2006).

In Anlehnung an das RFC 2450 wird die organisatorische Durchführung des CERT in einer Funktionsbeschreibung darstellt.[133] Informationen werden demnach vorwiegend über verschiedene Mailinglisten weitergegeben.[134] Hier interessierende Einzelheiten, wie der Zeitpunkt der Veröffentlichung, die Art und Weise der Beschreibung der Sicherheitslücke oder das Erfordernis eines Patches ist der Funktionsbeschreibung nicht zu entnehmen.[135] Es wird allerdings festgehalten, dass grundsätzlich *„keine Weitergabe konkret anlassbezogener Informationen (z. B. Name der Organisation, Typ des Vorfalls) ohne ausdrückliches Einverständnis aller Beteiligten an Dritte"*[136] erfolgt. Zudem wird darauf hingewiesen, dass die Menge der Warn- und Virenmeldung in Abhängigkeit von den Interessen der Rezipienten (Behörden) selektiert wird.[137] Dieser kurze Überblick soll deutlich machen, dass die Details der Informationen über Sicherheitslücken schwer zu fassen sind.

2. Instrumente der Informationsverwertung – Warnung, Aufklärung und Empfehlung

Öffentlichkeitsbezogene Informationstätigkeit des Staates lässt sich gliedern in Öffentlichkeitsarbeit und Aufklärung sowie Empfehlungen und Warnungen.[138] Soweit die Öffentlichkeitsarbeit als Werbung für die Staatstätigkeit begriffen wird und nicht als Tätigkeit der Gefahrenabwehr, wird sie nicht weiter untersucht.[139]

---

133 Vgl. http://www.bsi.bund.de/certbund/teaminfo/cb2350de.htm#5.1 (30.05.2006) und RFC 2350, Expectations for Computer Security Incident Response, 1998, http://www.ietf.org/rfc/rfc2350.txt (30.05.2006).

134 Dieser Warn- und Informationsdienst umfasst eine Mailingliste zu Virenwarnungen, eine über Sicherheitslücken und Schwachstellen in IT-Systemen sowie eine Veröffentlichung der Meldungen der Hersteller zu Sicherheitslücken und Schwachstellen, http://www.bsi.bund.de/certbund/infodienst/index.htm (30.05.2006).

135 Vgl. 5.1.2., http://www.bsi.bund.de/certbund/teaminfo/cb2350de.htm#5.1 (30.05.2006).

136 Vgl. 4.2., http://www.bsi.bund.de/certbund/teaminfo/cb2350de.htm#4.2 (30.05.2006).

137 Vgl. 5.1.2., http://www.bsi.bund.de/certbund/teaminfo/cb2350de.htm#5.1 (30.05.2006).

138 Lüdemann, Edukatorisches Staatshandeln, 2002, S. 87; a.A. Gusy, Verwaltung durch Information, in: NJW 2000, 977 (978), der die Öffentlichkeitsarbeit als Oberbegriff versteht. Ein ähnlich weites Verständnis von Öffentlichkeitsarbeit wird etwa vom BVerwG vorausgesetzt, wenn es ausführt: *„Die verfassungsrechtlichen Befugnisse der Bundesregierung zur Information und Aufklärung der Öffentlichkeit (sog. Öffentlichkeitsarbeit) schließen das Recht zu öffentlichen Warnungen ein."*, BVerwG „TM-Bewegung", Entscheidung v. 23.05.1989, 7 C 2/87, NJW 1989, 2272 (2272). Letztendlich hat sich in diesem Bereich keine einheitliche Begriffsverwendung durchgesetzt.

139 Auf eine weitere Thematisierung in diesem Kontext kann verzichtet werden, da eine so verstandene Öffentlichkeitsarbeit nur eine Information über die Staatstätigkeit und keine Staatstätigkeit selbst ist. In diesem Sinne auch Lüdemann, Edukatorisches Staatshandeln, 2002, S. 89 f.

Neben Aufklärung, Empfehlungen und Warnungen könnten Informationen über Sicherheitslücken begrifflich auch Beratung, Hinweis, Stellungnahme und Veröffentlichung umfassen. Mit unterschiedlicher Konnotation bezeichnen diese Begriffe Informationsvorgänge, die sich im rechtlichen Kontext wieder finden.[140] In ihrer Gesamtheit bezeichnen sie Erscheinungsformen, die der schlicht-hoheitlichen Verwaltungstätigkeit zugerechnet werden können.[141] In einer steuerungstheoretischen Betrachtung werden diese Instrumente auch als Risikokommunikation der Risikoprävention zugerechnet.[142]

a) Warnung

Der Begriff der „Warnung" soll einen unbestimmten Personenkreis vor Schäden schützen und ist eine Präventivmaßnahme, die thematisch dem Polizei- und Sicherheitsrecht zugeordnet werden kann.[143] Die Warnung ist auf den Schutz von Rechtsgütern wie Leben, Gesundheit und Eigentum oder den Schutz der Rechtsordnung gerichtet und ist somit grundsätzlich ein Instrument der Gefahrenabwehr. Sie stellt eine Handlungsmöglichkeit in Aussicht, ohne dem Adressaten eine bestimmte Handlungspflicht aufzuerlegen[144] oder eine Sanktion bei Nichtbefolgung in Aussicht zu stellen. Ihre Durchsetzungskraft ist bedingt von der faktischen Kraft des Inhalts der Warnung.[145] Soweit sachlich ein konkret gefährdendes Produkt (na-

---

140 Aufklärung: etwa § 2 Nr. 2 Abs. 1 UBAG (Gesetz über die Errichtung eines Umweltbundesamtes); Beratung: § 3 Abs. 1 Nr. 7 BSIG, diese ist ein individualbezogenes Verwaltungshandeln, weshalb sie hier grundsätzlich nicht in Betracht kommt; Empfehlung: etwa § 9 Abs. 1 Strahlenschutzvorsorgegesetz; Hinweis: dieser soll kein bestimmtes Verhalten aufzeigen und ist damit als Steuerungsinstrument nicht geeignet, vgl. Kloepfer, Staatliche Informationen, 1998, S. 17; Warnung: § 69 Abs. 4 AMG.

141 Schulte, Schlichtes Verwaltungshandeln, 1995, S. 18 ff., ein Unterfall sei das informale Verwaltungshandeln (a.a.O., S. 27.).

142 Scherzberg, Risikosteuerung durch Verwaltungsrecht, in: VVDStRL 63 (2004), S. 214 (255).

143 Voitl, Behördliche Warnkompetenz, 1993, S. 13, der die Öffentlichkeitswarnung durch eine konkrete Gefährdungslage veranlasst sieht. Konkret vgl. etwa § 28 Abs. 4 Medizinproduktegesetz. Zur Warnung im Sicherheitsrecht: Heintzen, Behördliches Informationshandeln, in: NuR 1991, 301 (303); Voitl, Behördliche Warnkompetenz, 1993, S. 27 f.

144 Keine faktische Durchsetzungskraft entfaltet die Warnung, wenn die Ziele der staatlichen Informationspolitik den tatsächlichen Informationsbedürfnissen der Verbraucher nicht entsprechen (Beispiel Rauchen), vgl. Lell, Umweltbezogene Produktkennzeichnung, 2003, S. 40. Darüber hinaus können Warnungen, deren Beachtung aus Eigeninteresse geboten ist und solche, deren Beachtung dem Allgemeinwohl dient, unterschiedliche faktische Durchsetzungskraft haben, vgl. Lüdemann, Edukatorisches Staatshandeln, 2002, S. 93 f.

145 Kloepfer, Staatliche Informationstätigkeit, 1998, S. 17; Leidinger, Hoheitliche Warnungen, Empfehlungen und Hinweise, in: DÖV 1993, 925, (926); Heintzen, a.a.O., (Fn. 143), 301, (303); Gusy, Verwaltung durch Information, in: NJW 2000, 977 (982 ff.); zur Einordnung

mentlich etwa die Software eines konkreten Herstellers) benannt wird oder wenn lediglich Modifikationen in den Einstellungen eines konkreten Produkts angeregt werden, kann eine Warnung in diesem Sinne verstanden vorliegen.

b) Aufklärung

Aufklärung setzt im (zivil)rechtlichen Kontext meist ein konkretes Verfahren oder individuelles Sonderverhältnis voraus.[146] Von öffentlicher Stelle abgegeben, zielt sie auf die Bewusstseinsbildung des Individuums.[147]

Regelmäßig bezieht sich die Aufklärung nicht auf ein konkret gefährliches Rechtssubjekt (etwa die allgemeine AIDS-Aufklärungskampagne).[148] In der fehlenden Konkretisierung eines Grundrechtsträgers soll sich die Aufklärung von der Warnung unterscheiden. Mit § 1 S. 3 SGB V oder § 7 Abs. 1 SGB XI etwa kann belegt werden, dass Aufklärung in der Rechtsordnung vielmehr als Hilfe zum eigenverantwortlichen Handeln eingesetzt wird.[149] Für ein IT-Sicherheitsrecht, das auch auf die Mithilfe und (Eigen)Verantwortung des Einzelnen angewiesen ist, könnte demnach der Begriff Aufklärung – so verstanden – eine zutreffende Bezeichnung für Informationen über Sicherheitslücken sein. Allerdings ist die Motivation „Hilfe zur Selbsthilfe“ auch bei Warnungen zutreffend, soweit diese eine lediglich faktische Durchsetzungskraft haben.

c) Empfehlung

Während die Warnung auf das Unterlassen einer bestimmten Handlung oder der Nutzung eines Produkts gerichtet ist, soll die Empfehlung die Kundgabe einer staatlichen Präferenz, die auf eine bestimmte Handlung (Verhaltensempfehlung) oder ein Produkt (Produktempfehlung) ausgerichtet ist, sein.[150] Empfehlungen können dann dem Rechtsgüterschutz dienen, wenn der Schutz gerade durch die Konkretisierung von Schutzmaßnahmen oder -produkten erfolgen soll.

---

behördlicher Informationen als Tathandlung und damit schlicht-hoheitliches Handeln, Philipp, Staatliche Verbraucherinformationen, 1989, S. 10.

146 Vgl. § 7 Abs. 2 S. 4 Hessisches Datenschutzgesetz; § 139 ZPO; BGH, Urteil v. 4. 4. 2001 - VIII ZR, NJW 2001, 2163.

147 Gröschner, Öffentlichkeitsaufklärung, in: DVBl. 1990, 619 (620).

148 Zur Aufklärung, Kloepfer, Staatliche Information, 1998, S. 15; eine Normierung der Öffentlichkeitsaufklärung findet sich etwa in § 2 Abs. 1 Nr. 2 UBAG.

149 Gröschner, Öffentlichkeitsaufklärung, in: DVBl. 1990, 619 (621).

150 Kloepfer, Staatliche Informationen, 1998, S. 16.

Die Empfehlung eines bestimmten Produktes kann nicht zuletzt eine Maßnahme der Wirtschaftssteuerung sein, und geht damit über ein rein gefahrenpräventives Handeln hinaus.[151] Wenn die Funktion der Gefahrenabwehr bereits durch eine Warnung zu erfüllen ist, bedarf es in der Regel keiner konkreten Produktempfehlung.

Eine bloße Verhaltensempfehlung verlässt indes den Bereich der Gefahrenabwehr (so sie diesem Bereich überhaupt zugerechnet werden kann) in der Regel nicht, soweit sie nicht ein bestimmbares Produkt bezeichnet, vgl. § 9 Abs. 1 Strahlenschutzvorsorgegesetz. Soweit ein konkretes Produkt empfohlen wird, kann ein Eingriff in die Wettbewerbsgrundrechte konkurrierender Hersteller vorliegen, womit eine gesetzliche Grundlage erforderlich wird.[152] Zum Teil wird die Produktempfehlung einer Warnung vor einem Produkt in ihren Grundsätzen und (verfassungs)rechtlichen Vorgaben gleichgesetzt.[153] Empfehlungen sollen der Natur nach durch die staatliche Autorität auch immer eine Warnung vor den nicht empfohlenen Produkten und Verhaltensweisen enthalten.[154] Soweit ein bestimmtes Produkt empfohlen wird, entsprechen sich Warnung und Empfehlung.[155] Bei gleichem Inhalt wird mit der Warnung nur eine eindringlichere Ausdrucksweise gewählt. Insoweit decken sich die Ausführungen zu Warnungen und Empfehlungen.

Soweit Empfehlungen sich nicht auf ein bestimmtes Produkt beziehen (Verhaltensempfehlungen), können sie in ihrer Wirkung entsprechend der Aufklärung zu beurteilen sein.[156]

d) Warnung, Aufklärung, Empfehlung und IT-Sicherheit

Neben der nicht immer trennscharfen Unterscheidung zwischen der Warnung vor einem bestimmten Produkt und der Empfehlung eines anderen Produkts sind beide Äußerungen – wie die Informationstätigkeit an sich – von einer Eigendynamik

---

151 Eine wirtschaftssteuernde Funktion könnte bereits die Warnung vor einem bestimmten Produkt haben.

152 Gröschner, Öffentlichkeitsaufklärung, in: DVBl. 1990, 619 (622), räumt der Empfehlung eine Mittelstellung zwischen Warnung (Befugnisnorm erforderlich) und Aufklärung (Aufgabe ausreichend, keine Befugnisnorm erforderlich) ein.

153 Gröschner, Öffentlichkeitsaufklärung, in: DVBl. 1990, 619 (621).

154 Gröschner, Öffentlichkeitsaufklärung, in: DVBl. 1990, 619 (621).

155 Die Empfehlung etwa Virenschutzprogramme zu installieren, entspricht der Warnung, niemals ohne Virenschutzprogramme zu surfen.

156 Gröschner, Öffentlichkeitsaufklärung, in: DVBl. 1990, 619 (621).

durch die *„Multiplikation und Verzerrung durch die Medien"*[157] gekennzeichnet. So wurde etwa in der Äußerung des BSI einen bestimmten Browser nicht zu benutzen, implizit eine Empfehlung des BSI gesehen, bestimmte Browser zu benutzen.[158] Auch aus diesem Grund ist es geboten Warnung und Empfehlung grundsätzlich gleichzusetzen.

Staatliche Informationen im hier interessierenden Bereich sind etwa die (Viren)Meldungen des BSI[159] und die Informationen zu Browsern (vgl. Szenario 1). Virenwarnungen sind grammatisch sind zwar Warnungen. Soweit allerdings kein konkretes Softwareprodukt als Virenträger genannt werden kann, sind Virenwarnungen „Aufklärung" im hier dargelegten Sinne, auch wenn regelmäßig nur eine spezifische

---

157 Tremmel/Nolte, Amtshaftung wegen behördlicher Warnungen, in: NJW 1997, 2256 (2256). Vgl. auch VG Köln, Beschluss v. 11.03.1999 – 20 L 3737/98, CR 1999, 557 (558), dem eine Beurteilung von warnenden Äußerungen des Bundesdatenschutzbeauftragten zu Grunde liegt, denen trotz Nicht-Nennung des betroffenen Unternehmens eine grundrechtsbeeinträchtigende Wirkung bescheinigt wurden, da das Unternehmen in der anschließenden Diskussion in den Medien namentlich genannt wurde.

158 Im Bereich der IT-Sicherheit wurde von staatlichen Stellen in den USA und in Deutschland vor der Nutzung des Internet Explorers gewarnt und gleichzeitig alternative Browser empfohlen. In den USA empfahl das US-Cert die Nutzung eines anderen Browser, ohne jedoch einen bestimmten Browser zu nennen, Vulnerability Note VU 713878, 09.08.2004, http://www.kb.cert.org/vuls/id/713878 (30.05.2006). Obwohl keine konkrete Präferenz für ein Produkt ausgesprochen wurde, haben nach der Veröffentlichung die Downloads von Mozilla-Browsern merklich zugenommen, vgl. auch Computerbase news vom 03.07.2004, http://www.computerbase.de/news/software/browser/2004/juli/us-regierung_internet_-explorer/ (30.05.2006). Dies wohl nicht zuletzt aufgrund der weltweiten Rezeption. Die Empfehlung des US-Cert wurde selbst in der deutschen Presse rezipiert. So ist sie etwa einem Artikel in Spiegel Online zu entnehmen, Spiegel Online vom 08.07.2004, http://www.spiegel.de/netzwelt/technologie/0,1518,307447,00.html (30.05.2006). Ähnlich informierte der Pressesprecher des BSI und empfahl in einem Zeitungsinterview mit der Berliner Zeitung die Nutzung anderer Browser, Wendel, Thomas, Warnung vor Internet-Banking, Berliner Zeitung, 11.09.2004. In anderen Artikel wurde diese Meldung als direkte Empfehlung von Mozilla und Opera weiterverbreitet. Der Pressesprecher, der für einen Mischwald aus Browsern votierte, wurde immer wieder mit einer Empfehlung für die alternativen Browser zitiert, vgl. heise news vom 11.09.2004, http://www.heise.de/newsticker/meldung/50965 (30.05.2006); Handelsblatt.com vom 13.09.2004, „Virenschutz durch Browser-Wechsel", http://www.handelsblatt.com/pshb/-fn/relhbi/sfn/cn_artikel_drucken/strucid/PAGE_200104/pageid/PAGE_204016/docid/789463/SH/0/depot/0/ (30.05.2006); tecchannel vom 12.09.2004, „Bundesamt warnt vor Internet Explorer", http://www.tecchannel.de/news/internet/17221/ (30.05.2006); Börsenreport vom 12.09.2004, „Das BSI rät: Gegen Viren und Würmer verwenden sie MOZILLA oder OPERA", http://www.boersenreport.de/technikmedien.asp?msg=0041764-00000001640000000000 (30.05.2006); n-tv vom 11.09.2004 „Bundesamt empfiehlt auch Mozilla und Opera nutzen", http://www.n-tv.de/5423591.html (30.05.2006).

159 Vgl. Newsletter des BSI mit aktuellen Sicherheitsinformationen, http://www.bsi-fuer-buerger.de/index.htm (30.05.2006).

Software Angriffsziel ist. Die Informationen über den Browser in Szenario 1 zielen auf Sicherheitslücken, die unabhängig von dem bestimmten Produkt eines Herstellers der Produktgattung zu Eigen sind, und sind damit Aufklärung im hier verstanden Sinn. Soweit sie auf Sicherheitslücken des konkreten Produkts zielen, ist dies als Warnung zu qualifizieren. Eine ausführliche Diskussion erfolgt unter Kapitel 5 B IV.

Die Informationstätigkeit des Staates im Bereich der IT-Sicherheit kann letztendlich allen genannten Formen der Informationstätigkeit zugeordnet werden. Die Wahl des Begriffes ist eine Frage der Subsumtion im Einzelfall. Als Instrumente der Informationsweitergabe sollen demnach die Aufklärung, Empfehlungen und Warnungen als Informationstätigkeit genauer betrachtet werden, da sie theoretisch alle geeignet sind, konkrete Sicherheitslücken bzw. Alternativen zu diesen der Allgemeinheit aufzuzeigen.

3. Instrumente der Informationsverwertung – Qualitätssicherung durch Empfehlung

Staatliche Empfehlungen im weiteren Sinn sind staatliche vorgegebene Zertifizierungs- und Evaluationsverfahren. Gütesiegel wie etwa der „Blaue Umweltengel“[160] oder das „Bio-Siegel“[161] können Empfehlungen „institutionalisieren“. Im Bereich Datenschutz und Datensicherheit gibt es das Datenschutz-Gütesiegel[162]. Hierbei wird die Vereinbarkeit eines Produkts mit den Vorschriften zum Datenschutz und

---

160 Inhaber des Zeichens der „Blauer Engel“ ist das Bundesministerium für Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit. An dem Vergabeverfahren sind zudem die Jury-Umweltzeichen mit privaten und öffentlichen Vertretern, das RAL Deutsches Institut für Gütesicherung und Kennzeichnung e.V. als Zeichenvergabestelle und das Umweltbundesamt beteiligt. Aufgrund diesem organisatorischen Zusammenwirken kann der „Blauer Engel“ nicht als private Informationstätigkeit gesehen werden, sondern muss als eine Produktwerbung angesehen werden, die dem öffentlichen Recht zuzurechnen ist, Di Fabio, Information als hoheitliches Gestaltungsmittel, in: Jus, 1997, 1. (3); Kloepfer, Staatliche Informationen, 1998, S. 24.

161 Das staatliche Bio-Siegel hat seine gesetzlichen Grundlagen in dem Öko-Kennzeichengesetz. Inhaber der Marke ist das Bundesministerium für Verbraucherschutz, Ernährung und Landwirtschaft. Die unberechtigte Verwendung wird durch eine Anzeigepflicht nach § 3 Öko-Kennzeichenverordnung gesichert und unter Strafe gestellt.

162 Inhalt, Ausgestaltung und das Verfahren der Vergabe werden nach § 4 Abs. 2 Landesdatenschutzgesetz (LDSG) Schleswig-Holstein i.V.m. der Datenschutzaudioverordnung geregelt. Produkte, die dieses Gütesiegel tragen, sollen nach § 4 Abs. 2 LDS in Behörden vorrangig eingesetzt werden.

zur Datensicherheit zertifiziert. Bisher wird ein solches Siegel nur vom ULD Schleswig-Holstein[163] verliehen.

Zertifizierungen können als Verfahren bezeichnet werden, mit denen die Einhaltung bestimmter IT-Sicherheitsstandards für Produkte/Dienstleistungen und ihre jeweiligen Herstellungsverfahren nachgewiesen werden. Sie verschaffen dem Nutzer Informationen über die Sicherheitsqualität eines Produkts. Dementsprechend werden Zertifizierungen eingeschätzt:

> *„Schon eine Zertifizierung auf der untersten Stufe EAL1 nach den Common Criteria ist für den Endnutzer eine wertvolle Aussage hinsichtlich der Sicherheit des eingesetzten Produktes, die schon weit über die gängigen Produkttests, wie sie in technischen Zeitschriften zu finden sind, hinausgeht."*[164]

Das BSI vergibt Zertifikate für unterschiedliche Arten von Zertifizierungen.[165] Die Zertifizierung nach technischen Normenwerken – etwa ITSEC[166] und Common Criteria (CC) – wurde durch staatliche Abkommen zur Anerkennung der IT-Sicherheitszertifikate, die auf den entsprechenden Standards beruhen, abgesichert.[167]

---

163 Das Unabhängige Landeszentrum für den Datenschutz (ULD) ist die „Dienststelle" des Datenschutzbeauftragten von Schleswig-Holstein, nach § 32 ff. LDSG. Als gesetzlich vorgesehene Aufsichtsbehörde nach § 39 LDSG entwickelte sich das ULD zu einem Innovationszentrum, vgl. 26. Tätigkeitsbericht des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein 2004, Landtagsdrucksache vom 06.05.2004, 15/3300, S. 9.

164 Auf die Frage, Was nützt mir als Endnutzer die Zertifizierung eines Produkts?, unter http://www.bsi.de/faq/zertifizierung.htm#a6001 (30.05.2006). Andere Ansicht etwa Gehring, Software Development, Intellectual Property, and IT Security, in: Journal of Information Law & Technology 2003, Issue 1, http://elj.warwick.ac.uk/jilt/03-1/gehring.htm (30.05.2006), *„Certification, as it is often proposed to close the information gap, will not be successful under the existing regulative framework (…)"*. Die Tatsache, dass der Hersteller des Produkts die Kosten der Zertifizierung zu tragen hat, könnte zu einem zum Ausverkauf der Zertifizierung führen (geringste Gebühr, kürzeste und einfachste Zertifizierung, etc.). Zum anderen verringert die Zertifizierung die Chance auf vollständige Informationen zu dem Produkt: „*A Common Criteria certificate might make a court much less ready to order disclosure, and thus could severely prejudice your rights.*", Anderson, Why Information Security is hard – an Economic perspective, 2001, http://www.cl.cam.ac.uk/ftp/users/rja14/econ.pdf (30.05.2006).

165 Unter http://www.bsi.de/faq/zertifizierung.htm#a6001 (30.05.2006) gibt das BSI einen Überblick.

166 Information Technology Security Evaluation Criteria.

167 Vgl. „Sogis-Abkommen über die Gegenseitige Anerkennung von IT-Sicherheitszertifikaten auf Grundlage der ITSEC" vom 18.03.1998. Es wurde von den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen, Portugal, Schweden, Schweiz und Spanien. Das Abkommen wurde zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der Evaluationsstufe EAL7 erweitert. Weitere Informationen: BSI-Zertifizierung und BSI-Produkt-Bestätigung, Hinweise für Hersteller und Vertreiber, August 2004, S. 5, http://www.bsi.de/zertifiz/zert/7138.pdf (30.05.2006). Vgl. „Common Criteria Mutual Recognition Arrangement" über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten und Schutzprofilen auf Basis der CC bis einschließlich der Vertrau-

Nicht zuletzt ist die Zertifizierung von IT-Sicherheitskriterien in einem amtlichen Zertifizierungsreport festgehalten und daher als staatlich zu betrachten.[168] In dem Report werden insbesondere die Details der vergebenen Zertifikate veröffentlicht und bieten dem Nutzer eine Gelegenheit, sich über die Qualität von Produkt- und Kommunikations- und Netzsicherheit von Produkten und Systemen zu informieren.[169]

Im Bereich der IT-Sicherheit gibt es darüber hinaus private Evaluationsverfahren beim TÜV, etwa im Bereich der Produktsicherheit die allgemeine Siegel CE (§ 6 GPSG) und GS (§ 7 GPSG), die Aufschluss über die Gewährleistung bestimmter Sicherheitsstandards geben können.

II. Informationsbegrenzung

Staatliche Informationstätigkeit ist die Informationsbeschaffung und -verteilung. Darüber hinaus kann der Staat Informationsvorgänge begrenzen. Diese Informationsbegrenzung soll als weitere Alternative staatlicher Informationstätigkeit im Bereich von IT-Sicherheitslücken angeführt werden.

Eine Begrenzung kann bei Informationsmängeln erforderlich werden. Soweit der Inhalt der Information (objektiv) unwahr, schädlich oder kontraproduktiv ist, kann der Staat je nach Relevanz für gefährdete Rechtsgüter verpflichtet sein, diese Qualitätsmängel oder den Informationsvorgang zu unterbinden.

Dies kann die Information über Sicherheitslücken betreffen, wenn etwa feststeht, dass die Offenbarung von Sicherheitslücken kontraproduktiv ist. Dies ist der Fall, wenn erst die Offenbarung der Sicherheitslücke die Ausnutzung derselben ermöglicht. So wenn so genannte Exploits, Programme zum Ausnutzen der Sicherheitslücke, aufgrund der technischen Information über die Lücke oder im Umkehrschluss

---

enswürdigkeitsstufe EAL 4 zwischen den nationalen Stellen in Australien, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Kanada, Neuseeland, Niederlande, Norwegen, Spanien und den USA unterzeichnet. Im November 2000 ist Israel der Vereinbarung beigetreten, Schweden im Februar 2002, Österreich im November 2002, Ungarn und Türkei im September 2003, Japan im November 2003.

168 BSI-Zertifizierung und BSI-Produkt-Bestätigung, Hinweise für Hersteller und Vertreiber, a.a.O., (Fn. 167).

169 Einen Überblick zu den vergebenen Zertifikaten: BSI, Deutsche IT-Sicherheitszertifikate Sicherheit von IT-Produkten und –Systemen, vom September 2004, http://www.bsi.de/-zertifiz/zert/7148.pdf (30.05.2006), Die detaillierten Zertifizierungsreports finden sich unter http://www.bsi.de/zertifiz/zert/report.htm (30.05.2006).

aus den Hinweisen zum Schließen der Lücke erst geschrieben werden (können).[170] Dies ist eine zentrale Frage im Rahmen der Verkehrssicherungspflicht, vgl. Kapitel 5 C III. 2. b) cc).

Für die Untersagung des grundsätzlich bestehenden und grundgesetzlich geschützten Rechts zu informieren (Art. 5 Abs. 1 S. 1 1. und 2. Alt. GG) bedarf es einer spezialgesetzlichen Ermächtigungsgrundlage. Eine solche besteht nicht. Man könnte allenfalls ein Verbot aus der Generalklausel im Sicherheits- und Ordnungsrecht der Länder in Betracht ziehen.[171] Darüber hinaus kommt im Fall von Betriebs- und Geschäftsgeheimnissen eine der dort erwähnten Informationsbegrenzungen aus dem Straf-, Zivil- und Wettbewerbsrecht in Betracht.[172] Im Zivil- und Wettbewerbsrecht gibt der Staat nur einen Rechtsrahmen und damit die Möglichkeit der Begrenzung vor, das tatsächliche Unterbinden und die Realisierung der Informationsbegrenzung liegen grundsätzlich in privaten Händen.

Für ein IT-Sicherheitsrecht kann grundsätzlich festgehalten werden, dass eine Informationsbegrenzung, d. h. letztlich auch eine Einschränkung des Rechts zu informieren, nur in Ausnahmefällen existiert. Im Regelfall besteht ein grundsätzliches Recht des Einzelnen, über IT-Sicherheitslücken zu informieren. Dies gilt auch, soweit diese Information die mehrfach angesprochene ambivalente Wirkung zeitigt.

D Ergebnis

Information über Sicherheitslücken im Internet strebt das Steuerungsziel der Sicherheit im Internet an. Zur Erreichung dieses Ziels kann sich das Steuerungssubjekt der Steuerungsmedien Recht und Information bedienen.

Für die Steuerung durch Information und Recht lässt sich Folgendes festhalten: Die typischerweise propagierte Hilflosigkeit des Rechts gegenüber dem Internet kann jedenfalls für Informationsrechte und –pflichten bei Sicherheitslücken nicht zu Grunde gelegt werden. Allerdings ist eine Informationspflicht sinnvoll mit der Inhaltsvorgabe zu verknüpfen, Abhilfemöglichkeit oder Patches zu veröffentlichen.

---

170 So geschehen bei der Programmierung des Sasser-Virus. Mit Hilfe der Darstellung der Sicherheitslücke (im konkreten Fall eine bloße Veröffentlichung der Sicherheitslücke, ohne Schadfunktion) im Local Security Authority Subsystem Service (LSASS) wurde der Sasser-Virus im Jahr 2004 geschrieben, vlg. Tatbestand bei LG Verden, Urteil v. 08.07.2005 – 3-5/05.

171 In Hessen etwa § 11 HSOG.

172 Vgl. Kapitel 3 A II. 1.

Darüber hinaus sind die Steuerungsinstrumente der Medien Information und Recht in ihrer zeitlichen Komponente neben der etablierten Einteilung ex post und ex ante durch eine Kategorie „in operatione" zu ergänzen. In dieser Phase müssen Mechanismen zum Umgang mit Unsicherheiten etabliert werden, die ein Ausnützen der „sicheren Unsicherheit" durch Dritte verhindern, damit die Sicherheit in der Anwendung (wieder) hergestellt werden kann. Das Recht kann in dieser Phase nur mittelbar einen Beitrag zur Sicherheit des Internets leisten, da es Handlungsoptionen eröffnet.

Ein weiterer Aspekt der Steuerungsinstrumente von Information und Recht für das hier angestrebte Steuerungsziel ist die Frage des Anstoßes des Informationsvorgangs. Ein solcher muss im Bereich der Informationen über Sicherheitslücken situativ-initiativ von demjenigen erfolgen, der sich im „Erfahrensbereich" der Sicherheitslücke befindet. Damit scheidet etwa eine Auskunftspflicht des Herstellers oder Anbieters gegenüber dem Nutzer aus. Eine Anzeigepflicht hängt von der Initiative (Anzeige oder Meldung) desjenigen ab, der die Realisierung einer Gefahr entdeckt.

Die staatliche Informationstätigkeit im technischen Bereich kann zum einen als durch die zeitlichen Komponenten der „legal lag" und des „legal age" geprägt, zum anderen durch eine grundsätzliche „information gap" des Staates als erforderlich angesehen werden. Zentral ist hier die Generierung und Verwertung von Wissen. Der Fokus der Organisation der staatlichen Informationsbeschaffung und –verwertung liegt auf dem CERT als Informationszentrum. Einzelheiten der Art und Weise der Verwertung von Informationen über Sicherheitslücken finden sich hier allerdings kaum.

Der Fokus liegt dabei auf eine Informationsverwertung, die sich an die Allgemeinheit richtet, da im Bereich der IT-Sicherheitslücken ein *„individualbezogenes Informationshandeln"* unergiebig erscheint. Demnach beschäftigt sich die staatliche Steuerung des Informationsvorgangs bei Sicherheitslücken im Internet mit den Steuerungsinstrumenten der Aufklärung, Warnung und Empfehlung. Diese können allerdings ihre intendierte steuernde Wirkung durch eine Eigendynamik und die Verzerrung durch die medial organisierten Rezipienten einbüßen.

KAPITEL 5 ZUM BEITRAG VON INFORMATIONSRECHTEN UND –PFLICHTEN – EIN IT-INFORMATIONSRECHT

In diesem Abschnitt sollen nun die Informationsrechte und –pflichten „rund um die Sicherheitslücke“ dargestellt werden. Da die unterschiedlichen Ausprägungen und Konstellationen grundsätzlich eine Bestimmung der Rechte und Pflichten als Einzelfallentscheidungen indizieren, sollen soweit möglich diese unter Rückgriff auf die Szenarien in Kapitel 1 getroffen werden.

Dort, wo die Optimierung von Sicherheit außerhalb der Kontrolle und des Entscheidungs- und Einwirkungsbereichs des Nutzers liegt[1] – er also grundsätzlich keine Eigenverantwortung übernehmen kann – kann diese strukturelle Verantwortungslücke durch Informationsrechte und -pflichten ausgeglichen werden. Voraussetzung ist allerdings, dass es sich tatsächlich um eine strukturelle Verantwortungslücke – Verantwortung kann mangels Informationen nicht übernommen werden – und nicht um eine personelle Sicherheitslücke, die aufgrund des Fehlverhaltens des Nutzers – etwa Missachtung von Informationen – entstanden ist, handelt.

Es wurde davon abgesehen, Informationspflichten des Staates in einem getrennten Kapitel zu behandeln. Damit soll deutlich gemacht werden, dass der Staat im Internet – unabhängig von seiner sonstigen dichotomischen Abgrenzung zum Bürger – mit den Anbietern, Herstellern und Nutzern hinsichtlich des Umgangs mit diesen sicherheitsrelevanten Informationen im Grundsatz gleichgestellt werden kann. Soweit bei den Informationsrechten – etwa bei der Beurteilung der Warnung durch den Staat – Ausnahmen indiziert sind, werden diese für sich untersucht.

Zunächst soll – unter Teil A – durch ein exemplarisches Heranziehen von Informationsrechten und –pflichten Sinn und Zweck von Informationsrechten und –pflichten im Allgemeinen herausgearbeitet werden, bevor – unter Teil B und C – auf die Informationsrechte und –pflichten bei Sicherheitslücken im Internet im Besonderen eingegangen wird. Inhaltlich werden diese bei proprietärer Software hervorgehoben, da sie von erheblicher praktischer Relevanz sind. Abschließend soll unter Teil D ein IT-Informationsrecht mittels zusammenwirkender Informationsrechte und –pflichte nach dem GPSG dargestellt werden.

---

[1] Nach Schneier ist dies der Regelfall: „*The sad truth is that most security problems are just not under the control of most people.*“, Schneier, Secrety & Lies, 2000, S. 350. Der an anderer Stelle auch den Menschen als größte Sicherheitslücke bezeichnet (a.a.O., S. 255: *„weakest link in the security chain*“).

A Informationsrechte und –pflichten

Informationsrechte und –pflichten können am Informationsvorgang orientiert entwickelt werden. Informationsrechte können intransitiv als das Recht zu informieren und transitiv als das Recht sich zu informieren verbalisiert werden. Ebenso können Informationspflichten intransitiv als Pflicht zu informieren und transitiv als Pflicht sich zu informieren verbalisiert werden. Mit dieser Verbalisierung tritt allerdings nicht unbedingt eine Konkretisierung ein.

Eine Konkretisierung soll im Folgenden mit Nominalformen versucht werden, etwa einem Auskunftsrecht, einer Aufklärungspflicht, einer Überwachungspflicht, etc. Hierbei sind weniger die konkreten Regelungen als solche von Interesse, sondern die dabei gewonnenen Erkenntnisse, die für und wider erforderlicher Informationsrechte und –pflichten bei Vorliegen von Sicherheitslücken streiten können.

Ob von einem Informationsrecht[2] oder von einer Informationspflicht zu sprechen ist, ist neben der normativen Ausprägung im Gesetz eine Frage des Standpunktes und der Verfasstheit des Wissenden und des Wissenwollenden teilweise auch des Wissensollenden. Der Informationsvorgang selbst bedarf einer Initiative des Informierenden oder Rezipienten.[3] Um korrespondierende Informationspflichten und –rechte abgrenzen zu können, soll unter Informationspflicht primär eine Pflicht verstanden werden, die ein initiativ-aktives Tun des Verpflichteten erfordert, d. h. eine Pflicht, die unabhängig von der Geltendmachung des Anspruchs besteht.[4] Dementsprechend ist ein Informationsrecht initiativ-aktiv vom Berechtigten wahrzunehmen.

---

2 Grundsätzlich wird der Plural von Informationsrecht in diesem Kontext bevorzugt. Kloepfer differenziert zwischen dem Informationsrecht im engeren Sinn, als Recht der Informationsinhalte, -vorgänge und –zustände, was bereits die „Uferlosigkeit" andeutet, die er dem Informationsrecht im weiteren Sinne zugesteht, Kloepfer, Informationsrecht, 2002, § 1 Rd. 67 und 76.

3 Im Gegensatz zu der wechselbezüglichen Komponente von Kommunikation bedarf das Recht zu informieren nicht notwendigerweise einen Rezipienten. Die Information ist hierbei nur ein Angebot, dessen Wahrnehmung von weiteren Faktoren abhängig ist.

4 So ist etwa die Belehrungspflicht des Richters nach § 53 Abs. 2 StPO initiativ-aktiv vom Richter (Wissender) wahrzunehmen. Das Recht auf Akteneinsicht im Verwaltungsrecht nach § 29 VwVfG initiativ-aktiv vom Wissenwollenden. Die Informationspflicht kann insofern ein Aufdrängen von Information sein, während die Wahrnehmung des Informationsrechts mit einem verantwortungsvollen Umgang mit Information im Sinne einer Informationsverantwortung begründet werden kann.

Eine Pflicht sich informieren oder zu informieren kann gedanklich jedoch nur dort gesetzlich, durch Richterrecht oder vertraglich (bzw. vorvertraglich) begründet werden, wo ein Wissensdefizit erkannt wurde oder hätte erkannt werden müssen.[5]

Teilweise wird vertreten, dass das Recht als „Flucht nach hinten" auf jegliche Normierung von Informationspflichten verzichten könne. Am freien Markt der Informationen solle die Regelung des Informationsflusses die Ausnahme bleiben und es müsse grundsätzlich Freiheit der Information gelten. Die mit rechtlichen Konsequenzen ausgestattete Informationspflicht bedürfe als Ausnahme stets einer besonderen Begründung.[6]

Auf den ersten Blick erscheint dies bezüglich Sicherheitslücken Realität zu sein, allerdings gebietet es der Rechtsgüterschutz, über konkrete Regelungen nachzudenken. Die Kehrseite der Freiheit der Information sind Unwägbarkeiten und Unsicherheiten. Die Gesellschaft und der Staat sind auf die Freiwilligkeit und die Verantwortung des Einzelnen, die Informationsasymmetrie auszugleichen, angewiesen. Rechte sich zu informieren und Pflichten zu informieren können jedoch bestimmte gesellschaftliche Funktionen und allgemeine Interessen realisieren und gewährleisten. Im Bereich der Sicherheitslücken, die sowohl Interessen der Allgemeinheit tangieren, als auch bei kritischen Infrastrukturen gesellschaftliche Bereiche „lahm legen" können, sind Regelungen im oben genannten Sinne erforderlich. Im Sinne einer begrenzenden Strategie könnte der Informationsvorgang situativ-initiativ von demjenigen angestoßen werden, dem eine Sicherheitslücke zuzurechnen ist, der sie beheben kann oder der eine Sicherheitslücke bemerkt.

Unabhängig von dem konkreten Bedeutungsgehalt von Informationsrechten und –pflichten kann für die anvisierte Fragestellung der Information über Sicherheitslücken die folgende Aussage herangezogen werden:

> *„Je globaler die Ordnung – sachlich und geographisch – desto weniger vermittelt sie subjektive Informierungsrechte."*[7]

---

5 Im Fall einer gesetzlichen Regelung hat der Gesetzgeber das Defizit erkannt. Für den vertraglichen Bereich etwa: BGH, Urteil v. 21.04.1994 - IX ZR 150/93, NJW 1994, 2293 (2293); BGH, Urteil v. 11.07.1991 - IX ZR 180/90, NJW 1991, 2839 (2841); ebenso: Fischer, Tendenzen der Rechtsprechung des BGH zum Anwaltshaftungsrecht, in: NJW 1999, 2993 (2994): Solange der Anwalt die Unrichtigkeiten der vorgetragenen Tatsachen des Mandanten nicht kenne oder kennen müsse, träfe ihn keine Pflichten eigene Nachforschungen anzustellen.

6 Loritz, Aufklärungs- und Informationsbeschaffungspflichten, in: NZG 2002, 889 (893).

7 Druey, Information als Gegenstand des Rechts, 1995, S. 218. Unter Informierungsrechten versteht Druey das Recht zu informieren. Als objektive Informierungsrechte nennt Druey

Übertragen auf die hier zu untersuchende Fragestellung können Infrastruktur und Anwendungen zu Gefahren in Relation gesetzt werden: Je globaler – sachlich und geographisch – die Gefahren verbreitet und systemimmanent zu begründen sind, desto sinnvoller sind objektive Informierungsrechte, d. h. Pflichten, die Allgemeinheit zu informieren.

Objektive Informierungsrechte können aber auch sinnvoll sein, wenn die Gefahren zentral zu lokalisieren und individuell begründbar (individuelle Nutzerfehler) sind und wenn solche Nutzerfehler zugleich global auftreten können.

Ein subjektives Recht auf Information (als Pflicht zu informieren oder als Recht sich zu informieren ausgestaltet), kann dann sinnvoll und ausreichend sein, wenn die Sicherheitslücken zentral zu lokalisieren sind und tatsächlich individuell begründbar sind (etwa die unzureichende Passwortvergabe zur Absicherung des Systems in einem Unternehmen).

I. Recht sich zu informieren

Das Recht sich zu informieren lässt sich mit einem institutionellen Aspekt, verfahrensgebunden oder als verfassungsmäßige Wertung einteilen.

In einer demokratischen Betrachtung ist das Recht des Bürgers sich zu informieren als Transparenzgebot des Staates zu verstehen und ist von seiner Konzeption daher der staatlichen Sphäre zuzuordnen und besitzt eine *„institutionelle Dimension"*[8]. Dieses Transparenzgebot wird von staatlichen und privaten Interessen an Geheimhaltung eingeschränkt. Diese Einschränkung und der Schutz der Geheimhaltung erfordern nicht zuletzt gesetzliche Regelungen des Zugangs zu Informationen.

In Sinne dieses Transparenzgebots wird das Recht sich zu informieren als Informationsfreiheit bezeichnet (Freedom of Information).[9] Eine Verallgemeinerung des Gebots als Beziehungsgebot unter Privaten ist aus zwei Gründen nicht selbstverständlich: Zum einen erfordert der Zugang zu Informationen von dem Wissen-

---

etwa den objektiven Vollzug des Bildungsauftrags durch den Lehrer (anstatt eines subjektiven Rechts des Schülers auf Bildung).

8 Druey, Information als Gegenstand des Rechts, 1995, S. 86.

9 Diese Informationsfreiheit ist in vielen Staaten, auf europäischer Ebene (etwa Art. 255 EG) und auf Länderebene und wird auf Bundesebene verankert. Die Gesetzesbemühungen reichen bis in die 60er Jahre zurück. Hier liegen mit der Entstehung des Freedom of Information Act (FOIA) von 1966 die Anfänge der Regelungen der Informationsfreiheit. Einen Überblick bietet: http://www.informationsfreiheit.de/index.htm (30.05.2006).

den unterstützende Maßnahmen (Zusammenstellung und Übermittlung der Information, Schutz von geheim zu haltender Information, etc.). Dem „wissenden Bürger“ solche Handlungspflichten gegen seinen Willen aufzuerlegen, erfordert eine (gesetzliche) Abwägung mit den Interessen des Wissenwollenden. Zum anderen sei der Informationszugang als verankerte Position der Staatskontrolle dem Individuum nicht um seiner selbst willen eingeräumt. Als Beziehungsgebot unter Privaten ist demnach das Recht sich zu informieren im Privatrecht nur in Ausnahmefällen zu finden.[10]

Das Recht sich zu informieren besteht neben den allgemeinen Informationsfreiheitsrechten[11] ebenso in abhängigen Auskunftsrechten gegenüber dem Staat, die in ein bestimmtes Verfahren eingebunden sind, etwa das Akteneinsichtsrecht gegenüber der Verwaltung (§ 29 VwVfG).

Informationsrechte sind nicht zuletzt Ausfluss einer verfassungsrechtlichen Wertung. So ist etwa das Recht nach § 34 BDSG gegenüber der verantwortlichen Stelle im Datenschutzrecht über gespeicherte personenbezogenen Daten Auskunft zu verlangen, auf die informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 S. 1 GG) zurückzuführen. Anknüpfend an das subjektive Recht ist diese Wertung in Normen mit Bezug zum öffentlichen und privaten Bereich parallel gehalten.[12]

Der Zugang zu staatlichen Informationen ist demnach institutionell begründet ein abhängiges Verfahrensrecht oder entspringt einer verfassungsrechtlichen Wertung. So wie die Informationsfreiheit institutionell begründet werden kann, kann privatrechtlich der Informationsvorgang organisationsrechtlich begründet werden. So

---

10 Aus Treu und Glauben können zur Durchsetzung von (Schadensersatz)Ansprüchen vorbereitende Auskunftsrechte gegenüber dem Vertragspartner bestehen, vgl. BGH, Urteil v. 13. 12. 2001 - I ZR 44/99, GRUR 2002, 602 (603); BGH, Urteil v. 28.11.1989 - VI ZR 63/89, NJW 1990, 1358 (1358). Eine weitere Ausnahme besteht beim Zugang zu Umweltinformationen. Hier haben Private einen Anspruch gegen natürliche und juristische Personen, soweit sie öffentliche Aufgaben wahrnehmen, Art. 2 Nr. 2 b), c) der Richtlinie 2003/4/EG über den Zugang zu Umweltinformationen vom 28.01.2003, ABl. L Nr. 41, vom 14.02.2003, S. 26.

11 Auf europäischer Ebene: Art. 255 EG, Verordnung Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30.05.2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (Informationszugangsverordnung) ABl. Nr. L 145, vom 31.05.2001, S. 43. Im deutschen Recht: das Umweltinformationsgesetz und die Informationsfreiheitsgesetze in Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein und des Bundes.

12 § 19 BDSG regelt das Auskunftsrecht gegenüber öffentliche Stellen und § 34 BDSG das Auskunftsrecht gegenüber nicht öffentliche Stellen.

kann etwa der Informationsanspruch des Aktionärs nach § 131 AktG bei Durchführung einer Hauptversammlung mit der „Optimierung der spezifischen Organisation „Aktiengesellschaft“[13] begründet werden. Insoweit ist ein Verfahrensrecht im Gesellschaftsrecht zu finden, regelmäßig fehlt es aber an vergleichbaren rechtlichen Verfahrensstrukturen in privaten Organisationen.[14] Neben den Referenzen zum institutionellen, verfahrensmäßigen oder wertungsabhängigen Informationszugang ist das Recht sich zu informieren im Privatrecht neben der Begründung durch Vertrag auch als „Hilfsanspruch“[15] denkbar.

Je kritischer der Informationsinhalt und je höher die „Sicherheitsstufe“ ist, desto weniger darf der Informationsvorgang als Recht sich zu informieren ausgestaltet werden, da hierbei die Information nicht notwendigerweise beim Rezipienten – da sie von dessen Initiative abhängig ist – ankommt. Dem möglichen Desinteresse und der mangelnden Initiative könnte durch die Etablierung bestimmter Schutzmaßnahmen und der Pflicht zu informieren entgegen getreten werden, etwa durch eine öffentliche Bekanntgabe am schwarzen Brett.

II. Recht zu informieren

Das Recht zu informieren ist das Recht, eine Information einem unbegrenzten oder begrenzten Personenkreis oder einer Person zugänglich zu machen. Dieses Zugänglichmachen von Information kann auf Interesse an der Information oder Interesse an der Verhinderung des Informationsvorgangs oder auf Desinteresse in Form von Gleichgültigkeit des Rezipienten oder Dritten stoßen. Es kann mithin auch auf Dritte stoßen, die ein bestimmtes Interesse haben, den Informationsvorgang zu verhindern, bzw. auf Rezipienten, die sich vor aufgedrängter Information schützen wollen.

Im Folgenden soll demnach das Recht zu informieren grundsätzlich von den Grenzen seiner Ausübung gekennzeichnet und konturiert werden. Das Recht zu informieren besteht, soweit das Recht keine Schranken aufzeigt. Staatliche Gren-

---

13 Druey, Information als Gegenstand des Rechts, 1995, S. 328. Das Entscheidende bei einem organisationsrechtlichen Auskunftsanspruch sei dabei nicht ein Über- oder Unterordnungsverhältnis, sondern der Einsatz des Beteiligten, den jeder in einer privatrechtlichen Organisation leistet, der seine Rolle im Ganzen bestimmt. So etwa der finanzielle Einsatz des Aktionärs in der Aktiengesellschaft.

14 Druey, a.a.O., (Fn. 13), S. 328, begründet dies mit der Organisationsautonomie.

15 Druey, a.a.O., (Fn. 13), S. 221, versteht unter dem sekundären Informationsanspruch diejenigen Hilfsansprüche, die zur Verwirklichung eines anderen rechtlichen Belangs dienen.

zen sind nur in den Schranken von Art. 5 II GG möglich. Die Schranken des Art. 5 II GG sind allgemeine Gesetze und gesetzliche Bestimmungen zum Schutz der Jugend und Ehre.

Im Privatrecht können grundsätzlich nur subjektive Rechte Dritter und des Rezipienten das Recht zu informieren begrenzen. Die Grenzen einer privaten Berichterstattung können etwa im allgemeinen Persönlichkeitsschutz[16] oder im Urheberrecht[17] liegen. Auch wirtschaftliche Interessen können kommerzieller Information und Berichterstattung (durch Konkurrenten) entgegenstehen.[18] Hier sind insbesondere Informationen als Betriebs- und Geschäftsgeheimnis zu betonen.[19]

Am Urheberecht lässt sich ein zentrales Spannungsverhältnis aufzeigen, das sich auch im Bereich der Information über Sicherheitslücken auswirkt. Da das Urheberrecht den Waren- und statischen Charakter von Information als Zustand betont, kann dem – der Informationsasymmetrie im Sicherheitsbereich entspringenden – Bedürfnis nach einem Informationsvorgang nicht Rechnung getragen werden.[20] Soweit die Information für sicherheitsrelevante Fragen genutzt werden kann und muss, kann hier die Verteilungsgerechtigkeit in Frage gestellt werden.[21]

Im Umkehrschluss kann jedoch grundsätzlich gelten, solange keine Interessen Dritter tangiert sind oder die Information dem Wohl aller nützen kann, besteht ein Recht zu informieren. Dies gilt zumindest für die Bürger. Ob dem Staat ein solches grundsätzliches Recht zugestanden werden kann, bleibt zu prüfen.

---

16 Vgl. etwa zum Persönlichkeitsschutz exemplarisch zur Bildberichterstattung über Prinzessin Caroline von Monaco „durch alle Instanzen“: EGMR, Urteil v. 24.06.2004 - 59320/00; BVerfG, Entscheidung v. 15.12.1999 - 1 BvR 653/96; BGH, Urteil v. 19.12.1995 - VI ZR 15/95; OLG Hamburg Urteil v. 08.12.1994 - 3 U 64/94; LG Hamburg, Urteil v. 04.02.1994 - 324 O 537/93.

17 Vgl. § 15 UrhG.

18 Etwa das Verbot der irreführenden Werbung in § 5 UWG, das Verbot der unzumutbaren Belästigung durch Information in § 7 UWG sowie der strafbare Verrat von Betriebs- und Geschäftsgeheimnissen nach § 17 UWG.

19 Vgl. Kapitel 5 B V. 2. a).

20 Dreier, „Wem gehört die Information im 21. Jahrhundert?“, in: Büllesbach/Dreier (Hrsg.), Wem gehört die Information, 2004, S. 96 f. Vgl. die drei Elemente von Information, Kapitel 3 A I.

21 Dreier, a.a.O., (Fn. 20), S. 109.

Im Bereich der Sicherheitslücken können entgegenstehende Interessen Dritter oder der Allgemeinheit bestehen, wenn die Veröffentlichung der Information die Erstellung von schädlichen Exploit erst ermöglicht.[22]

Die Wahrnehmung des Rechts zu informieren kann jedoch nicht nur rechtlich begrenzt werden, sondern auch – soweit darin eine Chance für die Erhöhung der Sicherheit besteht – durch Anreize steuernd gefördert werden.

III. Pflicht sich zu informieren

Die Pflicht sich zu informieren ist dem Staat, Unternehmen oder Einzelne mit unterschiedlichen Aspekten auferlegt.

Eine Pflicht des Staates sich zu informieren ist unter Heranziehung der staatlichen Schutzpflicht denkbar. Soweit Gefahren für kritische Infrastrukturen und/oder für bedeutende Rechtsgüter bestehen, könnte der Staat im Vorfeld verpflichtet sein, Informationen zur Schadensverhütung einzuholen. Die staatliche Informationsvorsorge dient insoweit der „*Effektivierung des grundrechtlichen Schutzauftrags an den Staat, die Freiheitsvoraussetzungen (…) zu sichern*".[23]

Als Überwachungspflicht im weiteren Sinne trifft „Experten" in Unternehmen unterschiedlicher Fachrichtungen die Verpflichtung, einen aktuellen Wissensstand zu halten.[24] So indiziert der Stand der Technik, etwa in § 3 Abs. 6 BImSchG, sich über den Entwicklungsstand des Verfahrens und des Produkts und aktuelle Kriterien zu informieren. Für andere Bereiche wurden durch Richterrecht im Rahmen der Produzentenhaftung etwa die Produktbeobachtungspflichten nach § 823 Abs. 1 BGB

---

22 In tatsächlicher Hinsicht bleibt das Problem der Steuerbarkeit. Eine Beschränkung der Information über Sicherheitslücken ist im Internet eine Herausforderung der Rechtsdurchsetzung.

23 Scholz/Pitschas, Informationelle Selbstbestimmung, 1984, S. 106. So sind Informationspflichten des Staates nicht zuletzt in sensiblen Bereichen wie der Justiz anzutreffen: Die Pflicht sich zu informieren, trifft etwa den Staatsanwalt, der alle Umstände einer Tat ermitteln muss, § 160 StPO, oder mit dem Amtsermittlungsgrundsatz den Richter, § 244 Abs. 2 StPO.
Im amerikanischen Recht kann in dem Gesetzesentwurf zum „Cyber Security Information Act" (H.R. 2435), eingebracht in den 107th Congress, ein interessanter Ansatz des Staates gesehen werden, durch Anreiz Informationen über die Sicherheit kritischer Infrastrukturen zu erlangen.

24 Für „Experten" der IT-Sicherheit: Vgl. LG Hamburg zur Überprüfung von Disketten auf Virenbefall, diese müsse mit den aktuellsten und verschiedenen Virenschutzprogrammen durchgeführt werden, LG Hamburg, Urteil v. 18.07.2001 – 401 O 63/00, MMR 2001, 831 (831).

ausgebildet.[25] Im Bereich der Sicherheit könnte die Pflicht sich zu informieren zwar nicht unbedingt als klassischer interaktiver Informationsvorgang begriffen werden, der Sicherheit dennoch zuträglich sein. Verstanden werden kann dies als Evaluation oder Inventur der angelegten Sicherheitsstandards und –vorkehrungen. So verstanden ist diese eine interne und reflexive Pflicht, sich über die Qualität der Sicherheit bewusst zu werden.[26]

Eine explizit normierte Pflicht sich zu informieren obliegt dem Einzelnen regelmäßig nicht. Die Privatautonomie stellt das „Ob", den Umfang und die Reichweite einer Informationspflicht grundsätzlich der Partei frei.[27] Eine „Pflicht" sich zu informieren, könnte für den Einzelnen als Informationsobliegenheit bestehen. Darunter sind nicht durchsetzbare Informationsgebote im eigenen Interesse des Nicht-Wissenden zu verstehen. Ihre Wahrung steht dem Nicht-Wissenden frei, doch hat er die Folgen des sich nicht Informierens zu tragen und muss die damit verbundene Verschlechterung seiner Rechtsstellung in Kauf nehmen.[28] Diese Obliegenheit ist im Haftungsrecht nach § 254 Abs. 1 BGB begründet. Grundsätzlich lässt die Rechtsordnung somit eine Selbstschädigung oder Selbstgefährdung[29] mangels hinreichender Information zu. Es besteht grundsätzlich keine Pflicht sich über Sicherheitsstandards zu informieren. Inwieweit dem Verbraucher zugemutet wird, sich (fehlende) Informationen selbst zu beschaffen, kann unter anderem dem Verbraucherleitbild der Rechtsprechung entnommen werden.[30]

---

25 Einen Überblick zur Produzentenhaftung nach § 823 Abs. 1 BGB bietet: MünchKommBGB/*Wagner,* § 823 Rd. 547.

26 Im Bereich der Rechnungslegung im Handelsrecht normiert. Sofern diese Rechnungslegung IT-gestützt erfolgt, existiert ein Prüfungsstandard für die Wirtschaftprüfung, die auch die Sicherheit der IT-Infrastruktur beachtet und bewertet, vgl. IDW Prüfungsstandard 330: Abschlussprüfung bei Einsatz von Informationstechnologie, WPg 2002, 1167.

27 BGH, Urteil v. 06.04.2001 - V ZR 402/99, NJW 2001, 2021 (2021): „*Jedermann darf grundsätzlich davon ausgehen, dass sich sein künftiger Vertragspartner selbst über Art und Umfang seiner Vertragspflichten im eigenen Interesse Klarheit verschafft.*"

28 Vgl. weitere Ausführungen, Fenchel, Negative Informationsfreiheit, 1997, S. 145: Als staatlicher „sanfter Zwang" könne die Informationsobliegenheit in die negative Informationsfreiheit nach Art. 5 Abs. 1 S. 1 GG eingreifen. Allerdings werde für die Informationsbeschaffung kein selbstständiger Zwang ausgeübt. Das Gebot für eine Gelegenheit (Fahrerlaubnis) erworbenes Wissen nachzuweisen, könne in das Grundrecht eingreifen, das die entsprechende Gelegenheit schützt (bei dem Erfordernis des Führerscheins ist etwa an die allgemeine Handlungsfreiheit zu denken).

29 Palandt, 65. Aufl. 2006, § 254 Rd. 1, mit der Folge, dass die Obliegenheit ein vorwerfbarer Verstoß gegen *„Gebote des eigenen Interesses"*, a.a.O., Rd. 1, mithin ein Verschulden gegen sich selbst; BGH, Urteil v. 18.04.97 - V ZR 28/96, NJW 1997, 2234 (2235).

30 Niemöller, Das Verbraucherleitbild in der deutschen und europäischen Rechtsprechung, 1999, S. 169; Fezer, Das wettbewerbsrechtliche Irreführungsverbot, in: WRP 1995, 671

Der Schutz durch Information wird soweit eine Entscheidung mit Relevanz für Rechtsgüter (Dritter) zu treffen ist, regelmäßig der anderen Partei durch eine Aufklärungspflicht auferlegt.[31] Speziell im Verbraucherrecht wird die Informationspflicht eher als Pflicht zu informieren geregelt.[32] Eine entsprechende Informationsobliegenheit des Verbrauchers besteht – wenn diese bejaht wird – regelmäßig nur bezüglich der Informationsangebote des Anbieters. Eine darüber hinaus gehende Informationsobliegenheit besteht grundsätzlich nicht.

IV. Pflicht zu informieren

Die Informationsasymmetrie ist für sich alleine keine zwingende Motivation, eine Pflicht zu informieren zu begründen, sondern bleibt als Tatsache eine hinzunehmende Regel. Ausnahmen von dieser Regel können verschiedenen Umständen entnommen werden. Die so begründbare Pflicht zu informieren sind Ausfluss eines *„überragenden Wissens"*[33], einer *„übergeordneten Kompetenz"*[34] oder einer *„staatlichen Schutz-*

(676) spricht von einer Informationspflicht des Verbrauchers, die keiner *„sanktionierten Rechtspflicht"*, mehr einem rechtlich zu erwartendem Marktverhalten entspräche; Meyer, Bemerkungen zur Mars-Entscheidung des EuGH, in: GRUR Int 1996, 101 (101), der von der Aufbürdung einer Informationsbeschaffungslast ausgeht. Wohl auch im Sinne einer Obliegenheit Lettl, Der Schutz des Verbrauchers nach der UWG-Reform, in: GRUR 2004, 449 (454): Die Frage der Einholung (weiterer) Information betreffe die Aufmerksamkeit und Verständigkeit des Verbrauchers und sei abhängig von dem zu erwerbenden Produkt. Bei selten erworbenen, hochwertigen Produkten sei zu erwarten, dass sich der aufmerksame Durchschnittsverbraucher eingehend informiere. Ausführlich zum Verbraucherleitbild unter Kapitel 3 C II. 2. A. A.: Wolf, Die Grundsätze der Rechtsprechung des EuGH, 2001, S. 28, lehnt eine solche Obliegenheit ab, da der Verlust der freien Entscheidungsbasis aufgrund nicht eingeholter Informationen keinen rechtlichen, sondern einen tatsächlichen Nachteil darstelle.

31 Dies ist nicht zuletzt auch der Zweckmäßigkeit geschuldet. Nur im Rahmen einer Aufklärungspflicht kann regelmäßig die Erkennbarkeit der Schutzbedürftigkeit berücksichtigt werden.

32 Dies ist nicht zuletzt eine Folge des Informationsmodells, das unter anderem auf der Pflicht Informationen weiterzugeben basiert, vgl. Kapitel 3 C II. 2. a). Vgl. auch: Grundmann, Ausbau des Informationsmodells, in: DStR 2004, 232 (232).

33 Ein überragendes Wissen einer Partei ist in allen Rechts- und Vertragsbereichen anzutreffen. Zu einer Aufklärungspflicht führt überragendes Wissen, wenn Informationen vorenthalten werden, die dem Wissenden leicht verfügbar sind und die andere vor Schaden bewahren können. In diesem Sinn ist die Aufklärungspflicht nicht immer gesetzlich verankert, sondern kann über die allgemeinen Verkehrspflichten auf den Einzelfall angewandt werden, vgl. etwa BGH, Urteil v. 09.11.1993 - VI ZR 248/92, NJW 1994, 799 zur ärztlichen Aufklärungspflicht nach § 823 BGB.

34 Mit der übergeordneten Kompetenz soll zum Ausdruck gebracht werden, dass derjenige, der eine gefährliche Einrichtung betreibt, ein gefährliches Produkt vertreibt oder gefährliches tut (Chirurg) die selbst initiierte Gefahr mit eigen Mitteln zu minimieren hat. So werden Aufklä-

pflicht“[35]. Mit unterschiedlichen Konnotationen wird sie im Bereich von „Gefahren“[36] als Hinweis-. Aufklärungs-, Belehrungs-, Beratungspflicht oder Pflicht zur Warnung bezeichnet. Im Folgenden soll die Pflicht zu informieren primär als Steuerungsinstrument des Verbraucherrechts betrachtet werden. Als solches trifft sie sowohl Anbieter und Hersteller als auch den Staat.

Eine Pflicht des Staates zu informieren besteht, soweit ein Verfahren zwischen Staat und Einzelnen (oder Unternehmen) dem Einzelnen (oder Unternehmen) gesetzlich aufgezwungen wird.[37] Diese Pflichten sollen den Ablauf eines fairen Verfahrens garantieren. Eine darüber hinausgehende, verfahrensunabhängige gesetzliche Pflicht des Staates zu Warnungen besteht in Bereichen, deren Sicherheit sektorspezifisch geregelt ist, vgl. etwa § 8 Abs. 4 S. 3 GPSG oder § 28 Abs. 4 S. 1 Medizinproduktegesetz.[38]

Im Verbraucherrecht sollte die Pflicht der Anbieter und Hersteller zu informieren mit der Informationsobliegenheit der Verbraucher gesetzlich oder durch Richterrecht zweckmäßigerweise austariert sein. Eine wichtige gesetzliche Grundlage der Pflicht des Anbieters zu informieren ist die BGB-Informationspflichtenverordnung, die die Pflicht zu informieren zulasten des anbietenden Unternehmers regelt. Regelmäßig ist die Pflicht zu informieren jedoch im Rahmen der Verkehrssicherungspflicht nach § 823 Abs. 1 BGB im Einzelfall zu bestimmen. Diese

---

rungspflichten besonderen Berufsgruppen, etwa Ärzten, Architekten, Rechtsanwälten, Steuerberater oder Unternehmen im Finanzdienstleistungssektor auferlegt. Für Ärzte: BGH, Urteil v. 29.06.1995 - 4 StR 760/94, NStZ 1996, 34; BGH, Urteil v. 21.11.1995 - VI ZR 329/94, NJW 1996, 776; für Rechtsanwälte: BGH, Urteil v. 16.05.1991 - IX ZR 131/90, NJW 1991, 2079 (2079 f.); für Steuerberater: BGH, Urteil v. 20. 11. 1997 - IX ZR 62-97, NJW 1998, 1221; für Banken: BGH, Urteil v. 28.9.2004 - XI ZR 259/03; BGH, Urteil v. 17.12.1991 - XI ZR 8/91, WM 1992, 216; BGH, Urteil v. 27.11.1990 - XI ZR 308/89, WM 1991, 85.

35 Vgl. etwa BVerfG, Beschluss v. 15.08.1989 - 1 BvR 881/89, NJW 1989, 3269 (3270), das eine Warnung vor Sekten mit der Schutzpflicht des Staates aus Art. 2 Abs. 2 GG, das Leben und die körperliche Unversehrtheit seiner Bürger zu schützen sowie den Jugendschutz, legitimiert.
Sollte der Staat seine Pflicht zu informieren mangels Wissen nicht erfüllen können, so könne an eine Delegation an Private gedacht werden, vgl. Kugelmann, Die informatorische Rechtsstellung des Bürgers, 2001, S. 120.

36 Dementsprechend ist ein allgemeines Auskunftsrecht, soweit es nicht einem Schutzbedürfnis oder einer „Gefahrenlage“ dient, nicht von Interesse.

37 So besteht etwa eine verfahrensabhängige Belehrungs- und Aufklärungspflicht der Judikative in § 53 Abs. 2 StPO, § 86 Abs. 3 VwGO oder die Begründungspflicht in § 39 VwVfG der Verwaltung.

38 Soweit diese in das Ermessen der Behörde gestellt ist, kann sie unter die Pflicht (bei Ermessensreduktion) und das Recht zu informieren fallen.

nimmt bei der Darlegung der Pflicht über Sicherheitslücken zu informieren eine herausragende Stellung ein.

V. Zusammenfassung

Informationsrechte und –pflichten sind im Kontext der Sicherheit relevant als Gegengewicht zur (Wissens)Übermacht, allgemein auch schon als *„Recht der Informationsmachtbalance"*[39] oder hier als Ausgleich der Informationsasymmetrie bezeichnet.

Während die Informationspflichten normativ ausgestaltet oder durch Richterrecht ausgefüllt sind, bedarf das Recht zu informieren keine gestaltende, sondern begrenzende Regelungen. Das Recht, sich zu informieren, darf nicht verfahrensabhängig, sondern sollte im Sinne einer unabhängigen produktbezogenen Information und im Sinne einer Information über technisch-organisatorische Maßnahmen ausgestaltet sein. Inwieweit ein Recht sich zu informieren im Privatrecht losgelöst von Sonderbeziehungen zwischen Produzenten, Vermarkter und Verbraucher durchsetzbar ist, ist fraglich. Das Recht sich zu informieren entspricht der Eigenverantwortung als rechtlicher Kategorie der Sicherheit. Als aktive Möglichkeit zur Erlangung von Sicherheit bedarf sie der Chance durch das Bereitstellen von Information durch Dritte, und wird demnach durch die Pflicht zu informieren ergänzt.

Die normativen Regelungen des Rechts sich zu informieren sind demnach Regelungen, die dem Einzelnen helfen, seine Informationsverantwortung wahrnehmen zu können, etwa durch staatliche Informationsfreiheitsgesetze oder Auskunftsrechte. Im Zentrum der Darlegung der Informationsrechte und –pflichten werden weniger normative Regelungen als vielmehr eine Ausfüllung durch Verkehrssicherungspflichten stehen.

B Informationsrechte bei Sicherheitslücken

Anders als Träger öffentlicher Gewalt handeln privatrechtliche Rechtssubjekte nicht aufgrund von Kompetenzen und Befugnissen, sondern auf der Basis von

---

[39] Burkert, Internetrecht – Informationsrecht, in: Schweizer/Burkert/Gasser (Hrsg.), Festschrift für Jean Nicolas Druey, 2002, S. 693 (714).

Freiheiten.[40] Dementsprechend können Informationsrechte über Sicherheit vielfältig sein. Beispielhaft sollen einige Formen des Informationsvorgangs dargestellt werden. Diese wurden ausgewählt, weil sie einen innovativen Weg darstellen (Belohnungen), sie aktuellen Änderungen unterworfen werden können (Strafbarkeit von Hacken) und in der Praxis Begrenzungen erfahren (Beschränkung von Informationsrechten durch Urheberrecht).

Zur Begriffklarheit sei noch einmal darauf hingewiesen, dass unter Hersteller grundsätzlich die Hersteller sicherheitsrelevanter- und bedürftiger Produkte (Soft- und Hardware) und unter Anbieter grundsätzlich Unternehmen und Staat – soweit sie Webseiten anbieten, Interaktionen ermöglichen oder einen Internetzugang haben – verstanden werden.

Soweit dem Staat als Akteur und dem Arbeitsplatz eine besondere Rolle zugestanden werden kann und die Informationsrechte durch spezifische Interessen geprägt sind, sollen diese unter Kapitel 5 B IV. und V. erörtert werden.

I. Recht sich zu informieren

1. Hersteller und Anbieter

Soweit sich Hersteller – ohne verpflichtet zu sein – über den Sicherheitsstand der eigenen Produkte bzw. Webseiten informieren, ist eine Einordnung in die Sphäre des Rechts im oben verstandenen Sinn als Regelung der Kommunikationsbeziehungen zwischen mehreren Beteiligten nicht zwingend erforderlich, wenn auch ein solches Recht aus Art. 14 oder 12 GG bestehen kann. Das Recht an Produkten umfasst grundsätzlich auch das Recht, sich über den Zustand dieser zu informieren. Soweit dadurch Rechte Dritter eingeschränkt werden, könnte dieses Recht begrenzt sein. Dies soll unter Kapitel 5 B V. 1. exemplarisch am Arbeitsverhältnis dargestellt werden.

Das „Security Bug Bounty Program“ eines Browsers eines Open Source Software-Projekts lobt eine Belohnung von $ 500 und ein T-Shirt für denjenigen aus, der ei-

[40] Lübbe-Wolff, Rechtsprobleme der behördlichen Umweltberatung, in: NJW 1987, 2705 (2707).

ne kritische Sicherheitslücke aufdeckt.[41] Es ist damit eine aktive Initiative, Sicherheitslücken ausfindig machen zu lassen, bevor sie ausgenutzt werden können.

Wird der Hersteller über die Sicherheitslücke informiert, so wird die Information einen begrenzten Zeitraum geheim gehalten, bis die Sicherheitslücke geschlossen werden kann. Eine Veröffentlichung der Information über die Sicherheitslücke zur Warnung der Nutzer wird als Ausgleich zwischen den Chancen des Selbstschutzes und den Risiken eines Exploits gesehen. Konkrete Angaben wie mit einer Sicherheitslücke verfahren wird, finden sich in der Policy[42] über Security Bugs[43]. Danach wird die vollständige Information über die Sicherheitslücke auf eine bestimmte Gruppe begrenzt. Der „Finder" wird gebeten, diese Information grundsätzlich geheim zu halten (etwa Beschreibungen der Lücke nicht in Foren zu posten), jedoch ist die Belohnung nicht an die Wahrung der Vertraulichkeit durch den Finder geknüpft.[44] Hier besteht ein Anknüpfungspunkt an das Recht. Die Auslobung kann als Steuerungsinstrument rechtlich abgesichert werden, indem an die Aufdeckung von Sicherheitslücken konkrete Anforderungen gestellt werden; etwa die Wahrung der Vertraulichkeit.

Die Belohnung für die Information über die Sicherheitslücken wäre nach deutschem Recht über § 657 BGB abgesichert. Das Gesetz spricht abstrakt von der „Herbeiführung eines Erfolges". Es lässt dem Auslobenden einen Gestaltungsspielraum, in welcher Art und Weise der Erfolg herbei zu führen ist, so könnten Fristen, Vertraulichkeit und sogar die Erstellung eines Patches an die Belohnung geknüpft werden.

---

41 Mozilla Security Bug Bounty Programm, http://www.mozilla.org/security/bug-bounty.html (30.05.2006).
Voraussetzung für die Belohnung: die Sicherheitslücke muss bisher unveröffentlicht sein, durch ein Exploit von außen „nutzbar", in der aktuellen Version der Software auftreten und der „Finder" darf nicht der Entwickler des Exploits sein. Sicherheitslücken, die durch Software Dritter entstehen (Java, Plugins, etc.) sind von dem Programm ausgenommen. Eine kritische Sicherheitslücke im Sinne dieses Programms ist eine Lücke, die einen ausführbaren Code auf dem System des Nutzers gestattet oder einen Zugang zu vertraulichen Informationen des Nutzers ermöglicht – dies gilt nur für *„high-value personal information (e.g., passwords, credit card numbers, and the like)",* Mozilla Security Bug Bounty FAQ, http://-www.mozilla.org/security/bug-bounty-faq.html (30.05.2006). Ebenso zahlt die Sicherheitsfirma Tippingpoint Prämien, http://www.zerodayinitiative.com/details.html (30.05.2006).

42 Handling Mozilla Security Bugs, Version 1.1., 11.02.2003, http://www.mozilla.org/projects-/security/security-bugs-policy.html (30.05.2006).

43 Bugs sind Programm- oder Softwarefehler, http://de.wikipedia.org/wiki/Programmfehler (30.05.2006).

44 Mozilla Security Bug Bounty FAQ, a.a.O., (Fn. 41).

Hier haben Hersteller und Entwickler einen Weg gefunden, das „Recht" sich zu informieren durch Anreize steuernd zu fördern. Insoweit wird im Folgenden nicht das Recht sich zu informieren, das ja grundsätzlich besteht, konkret dargestellt, sondern mit der Auslobung von Belohnungen eine Form gefunden, andere zu einem Beitrag zur Wahrnehmung des Rechts sich zu informieren zu animieren. Wissende werden durch Belohnungen motiviert, ihr Recht zu informieren, wahrzunehmen, wobei durch die Spezifikationen der Auslobung gleichzeitig der Informationsvorgang zu kontrollieren versucht werden kann.

Anbieter von Webseiten haben entsprechend den Herstellern das Recht, sich über ihre Betriebsabläufe, mithin den Sicherheitsstand(ard) ihrer Kommunikationsangebote, zu informieren.[45] Hinsichtlich der Begrenzung wird ebenfalls auf Kapitel 5 B V. 1. verwiesen.

2. Nutzer

Das Recht des Nutzers sich zu informieren soll in zwei Modifikationen diskutiert werden. Beide setzen den technisch versierten Nutzer voraus. Zum einen ist die Information über Sicherheitslücken technisch über das Reverse Engineering oder die Dekompilierung zu erreichen. Zum anderen kann Wissen über den Sicherheitsstand eines Systems durch Hacken erreicht werden und ist rechtlich unter dem Aspekt des Ausspähens von Daten zu erörtern.

Als Einstieg in die folgende Diskussion soll ein Gerichtsverfahren gegen den „Entdecker" einer Sicherheitslücke in Frankreich vorangestellt werden.

In der Sache geht es um die Veröffentlichungen der Schwächen einer Anti-Virensoftware und den Beweis in Internetforen, dass der nach Herstellerangaben hundertprozentige Schutz vor Viren nicht gegeben ist. Unter anderem wurde zum Beweis der Sicherheitslücke ein „proof of concept"[46] veröffentlicht, welches einen Teil des Quellcodes wiedergeben soll. Der Hersteller der Software hat daraufhin Anzeige wegen Verletzung des Urheberrechts erstattet.[47] Mit Urteil vom 08.03.2005

---

45 Hiermit ist nicht die Information über mithin die Überwachung der Arbeitnehmer gemeint.

46 Der Nachweis von Sicherheitslücken erfolgt nicht selten über den Beweis mit „Exploits", Programmen, die die spezifischen Schwächen eines anderen ausnutzen, vgl. Internetlexikon Wikipedia, http://de.wikipedia.org/wiki/Exploit (30.05.2006), oder sonstigen „proof of concepts".

47 Art. L 335.2 des Gesetzes zum Urheberrechtsschutz: *„Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon; et toute contrefaçon est un délit.*

wurde der „Entdecker" zu einer Geldstrafe von 5.000 € auf Bewährung verurteilt, diese Strafe wurde in der Berufungsentscheidung vom 21.02.2006 bestätigt.[48] Dieses Urteil kann aufgrund der Harmonisierung des Urheberrechts durch Richtlinien[49] Indizwirkung auch für Deutschland haben. Sicherheitslücken in Software könnten auf diese Art und Weise demnach nur mit Zustimmung des Urhebers offenbart werden.[50] Im Folgenden wird der Sachverhalt aus deutscher Sicht beleuchtet.

a) Reverse Engineering

Nutzer mit entsprechendem technischen Verständnis können durch Reverse Engineering Informationen über das Programm und die Qualität seiner sicherheitsrelevanten Bestimmungen erhalten. Reverse Engineering *„umfaßt sämtliche Formen der Rückwärtsentwicklung eines Computerprogramms, die eine Analyse des Programms bezwecken."*[51] Speziell bei Softwareprodukten werden hierfür Rückschlüsse aus dem Quellcode gezogen. Begrifflich enger kann für Softwareprodukte auch die Bezeichnung Dekompilierung, also die Rückübersetzung des Objektcodes[52] in die vorgegebene Programmiersprache und den Quellcode, verwendet werden.[53]

(…)." Art. L 335.2 des Gesetzes zum Urheberrechtsschutz. [eigene Übersetzung der Autorin] *„Jede Veröffentlichung von Geschriebenen, einer musikalischen Komposition, einer Zeichnung, eines Gemäldes oder jedes anderen Erzeugnisses, welches ganz oder teilweise ungeachtet der Gesetze und Vorschriften hinsichtlich des Schutzes geistigen Eigentums gedruckt oder aufgenommen werden, ist eine Nachahmung; und jede Nachahmung ist strafbar. (…)"*

48 Auszüge aus der Entscheidung erster Instanz vom 08.03.2005 und der Berufungsentscheidung vom 23.02.2006 finden sich unter http://maitre.eolas.free.fr/journal/index.php?-2006/02/23/296-l-arret-de-la-cour-d-appel-dans-l-affaire-guillermito (30.05.2006). Informationen zum Fall Guillermito unter, http://maitre.eolas.free.fr/journal/index.php?Laffaire-guillermito (30.05.2006).

49 Vgl. umfassende Urheberrechtsrichtlinie: Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22.05.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. Nr. L 167, vom 22.06.2001, S. 10.

50 Eine Erkenntnis, die ein Autor unter der Überschrift „Umwertung der Werte" teilt, Glaser, Peter, Stuttgarter Zeitung vom 19.01.05.

51 Marly, Urheberrechtsschutz für Computersoftware, S. 269.

52 Der Objektcode (Maschinensprache) ist die für den Computer ausführbare Sprache aus Binärdaten (Einsen und Nullen).

53 Die Dekompilierung leitet sich ab von dem hierbei verwendeten Programm, dem Decompiler. Auf das Auffinden von Fehlern in Hard- und Software zugeschnitten nennt sich dieses auch Debugger. Der Begriff Reverse Engineering ist weiter, da er sämtliche Formen der Rückübersetzung erfasst, vgl. Marly, Urheberrechtsschutz für Computersoftware, S. 269. Das Resultat der Dekompilierung entspricht in der Regel nicht hundertprozentig dem ur-

Damit stellt sich die Frage, ob dem Nutzer das aktiv-initiative Recht[54] zusteht, sich mittels Reverse Engineering – in Form der Dekompilierung – über Sicherheitslücken zu informieren. Aufgrund der Komplexität der meisten Software wird dabei festgestellt: *„Nur durch Reverse Engineering kann dem öffentlichen Interesse an IT-Sicherheit"*[55] geeignet Rechnung getragen werden.

Die folgenden Überlegungen gelten grundsätzlich für proprietäre Software. Soweit sich für Open Source Software etwas anderes ergibt erfolgen entsprechende Hinweise.

Die grundsätzliche Zulässigkeit der Offenlegung des Quellcodes zur Optimierung der Sicherheit mag urheberrechtlich strittig sein. Reverse Engineering und der Dekompilierung sind allerdings wirksame Methoden zur Optimierung der Sicherheit. Allerdings hat hier eine Abwägung mit den Urheberrechten Dritter zu erfolgen. Grundsätzlich könnte die Abwägung und die Verteilung der Rechte beim Reverse Engineering und der Dekompilierung als Chance auf eine rechtliche Regelung der IT-Sicherheit betrachtet werden.[56] Gesetzlich nicht ausdrücklich normiert, scheint diese Abwägung zugunsten der Urheberrechte ausgefallen zu sein. Zumindest wurde in der entsprechenden Richtlinie und im Gesetzgebungsverfahren keine Abwägung des Rechts sich über IT-Sicherheit zu informieren – das heißt Reverse Engineering zu betreiben und zu dekompilieren – mit den Rechten des Urhebers proprietärer Software getroffen.[57] Dem entsprechend wird zum Reverse Engineering konstatiert:

> *„The laws don't increase the security of systems, or prevent hackers from finding flaws. What they do is allow product vendors to hide behind lousy security, blaming other for their own ineptitude. It's certainly easier to implement bad security and make it illegal for anyone to notice than to implement good security. While*

---

sprünglichen Quellcode, da bestimmte für den Computer irrelevanten Anmerkungen bei der Compilierung beseitigt werden, und deshalb nicht mehr rückübersetzbar sind, vgl. Köhntopp/Köhntopp/Pfitzmann, Sicherheit durch Open Source?, in: DuD 2000, 508 (509).

54 Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3149 f.), diskutiert das Reverse Engineering unter der Schadensabwendungspflicht des Nutzers. M. E. geht dieser Ansatz jedoch an der Realität und der gesetzlichen Wertung in § 69d Abs.1 und § 69e UrhG vorbei.

55 Lutterbeck/Horns/Gehring, Sicherheit in der Informationstechnologie und Patentschutz für Software-Produkte, 2000, S. 10, http://www.ipjur.com/data/LuGeHo.pdf (30.05.2006).

56 Lutterbeck/Horns/Gehring, a.a.O., (Fn. 55), S. 122.

57 Vgl. Richtlinie des Rates vom 14.05. 1991 über den Rechtsschutz von Computerprogrammen (91/250/EWG), ABl. L 122, vom 17.05.1991, S. 42; Entwurf eines Zweiten Gesetzes zur Änderung des Urheberrechtsgesetzes vom 18.12.1992, BT-Drs. 12/4022.

these laws have the side effect of helping stem the dissemination of hacked software (…) the laws will reduce security in the long run."[58]

Zu den Chancen der IT-Sicherheit durch Dekompilierung nimmt das deutsche UrhG wie folgt Stellung. Ein generelles Dekompilierungsverbot besteht im Urheberrecht nach § 69c Nr. 2 1. Alt. UrhG. Dieses Verbot wird für die Ermittlung von Informationen, die der Herstellung von Interoperabilität dienen, in § 69e UrhG unterbrochen.[59] Zudem gestattet § 69d Abs. 1 UrhG eine Ausnahme von § 69c Nr. 2 UrhG, soweit sie zur bestimmungsgemäßen Benutzung des Computerprogramms, einschließlich der Fehlerbeseitigung, notwendig ist und soweit keine besonderen vertraglichen Bestimmungen (Ausschluss von § 69d Abs. 1 UrhG) vorliegen. In der Literatur wird hierunter teilweise auch ein Recht zur Fehlerbeseitigung durch Dekompilierung angenommen, soweit diese zur bestimmungsgemäßen Nutzung des Programms notwendig ist.[60] Teilweise wird wegen des abschließenden Charakters von § 69e UrhG die Dekompilierung ausgeschlossen.[61]

§ 69d Abs. 1 UrhG setzt demnach voraus, dass die Dekompilierung der Fehlerbeseitigung dienen kann und hierfür notwendig ist.

---

58 Schneier, Secrets & Lies, 2000, S. 346. Der an anderer Stelle beispielhaft anführt, dass es beim Reverse Engineering auch darum gehe, zu wissen, wie die Software funktioniert. Dieses Recht sich zu informieren werde den Kunden ja auch bei jedem anderen Produkt zugestanden, etwa beim Auto, a.a.O., S. 392.

59 Wandtke/Bullinger-*Grützmacher*, § 69e Rd. 28 hält explizit fest, dass die Dekompilierung zur Fehlerbeseitigung nicht durch § 69e privilegiert wird.

60 Hoeren/Schuhmacher, Verwendungsbeschränkungen im Softwarevertrag, in: CR 2000, 137 (140). Ebenso Kotthoff in: Dreyer/Kotthoff/Meckel, Urheberrecht 2004, § 69d Rd. 6; Loewenheim, Handbuch des Urheberrechts, 2003, § 76, Rd. 29 f., mit der Einschränkung einer partiellen Dekompilierung zum Zweck der Fehlerbeseitigung als Ultima Ratio des Käufers oder Lizenznehmers; ebenso Möhring/Nicolini-*Hoeren,* § 69d UrhG Rd. 9, mit der Beschränkung auf schwere Programmfehler und (kumulativ) für den Fall, dass der Hersteller nicht in angemessener Zeit kostenfreie Fehlerbeseitigung anbietet; Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3149 f.): Spindler will eine Pflicht dann annehmen, wenn die *„drohenden Schäden in keinem Verhältnis mehr zu den möglichen Risiken einer Urheberrechtsverletzung stehen, der Geschädigte über dem Hersteller gleichwertige Kenntnisse verfügt und das Programm nicht ohne weiteres ausgetauscht werden kann."* Eine solche Pflicht verkennt den Umstand, dass es – will der Hersteller die Fehlerbeseitigung nicht selbst durchführen – die Schadensabwendungspflicht des Herstellers sein könnte, den Quellcode dem Nutzer zur Fehlerbeseitigung zu überlassen, wenn dieser über die personellen und fachlichen Kapazitäten verfügt, den Quellcode zur Fehlerbeseitigung auch tatsächlich nutzen zu können.

61 Dreier/Schulze-*Dreier* UrhG Kommentar, § 69d Rd. 10, der § 69e als eine abschließende Regelung der Dekompilierung betrachtet; Wandtke/Bullinger-*Grützmacher*, § 69d UrhG Rd. 22, der darauf hinweist, dass kein Programm fehlerfrei sei und somit die Wertung des § 69e und der Schutz des Know-hows umgangen werden könne; ebenso Schricker-*Loewenheim*, § 69d Rd. 3 mit Verweis auf § 69e und die Gesetzgebungsgeschichte.

„Notwendig" sind Maßnahmen, wenn andere Maßnahmen die bestimmungsgemäße Nutzung nicht auf zumutbare Weise ermöglichen.[62] Zum Teil wird „notwendig" demnach im Sinn einer Ultima Ratio, d. h. ohne eine andere Alternative, verstanden.[63] Eine – zumutbare – Handlungsalternative wäre etwa ein Ersuchen um Fehlerbeseitigung beim Hersteller,[64] soweit die Kosten und der Zeitraum zumutbar sind. Nicht ausreichend ist hingegen, dass die Fehlerbeseitigung lediglich nützlich ist.[65]

Ausgehend von der Abwägung der Interessen des Urhebers und des Nutzers könnte der Quellcode zumindest den Nutzern, die gesetzlich oder vertraglich der IT-Sicherheit verpflichtet sind, vertraulich überlassen werden bzw. ihnen ein Recht auf Dekompilierung eingeräumt werden muss. Die Notwendigkeit i.S.d. § 69d Abs. 1 UrhG könnte zum einen aufgrund des Zeitfaktors – bedingt durch die „sichere Unsicherheit"[66] – und aus der eigenen Handlungsverpflichtung zu bejahen sein. Wohl unterdurchschnittlich wenig (private) Nutzer können tatsächlich die Sicherheit ihres eigenen Systems mittels Reverse Engineering erhöhen und damit eine notwendige Fehlerberichtigung im Sinne des § 69e Abs. 1 UrhG durchführen. Den Quellcode in diesem Sinne nutzen kann prinzipiell jeder, tatsächlich aber nur Experten mit entsprechendem Fachwissen.[67]

Mit dem „Government Security Program" (GSP) wird diese Idee bereits vereinzelt freiwillig umgesetzt, dies ist ein Fall des vom Hersteller gestatteten Reverse Engineerings von proprietären Produkten zum Zweck der Erhöhung der IT-Sicherheit (zu dem Programm vgl. Kapitel 5 B I. 3.).

Ob eine Fehlerbeseitigung mittels Dekompilierung tatsächlich erfolgen kann, ist eine technische Frage. Was eine Fehlerbeseitigung ist, ist eine Frage der Definition. Hier kann der Fehlerbegriff des allgemeinen Zivilrechts nur bedingt zu Grunde gelegt werden.[68] Fehler sind die Umstände, die eine bestimmungsgemäße Benutzung

---

62 Dreier/Schulze-*Dreier* UrhG Kommentar, § 69d Rd. 11.

63 Kotthoff in: Dreyer/Kotthoff/Meckel, Urheberrecht 2004, § 69d Rd. 7.

64 Kotthoff in: Dreyer/Kotthoff/Meckel, Urheberrecht 2004, § 69d Rd. 7, zunächst muss etwa um Fehlerberichtigung beim Urheberrechtsinhaber nachgesucht werden; in diesem Sinne auch Wandtke/Bullinger-*Grützmacher*, § 69d UrhG Rd. 22.

65 Dreier/Schulze-*Dreier* UrhG Kommentar, § 69d Rd. 11.

66 Vgl. Kapitel 3 B.

67 In diesem Sinne auch Schneider, Neues zu Vorlage und Herausgabe des Quellcodes?, in: CR, 2003, 1 (4). Als Option für Autodidakten kann das Internet in entsprechenden Newsgroups und Mailinglisten Hilfestellungen geben.

68 Loewenheim, Handbuch des Urheberrechts, 2003, § 76, Fn. 112, demnach wird ein objektiver informationstechnikbezogener Fehlerbegriff zu Grunde gelegt, der grundsätzlich vom

des Programms objektiv beeinträchtigen.[69] So werden neben Viren, Bugs oder Programmabsturz ausdrücklich im Programm angelegte und später auftretende Fehler miteingeschlossen.[70] Soweit Sicherheitsmängel den bestimmungsgemäßen Gebrauch verhindern oder mindern, liegen demnach Fehler vor.

Regelmäßig wird in den Lizenzbedingungen das Reverse Engineering und die Dekompilierung und damit ein Recht zur Fehlerbeseitigung im oben genannten Rahmen vertraglich ausgeschlossen.[71] Etwa in folgender typischen Lizenzbestimmung:

> *"Kein Reverse Engineering. Es ist dem Kunden nicht erlaubt, Reverse Engineering durchzuführen, die SOFTWARE zu dekompilieren oder zu zerlegen oder auf eine andere Weise zu versuchen, den Quellcode zu ermitteln."*[72]

Nicht zuletzt werden in der Praxis regelmäßig Beschränkungen durch vertragliche Abreden hinsichtlich der Art und Weise der Nutzung, etwa zeitliche Dauer (Lauffähigkeit bis zum nächsten Update[73]) getroffen. Diese Einschränkung wird im Hinblick auf den Sinn und Zweck des Urheberrechts (wettbewerbsrechtlicher Schutz) als zu weitgehend zu kritisieren, da dieser Zweck nicht zwangsläufig eine Einschränkung der Sicherheit mit sich bringen müsse.[74]

Bei Open Source Software ist die Fehlersuche und -beseitigung durch Reverse Engineering grundsätzlich möglich, da die Software durch den in den Lizenzbestim-

---

subjektiv-objektiven Fehler des BGB zu unterscheiden ist; a. A. Möhring/Nicolini-*Hoeren*, § 69d UrhG Rd. 11, der eine Identität des Fehlerbegriffs des BGB bejaht.

69 Loewenheim, Handbuch des Urheberrechts, 2003, § 76, Rd. 29.

70 Dreier/Schulze-*Dreier* UrhG Kommentar, § 69d Rd. 9; ebenso Schricker-*Loewenheim*, § 69d Rd. 9 der sich nicht auf programmimmanente Fehler beschränkt, sondern auch eine Verseuchung mit Viren als Fehler ansieht.

71 Lutterbeck/Horns/Gehring, Sicherheit in der Informationstechnologie und Patentschutz für Software-Produkte, 2000, S. 79, http://www.ipjur.com/data/LuGeHo.pdf (30.05.2006).

72 Es handelt sich um eine typische Lizenz Vereinbarung für proprietäre Software, hier des Herstellers NVIDIA Software, http://www.nvidia.de/object/nvidia_license_de.html (30.05.2006).

73 Dreier/Schulze-*Dreier* UrhG Kommentar, § 69d Rd. 12.

74 Zumal das Urheberecht nicht grundsätzlich frei von Einschränkungen ist. So sind etwa Einschränkungen zugunsten der Informationsfreiheit in § 5 UrhG vorgesehen, mit weiteren Ausführungen Rehbinder, Urheberrecht, § 38 Rd. 278. Etwas anderes könnte gelten, wenn der Hersteller eine *„Security Reporting Policy"* veröffentlicht, welche eine entsprechenden beweisbaren Report der Sicherheitslücke und eine Zusammenarbeit mit dem Finder vorsieht. Vgl. etwa Guidelines for Security Vulnerability Reporting and Response Version 2.0, 01.09.2004, http://www.oisafety.org/guidelines/secresp.html (30.05.2006). 1.3 des Draftes empfiehlt die Veröffentlichung einer entsprechenden „Security Reporting Policy". Weitere Ausführungen hierzu oben Kapitel 3 B.

mungen gestatteten Zugriff auf den Quellcode den Bedürfnissen des Nutzers angepasst werden kann.[75]

Unter der Prämisse, dass die Offenlegung oder Ausforschung des Quellcodes tatsächlich eine die Sicherheit erhöhende Funktion hat, bietet der Quellcode eine

> *„Signalfunktion, wie sie zur Überwindung von Informationsasymmetrien dringend benötigt wird: Wenn der Anwender wissen will, ob ein proprietäres Produkt oder ein Open-Source-Produkt vergleichbarer Funktionalität seinen Zwecken besser genügt, ist er zu einer Evaluation der Produkteigenschaften gezwungen. (…) Gerade der Faktor Sicherheit lässt sich nur sehr schlecht bewerten, wenn der Quellcode nicht zur Verfügung steht."*[76]

Abschließend kann festgehalten werden, dass das Recht, sich mittels Reverse Engineering oder Dekompilierung über Sicherheitslücken von proprietärer Software zu informieren, regelmäßig durch das Urheberrecht eingeschränkt wird. Als Recht muss dem Nutzer das Reverse Engineering erst durch ein entsprechendes urheberrechtliches Nutzungsrecht eingeräumt werden.

b) Hacken zur Information über die Sicherheit

Nicht selten werden Sicherheitslücken und Schwachstellen in IT-Systemen Dritter durch wohlmeinende Hacker[77] als selbsternannte „Sicherheitstester"[78] aufgedeckt. Als Recht sich über Sicherheitslücken und Schwachstellen IT-Systemen Dritter zu informieren, könnte das Hacken durch § 202a StGB als Ausspähen von Daten mit Strafandrohung begrenzt sein. Soweit das Hacken personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse tangiert, kommen auch § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nr. 3 BDSG oder § 17 Abs. 2 UWG in Betracht.

Fraglich ist, ob Daten im Sinn des § 202a StGB auch Informationen über die Infrastruktur und damit über Sicherheitslücken und Schwachstellen des IT-Systems sind. Daten im Sinne des Abs. 2 der Vorschrift sind alle durch Zeichen codierte In-

---

75 Lutterbeck/Horns/Gehring, a.a.O., (Fn. 55), S. 78.

76 Gehring, Sicherheit mit Open Source, in: Gehring/Lutterbeck (Hrsg.), Open Source Jahrbuch 2004, S. 209 (225 f.).

77 Ausführlich zum Begriff des Hackers und seinen Abgrenzungen und Spielarten: Schmid, Computerhacken und materielles Strafrecht, S. 18 ff. Hacken soll hier mit Dannecker, Neuere Entwicklungen im Bereich der Computerkriminalität, in: BB 1996, 1285 (1289), als *„Eindringen in fremde Computersysteme, das nicht mit dem Ziel der Manipulation, Sabotage oder Spionage erfolgt, sondern aus Freude an der Überwindung von Sicherungssystemen"* begriffen werden. Ebenso Sieber, Computerkriminalität und Informationsstrafrecht, in: CR 1995, 100 (103); vgl. Beschlussempfehlung und Bericht zum Entwurf eines Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität (2.WiKG) vom 19.02.1986, BT-Drs. 10/5058, S. 28.

78 Heise news vom 24.02.2005, http://www.heise.de/newsticker/meldung/56775 (30.05.2006).

formationen, die Mittel oder Gegenstand der Datenverarbeitung sind.[79] Als Mittel der Datenverarbeitung sind Daten auch Programme oder Informationen über Teile von Programmen.[80] Ebenso sind wohl auch Informationen über die weitere (techno)logische und physikalische Infrastruktur Daten im Sinn des § 202a StGB. Dies kann etwa die nach Zugang erlangte Kenntnis von der Verwendung einer bestimmten schwachstellenbehafteten Serversoftware sein.

Nach bisher herrschender Meinung und Intention des Gesetzgebers ist das bloße Ausforschen der Systeminfrastruktur (Hacken) – und damit auch eine Untersuchung des verwendeten Sicherheitsstandards – nach § 202a StGB nicht strafbar, solange sich keine Daten verschafft werden.[81]

Das Tatbestandsmerkmal des sich Verschaffens wird mit der tatsächlichen Herrschaft über die Daten durch Erlangung oder Kopie des Datenträgers oder auch bereits durch die Kenntnisnahme als erfüllt angesehen.[82] Sich Verschaffen im Sinn der Vorschrift ist allerdings auch die bloße Kenntnisnahme von den Daten, etwa eines Passwortes, weshalb die vom Gesetzgeber gewollte Straflosigkeit des Hackens nur über eine teleologische Auslegung des sich Verschaffens erreicht werden kann.[83] Letztendlich sollen die Daten – etwa das Passwort oder Informationen über

---

79 Schönke/Schröder-*Lenckner*, § 202a Rd. 3.

80 Schönke/Schröder-*Lenckner*, § 202a Rd. 3.

81 Für eine Straflosigkeit: Lackner/Kühl, § 202a Rd. 4; Schmid, Computerhacken und materielles Strafrecht, 2001, S. 127; Schönke/Schröder-*Lenckner,* § 202a Rd. 10; vgl. Beschlussempfehlung und Bericht zum Entwurf eines Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität (2.WiKG) vom 19.02.1986, BT-Drs. 10/5058, S. 28, das Strafrecht solle erst dort eingreifen, wo eine Rechtsgutbeeinträchtigung, wie z. B. die Verletzung von Verfügungsrechten über Informationen, eingetreten sei. *„Insbesondere sollen sog. „Hacker", die sich mit dem bloßen Eindringen z.B. in ein Computersystem begnügen, also sich keine Daten unbefugt verschaffen, von Strafe verschont beleiben.";* einschränkend MünchKommStGB-*Graf*, § 202a Rd. 51, der Straffreiheit nur für den Erstzugang annehmen will. Soweit danach kein Abbruch erfolgt und Kenntnis von weiteren Daten erlangt wird, sei eine Strafbarkeit anzunehmen. Kritisch: Dannecker, Neuere Entwicklungen im Bereich der Computerkriminalität, in: BB 1996, 1285 (1289). Für eine Strafbarkeit: Hoeren/Sieber Handbuch Multimedia-Recht, Kap 19. Rd. 421; Tröndle/Fischer § 202a, Rd. 11; Jessen, Zugangsberechtigung, 1994, S. 182 ff., mit Hinweis auf das Bundesverfassungsgericht, nach dem der Wille des Gesetzgebers nur insoweit Berücksichtigung finden kann, als er im Gesetz hinreichend Ausdruck gefunden habe; Krutisch, Strafbarkeit des unberechtigten Zugangs, 2003, S. 139 f.

82 Statt vieler, MünchKommStGB-*Graf*, § 202a Rd. 43.

83 Lackner/Kühl, § 202a Rd. 4; Schönke/Schröder-*Lenckner*, § 202a Rd. 10; SK-StGB-*Hoyer,* § 202a Rd. 13 will die Einschränkung des Tatbestandes über eine Absicht, den gesicherten Inhalt kennen zu lernen erreichen. Hilgendorf schlägt eine teleologische Reduktion auf das Merkmal der Reproduktion der Daten vor. Eine Kenntniserlangung soll demnach erst angenommen werden, wenn der Täter den Informationsgehalt reproduzieren kann, was bei größeren Datenmengen regelmäßig eine Speicherung der Information erfordere, Hilgendorf,

das System und damit die (techno)logische und physikalische Infrastruktur – die quasi nur als „Abfallprodukt" der allein bezweckten Überwindung der Zugangsicherung anfallen, nicht als sich verschafft gelten.[84]

Soweit Sicherheitslücken mittels Software ausgeforscht werden, erscheint diese strafrechtliche Bewertung gerechtfertigt. Denn Sicherheitslücken, im automatisierten Verfahren mittels Trojanischer Pferde, Port-Scans, etc. ausgeforscht, führen nicht automatisch zu einer tatsächlichen Kenntnisnahme der anfallenden Systemdaten. Sie sind vielmehr Vorbereitungshandlungen, um in das System eindringen und zu den zugangsgesicherten Daten vordringen zu können. Soweit das Bestehen von Sicherheitslücken in dieser Weise ausgetestet wird, ist das Hacken nicht strafbar.[85] Auf dieses Bild des Hackers gründet auch die Motivation des Gesetzgebers. Zum Zeitpunkt des Erlasses wurde der Beitrag des Hackers in der Unterstützung und Fortentwicklung von IT-Systemen durch das Auffinden von Sicherheitslücken gesehen, eine kriminelle Zielrichtung des Hackens wurde prima facie nicht angenommen.[86]

Etwas anderes könnte allerdings gelten, wenn zielgerechtet Informationen über Sicherheitslücken (Programme, etc.) eines Systems zur Veröffentlichung gesammelt werden. Hier fallen die Daten nicht als „Abfallprodukt" an, sondern sind Ziel und Zweck des Handelns. Es ist nicht ersichtlich, warum hier Informationen über das System anders behandelt werden sollen als sonstige Informationen über ein Unternehmen (Daten *im* System), deren sich Verschaffen eine Strafbarkeit begründen sollen. Es wird in das geschützte Rechtsgut, das Verfügungsrecht[87] des Unternehmens über seine Daten (diese umfassen auch Programme und damit Teile des IT-Systems), eingegriffen. Für das Unternehmen, das berechtigt oder unberechtigt eine Sicherheitslücke geheim halten will, ist gerade mit einer anschließenden Veröffentlichung der gleiche „Handlungsunwert" wie bei Kenntniserlangung und Ver-

---

Grundfälle zum Computerstrafrecht, in: JuS 1996, 702 (704 f.). Eine Übersicht findet sich bei Schmid, Computerhacken und materielles Strafrecht, 2001, S. 122 ff.

84 Soweit so mit dem Zweck zwischen Straffreiheit und Strafbarkeit differenziert wird (vgl. Schönke/Schröder-*Lenckner,* § 202a Rd. 10) ist dies ein Abstellen auf ein subjektives Tatbestandsmerkmal, das angesichts des klaren Wortlauts des objektiven Tatbestandsmerkmals „verschaffen" im Hinblick auf die Rechtssicherheit des Betroffenen und Täters nicht angezeigt ist.

85 Schmid, Computerhacken und materielles Strafrecht, 2001, S. 170 und 176.

86 Krutisch, Strafbarkeit des unberechtigten Zugangs, 2003, S. 137, mit dem Hinweis, dass zum Zeitpunkt des Erlasses der Regelung noch keine spektakulären kriminellen Hackerfälle bekannt waren.

87 Hilgendorf, Grundfälle zum Computerstrafrecht, in: JuS 1996, 509 (511); Hoeren/Sieber Handbuch Multimedia-Recht, Kap 19. Rd. 418.

wertung sonstiger interner Daten erreicht, da in die Geheim- und Privatsphäre eingedrungen wird.[88] Auf der anderen Seite kann der Nutzer mit einer (wiedergewonnenen) Entscheidungsfreiheit bei Kenntnis der Systemunsicherheit von einem solchen Ausspähen der Daten profitieren.[89] Eine strafrechtliche Sanktionierung veröffentlichter Sicherheitstests ist somit nicht Interesse des Nutzers.[90]

Nach einschränkender Ansicht soll ein öffentlichkeitswirksamer „Sicherheits-Check" zumindest dann unter den Tatbestand des § 202a StGB fallen, wenn „probeweise" Daten erhoben werden.[91]

Der Sicherheitstester, der Daten über das System und mit den Sicherheitslücken in Programmen auch Daten im System erlangt, verschafft sich demnach Daten im Sinn des § 202a StGB. Aus dem Zweck der Vorschrift, die Datenbestände zu schützen, könnte die Strafbarkeit anders zu beurteilen sein, wenn die entdeckten Sicherheitslücken und Schwachstellen des IT-Systems ausschließlich dem Unternehmen mitgeteilt werden und auf eine weitere Veröffentlichung verzichtet wird. In einem solchen Fall wird dem Unternehmen quasi sein ausschließliches Verfügungsrecht über die Daten zurückgegeben.[92] Bei der Veröffentlichung einer entsprechenden *„Security Reporting Policy"*[93], die eine Zusammenarbeit bei der Entdeckung mit dem Finder vorsieht, könnte sogar von einem Ausschluss des Tatbestandes (unbefugt) ausgegangen werden.[94]

Darüber hinaus ist eine Strafbarkeit nur gegeben, wenn die Daten gegen unberechtigten Zugriff gesondert gesichert sind. Diese Sicherung muss nicht lückenlos ge-

---

88 Tröndle/Fischer, § 202a Rd. 11.

89 Der Kunde eines Finanzinstituts mit einem unsicheren System kann etwa entscheiden, ob er weiterhin die Leistungen dieses Instituts in Anspruch nehmen will.

90 So auch Schmid, Computerhacken und materielles Strafrecht, 2001, S. 135 f., der dennoch aufgrund des Integritätsinteresses des Systembetreibers eine Strafbarkeit befürwortet.

91 MünchKommStGB-*Graf*, § 202a Rd. 80.

92 Der Täter begnügt sich in diesem Fall mit dem Eindringen und hat keinerlei Interesse an den Daten. Gegen den hier angedachten strafbefreienden Rücktritt könnte die Vollendung des Tatbestandes entgegengehalten werden.

93 Vgl. etwa Guidelines for Security Vulnerability Reporting and Response Version 2.0, 01.09.2004, http://www.oisafety.org/guidelines/secresp.html (30.05.2006) weiter Ausführungen hierzu oben (Kap. 4 C. II). 1.3 des Draftes empfiehlt die Veröffentlichung einer entsprechenden „Security Reporting Policy".

94 Es wäre zumindest schwerlich hinzunehmen, wenn der Finder einer Sicherheitslücke in seinem „Security Vulnerability Report" (vgl. Kapitel 3 B) etwa angeben sollte, wie er die Sicherheitslücke gefunden hat (4.1.3 des Draftes), und sich so der Strafverfolgung aussetzt.

währleistet werden.[95] Auch bei Vorliegen von Sicherheitslücken, die gerade erst den Zugang ermöglichen, ist das Tatbestandsmerkmal erfüllt.

Die Feststellung der grundsätzlichen Strafbarkeit für das „Ausspähen von Sicherheitslücken" findet sich auch in der Convention on Cybercrime (CCC)[96] des Europarats wieder. Dieses völkerrechtliche Abkommen ist zum 01.07.2004 gemäß Art. 36 Abs. 3 CCC in Kraft getreten. Die Umsetzung in deutsches Recht ist bisher nicht erfolgt.[97] Die gleiche Richtung gibt auch das Europarecht vor. Mit dem Rahmenbeschluss über Angriffe auf Informationssysteme[98] werden Mindeststandards für die Bekämpfung der Kriminalität im Internet geschaffen. Beiden Vorschriften ist gemein, dass sie nicht den Zugang zu Daten – wie § 202a StGB – sondern den Zugang zum System pönalisieren.

Art. 2 CCC:

> *„(…) to establish as criminal offences under its domestic laws, when committed intentionally, the access to the whole or any part of a computer system without right."*

Art. 2 des Rahmenbeschlusses:

> *„(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass der vorsätzliche und unbefugte Zugang zu einem Informationssystem als Ganzes oder zu einem Teil eines Informationssystems zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.*
>
> *(2) Jeder Mitgliedstaat kann beschließen, dass Handlungen nach Absatz 1 nur geahndet werden, sofern sie durch eine Verletzung von Sicherheitsmaßnahmen erfolgen."*

Kein unrechtmäßiger Zugang lag nach dem Vorschlag des Rahmenbeschlusses vor, wenn eine durch Vertrag oder Gesetz befugte Person ein Informationssystem kontrolliert, erprobt oder im rechtlich zulässigen Rahmen wissenschaftlich erforscht, vgl. Art. 3 i.V.m. Art. 2 g) und f) des Vorschlags des Rahmenbeschlusses.[99] In der

---

95 Ernst, Hacker und Computerviren, in: NJW 2003, 3233 (3236 f.). Etwas anderes könne gelten, wenn die Sicherheitslücke allgemein bekannt ist, a.a.O., (3237). Ausführlich zu den Abstufungen der Sicherungsgrade: Schmid, Computerhacken und materielles Strafrecht, 2001, S. 75 ff. Im Ergebnis will Schmid auf die Erkennbarkeit des Geheimhaltungswillens abstellen. Dieser sei ausreichend dokumentiert, wenn der Computerlaie nicht ohne weiteres die Sicherung überwinden kann, a.a.O., S. 82.

96 Einen kurzen Überblick über die CCC gibt etwa Valerius, Der Weg zu einem sicheren Internet?, in: K&R 2004, 513.

97 Vgl. die Liste der Ratifikationen unter, http://conventions.coe.int/Treaty/Commun/-ChercheSig.asp?NT=185&CM=8&DF=16/04/04&CL=ENG (30.05.2006).

98 Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl. L 69 Nr. 67, vom 16.03.2005, S. 67. Dieser ist gem. Art. 34 Abs. 2 b) EU i.V.m. Art. 12 des Rahmenbeschlusses bis zum 16.03.2007 in deutsches Recht umzusetzen.

99 Vorschlag für einen Rahmenbeschluss des Rates über Angriffe auf Informationssysteme vom 19.04.2002, KOM(2002)173 endg.. Vgl. die explizite Heraushebung von Sicherheitstester in der Begründung zu Art. 3 f) des Vorschlags, vgl. S. 13, die sich, zwar nicht in dieser

verabschiedeten Fassung wurde diese Präzisierung der Formulierung „unbefugt" als rechtliche oder gesetzliche Gestattung aufgegeben, vgl. Art. 1 d) des Rahmenbeschlusses.

Nach der hier vertretenen Ansicht kann bei dem gezielten Suchen und anschließendem Veröffentlichen von Sicherheitslücken und Schwachstellen in IT-Systemen von Unternehmen bereits nach geltendem Recht eine nach § 202a StGB strafbare Handlung vorliegen. Danach können Hacker als „Sicherheitstester" bei Umsetzung dieser Vorschriften in deutsches Recht grundsätzlich nur mit Zustimmung oder gesetzlicher Erlaubnis straffrei tätig werden. Dies schließt regelmäßig „selbsternannte" Sicherheitstester aus.

3. Recht des Staates sich zu informieren (Governmental Source Code)

Dem Staat wird mitunter ein besonderes Informationsbedürfnis zugestanden, welches mit den „besonderen" Aufgaben, die der Staat wahrzunehmen hat, begründet wird. Zur Gewährleistung der öffentlichen Sicherheit wird dem Staat etwa ein berechtigtes Interesse an Informationen über technischen Überwachungseinrichtungen nach § 110 Abs. 1 TKG zugestanden.

Durch das „Government Security Program" (GSP) eines Softwareherstellers werden dem Staat besondere Informationsrechte aufgrund besonderer Sicherheitsinteressen durch ein Unternehmen vertraglich zugestanden und eingeräumt. Ob nur Vermarktungsstrategie oder tatsächlich konzediertes Interesse ist hier nicht zu entscheiden. Durch den (kontrollierten) Zugang zum Quellcode und anderen technischen Informationen werden dem Staat vertraglich Informationsrechte (Recht sich zu informieren) eingeräumt, um seine Möglichkeiten der Anordnung und des Einsatzes von sicheren IT-Infrastrukturen zu erhöhen.[100] Dieses Angebot wird unter anderem durch das Bundesinnenministerium Österreichs genutzt.[101]

Klarheit, aber im Wortlaut des Art. 3 des Rahmenbeschlusses über das Zusammenspiel der Formulierung „unrechtmäßig" und der Legaldefinition von „unrechtmäßig" und „befugter Person" in Art. 2 f) wiederfindet.

100 Vgl. http://www.microsoft.com/presspass/features/2003/Jan03/01-14gspmundie.asp (30.05.2006).

101 Im Januar 2004 schlossen Microsoft und Österreich ein Government Security Program ab, http://www.electronic-business.at/news/865.html?sws_news_pop=70 (30.05.2006). Weltweit nehmen an dem GSP etwa 30 Länder bisher (Stand September 2004) teil, http://-www.newratings.com/analyst_news/article_492343.html (30.05.2006).

Im Umkehrschluss liegt nahe, dass ein entsprechender Sicherheitsstandard ohne diese Informationen nicht möglich wäre. Dies ist im Rahmen dieser Arbeit jedoch nicht zu verifizieren. Welchen Vertragspartnern ein entsprechender Vertrauensstatus für den Zugang zu den technischen Informationen eingeräumt wird, ist grundsätzlich eine Entscheidung, die der Vertragsfreiheit unterliegt und nicht verallgemeinerungsfähig ist. Ob der Zugang zu den Informationen als vertragliche Nebenpflicht jedem Vertragspartner eingeräumt werden muss, unterliegt einer Interessenabwägung zwischen den wirtschaftlichen Interessen des Unternehmens und dem Schadensrisiko des Einzelnen. Bisher wurde diese Interessen im Recht zugunsten des Urheberrechts (vgl. oben) und damit zugunsten der wirtschaftlichen Interessen der Hersteller und Entwickler von Software abgewogen.

II. Recht sich nicht zu informieren

Spiegelbildlich zur negativen Informationsfreiheit könnte auch es auch ein Recht des Nutzers geben, sich nicht über Sicherheitslücken zu informieren.

Der Ansatz der BGH Entscheidung zum Dialer-Missbrauch[102], dass der Nutzer grundsätzlich keine Obliegenheit hat, sich über Sicherheitssoftware Gedanken zu machen, ist wohl verfehlt. Der Umfang und die Reichweite des „Rechts" sich nicht zu informieren entstehen vielmehr im Umkehrschluss aus dem Umfang und der Reichweite der Pflichten des Nutzers, sich zu informieren.

III. Recht zu informieren

1. Hersteller und Anbieter

Unter dem Stichwort der *„unpredictable Full-Disclosure"*[103] wird das „Recht" der Hersteller und Anbieter über Sicherheitslücken eigener Produkte und Systeme zu informieren, durch die (technische) Frage nach der Chance für die Erhöhung der Sicherheit und dem Risiko der Missbrauchsgefahr (Ausnutzung durch Exploits) geprägt und begrenzt. Soweit die Informationen über Sicherheitslücken schädliche Auswirkungen haben, weil erst durch die Informationen Exploits möglich sind und geschrieben werden, kommt eine Begrenzung des Rechts zu informieren über eine

---

102 BGH „Dialer", Entscheidung v. 04.03.2004 - III ZR 96/03, MMR 2004, 308.

103 Vgl. Kapitel 3 B.

Verkehrssicherungspflicht nach § 823 Abs. 1 BGB in Betracht. Entsprechend der zögerlichen Praxis über eigene Sicherheitslücken tatsächlich zu informieren,[104] ist fraglich, inwieweit hier eine Pflicht zu informieren nicht angebracht wäre. Im Rahmen dieser Pflicht sind die schädlichen Auswirkungen zu berücksichtigen. Informationen der Hersteller und Anbieter über Sicherheitslücken und Schwachstellen sollen demnach unter der Pflicht zu informieren betrachtet werden.

Soweit Hersteller über Sicherheitslücken von Produkten und Systemen von Konkurrenten berichten, soll darauf im nächsten Punkt bei den Publikationen der Nutzer eingegangen werden.

2. Nutzer – Publikation

Eine Beschränkung des Rechts über erworbenes Wissen frei zu verfügen, ist gegebenenfalls an Art. 5 Abs. 1 S. 1 1. Alt. GG zu messen. Ebenso stellt sich die Frage nach absoluten Rechten[105] an Information. Schließlich können für bestimmte Bereiche beschränkende „Besitzverhältnisse" an Informationen fest gemacht werden. So können etwa die Rechte auf Intim- und Privatsphäre[106], das informationelle Selbstbestimmungsrecht[107] oder das Urheberrecht das Recht, Informationen aus diesen Bereichen zu veröffentlichen, beschränken.

---

104 Ein seltenes Beispiel ist etwa die Stellungnahme des CCC (Chaos Computer Club) zum Hack eines Servers des CCC: *„Uns ist diese Angelegenheit äußerst peinlich. Jedoch ist es für uns selbstverständlich, die Informationen zu dem Hack publik zu machen. Wir danken an dieser Stelle den spanischen Hackerkollegen für den Hinweis auf die Sicherheitslücke."*, https://www.ccc.de/-updates/2004/camp-server-hack?language=de (30.05.2006).

105 Diskutiert wird dies in (der Schweiz) in den Kategorien absolute und relative bzw. subjektive und objektive Rechte an Information. Vgl. Weber, Ali Baba oder das Risiko exklusiver Informationsinhaltsrechte, in: Schweizer/Burkert/Gasser (Hrsg.), Festschrift für Jean Nicolas Druey, 2002, S. 1009 (1010); Druey, Schutz der Information, in: Weber/Hilty (Hrsg.), Daten und Datenbanken, 1999, S. 7 (12). Eine Analogie zum Sachenrecht ablehnend, Spinner, Ist Wissen analogiefähig?, in: Schweizer/Burkert/Gasser (Hrsg.), Festschrift für Jean Nicolas Druey, 2002, S. 947 (963): „*Wissen ist von Natur aus tauschfreundlich und deshalb tendenziell besitzflüchtig."* Ebenso zur Frage, wem Informationen gehören: Dreier, „Wem gehört die Information im 21. Jahrhundert?", in: Büllesbach/Dreier (Hrsg.), Wem gehört die Information, 2004, S. 95 ff.

106 Zuletzt ein Thema in unterschiedlichen Rechtsordnungen die Entscheidungen im Fall von Caroline von Monaco, vgl. EGMR, Urteil v. 24.06.2004 - 59320/00; BVerfG, Entscheidung v. 15.12.1999 - 1 BvR 653/96; BGH, Urteil v. 19.12.1995 - VI ZR 15/95; OLG Hamburg Urteil v. 08.12.1994 - 3 U 64/94; LG Hamburg, Urteil v. 04.02.1994 - 324 O 537/93.

107 Hierbei werden personenbezogene Daten grundsätzlich – ohne Einwilligung nach § 4 Abs. 1 BDSG – von dem Recht zu informieren, d. h. die Daten weiterzugeben, ausgenommen.

Grundsätzlich gilt, dass die Ausübung von Rechten grundsätzlich auch dann legitim ist, wenn damit Schädigungen Dritter verbunden sind.[108]

In einem ersten Schritt ist jedoch das Recht zu informieren zu konturieren. Unter der Prämisse, dass dieses Recht grundsätzlich unbeschränkt besteht[109], kann das Recht nur über gesetzliche und vertragliche Schranken – für Form und Inhalt – konturiert werden. Im Sinn des gegebenen Themas werden diese Schranken im Kontext der Sicherheit betrachtet.

In Betracht kommen Schranken durch das Urheberrecht und eine mögliche Einordnung der Sicherheitslücken als Betriebs- und Geschäftsgeheimnis sowie bei Informationen durch Konkurrenten das Wettbewerbsrecht. Die Beschränkung durch das Urheberrecht wurde bereits oben dargelegt.[110] Es beschränkt nicht nur das Recht sich zu informieren, sondern auch das Recht zu informieren, soweit etwa die Informationen über Sicherheitslücken in Software Details über den Quellcode enthalten (§§ 69a Abs. 4 i.V.m. 15 Abs. 1 Nr. 2 UrhG).

Ebenso existieren Schranken im Strafrecht, vgl. die bereits erwähnten § 202a Abs. 1 2. Alt. StGB und Art. 6 (1) a CCC, die die Veröffentlichung von Programmen, die einen unberechtigten Zugang ermöglichen, unter Strafe stellen.

Mit den Mitteln des Urheber- und Strafrechts werden demnach sowohl kontraindizierte Informationen verboten – d. h. es besteht kein Recht derjenigen, die zur Ausnutzung der Sicherheitslücke Informationen verbreiten und Exploits als qualifizierte Information zur Verfügung stellen wollen, als auch denjenigen kein Recht zugesprochen wird, die grundsätzlich einen Beitrag zur Sicherheit leisten wollen, in dem sie entsprechende Informationen verbreiten. Gerade das Urheberrecht erhebt – an Werken und letztlich Waren orientiert – einen Anspruch auf statische Infor-

---

108 Soergel/*Hönn,* § 826 Rd. 42.

109 Dies kann im Umkehrschluss aus den Urteilen des BVerfG zur staatlichen Informationstätigkeit – der inhaltlich zutreffende Tatsachen zu Grunde lag – gefolgert werden. Vgl. dazu BVerfG „Glykol", Beschluss v. 26.06.2002 - 1 BvR 558/91, NJW 2002, 2621 (2622): Wenn Unternehmen aus den Grundrechten (Art. 12 Abs. 1 GG) schon kein „*ausschließliches Recht auf eigene Außendarstellung und damit auf eine unbeschränkte Selbstdarstellung am Markt"* gegenüber dem Staat gelten machen können, so können sie ein solches erst recht nicht gegenüber dem Bürger und nur ihm Rahmen des Wettbewerbsrechts gegenüber konkurrierenden Unternehmen geltend machen. Das BVerfG führte weiter aus, es fördere „*die Funktionsweise des Marktes, wenn in solchen Situationen durch zusätzliche, gegebenenfalls auch staatliche Informationen Gegengewichte gesetzt werden.*", BVerfG a.a.O., (2622). Ebenso zur sachgerechten Kritik durch Private: BVerfG, Beschluss v. 25.01.1961 - 1 BvR 9/57, BVerfGE 12, 113 (125); BGH, Urteil v. 09.12.1975 - VI ZR 157/73, BGHZ 65, 325 (331); MünchKommBGB/*Wagner,* § 823 Rd. 198.

110 Vgl. Kapitel 5 B I. 2. a).

mation.[111] Dieser kollidiert mit dem Bedürfnis nach der Verteilung von Information für sicherheitsrelevante Fragen. Insoweit kann hier die Verteilungsgerechtigkeit in Frage gestellt werden.[112]

Soweit das Urheber- und Strafrecht nicht tangiert ist, stellt sich die Frage, ob darüber hinaus über Sicherheitslücken informiert werden darf. Begrenzungen indiziert zum einen der Aspekt der ruf- oder geschäftsschädigenden Wirkung zum anderen der Aspekt der Anleitung zum Exploit.

a) Aspekt der ruf- und geschäftsschädigenden Wirkung

Ausgangspunkt ist wiederum die grundsätzliche Unbeschränktheit des Rechts zu informieren. Begrenzungen sind ex post über eine Anwendung der §§ 824, 826, 823 BGB denkbar.[113]

Ein grundlegendes Kriterium bei der Beurteilung der Rechtmäßigkeit der Weitergabe von Informationen ist die Unterscheidung zwischen (ruf- oder geschäftsschädigenden) wahren und falschen Tatsachenbehauptungen und Werturteilen. Diese Trennung besteht nicht nur im hier angesprochenen Deliktsrecht, sondern durchzieht auch die Bewertung von Informationsvorgängen im Wettbewerbs-, Straf- und Verfassungsrecht[114] und soll demnach hier vertieft betrachtet werden.

Tatsachen sind im zivil-, straf- und verfassungsrechtlichen Kontext definiert als sinnlich wahrnehmbare Vorgänge oder Zustände, deren Richtigkeit mit Beweisen überprüfbar ist.[115] Tatsachenbehauptungen haben einen besonders überzeugenden

---

111 Dreier, a.a.O., (Fn. 105), S. 96 f. Vgl. die drei Elemente von Information, Kapitel 3 A I.

112 Dreier, a.a.O., (Fn. 105), S. 109.

113 Im oben vorangestellten Fall (Kapitel 5 B. I. 1. b)) des französischen Sicherheitstesters wurde dieser (nicht rechtskräftig) in erster Instanz zu einem Schadensersatz in Höhe von 13.300 € verurteilt. Beantragt wurde für den Imageschaden *„(…) - 631 100 € HT au titre du manque à gagner résultant de la campagne de dénigrement et la mise à disposition sur Internet des éléments permettant de copier ou de neutraliser le logiciel VIGUARD. - 182 748,40 € HT en réparation des conséquences de l'atteinte à son image de marque. (…)"* [Eigene Übersetzung der Autorin: *-631.100 € (vor Steuer) als Umsatzeinbuße, erlitten durch den Imageverlust des Produktes, insbesondere durch das zur Verfügungstellen über das Internet von Komponenten, die eine Kopie der Software Viguard darstellen und ihre Wirksamkeit herabsetzen bzw. neutralisieren. - 182 748,40 € (vor Steuer) für die Behebung des Imageschadens der Marke*], Auszüge aus der zivilrechtlichen Entscheidung vom 07.06.2005 finden sich unter http://maitre.eolas.free.fr/journal/index.php?2006/02/23/296-l-arret-de-la-cour-d-appel-dans-l-affaire-guillermito (30.05.2006).

114 Vgl. § 824 BGB, § 4 Nr. 8 UWG, § 3 185 ff. StGB und Art. 5 GG.

115 Statt vieler: MünchKommBGB/*Wagner,* § 824 Rd. 9, mit weiteren Hinweisen. Werturteile sind dagegen von der subjektiven Einstellung zum Inhalt der Information geprägt, durch ein Element der Stellungnahme gekennzeichnet und lassen sich deshalb nicht als wahr oder

Informationsinhalt, da sie mit einem Wahrheitsanspruch behaftet sind und ihnen ein erheblicher Einfluss auf die Meinungsbildung eingeräumt wird.[116] Öffentlich geäußert können sie deshalb – wahr oder falsch – die Interessen Dritter gefährden.

Informationen über Sicherheitslücken lassen sich primär als Tatsachenbehauptung qualifizieren, soweit sie einem technischen Beweis zugänglich sind. Bei Bestehen einer Sicherheitslücke lässt sich dieser Beweis theoretisch etwa mit dem Quellcode, Port-Scanner, durch einen reproduzierbaren „Datenbeweis" (exemplifizierende Erhebung geschützter Daten) oder ein Exempel der Funktionstätigkeit führen. Soweit die Behauptung einer Sicherheitslücke jedoch als wissenschaftliche These Raum für andere Schlussfolgerungen lassen, sind sie als Werturteile zu qualifizieren.[117]

Haftungsrelevant ist die Veröffentlichung einer falschen Tatsache – also einer nicht bestehenden Sicherheitslücke – regelmäßig, wenn zusätzliche Tatbestandsmerkmale erfüllt werden, etwa das Bestehen eines Wettbewerbsverhältnisses bei § 4 Nr. 8 UWG oder im Rahmen des § 824 BGB die Eignung zur Kreditgefährdung oder sonstige Nachteile für Erwerb oder Fortkommen.[118] Bei unwahrer Information über Sicherheitslücken einer Software kann der Absatz der Software und somit die Erwerbsgrundlage gefährdet sein.

An § 823 Abs. 1 BGB sind ruf- und geschäftsschädigende Werturteile ebenso zu messen, wie (ruf- und geschäftsschädigende) falsche Tatsachenbehauptungen.[119] Die Informationen könnten in den eingerichteten und ausgeübten Gewerbebetrieb als sonstiges Recht im Sinn des § 823 Abs. 1 BGB eingreifen. Während bei ruf- und geschäftsschädigenden Werturteilen ein großzügiger Maßstab anzulegen ist, sollen falsche Tatsachenbehauptungen stets einen Eingriff darstellen.[120] Die Ver-

---

falsch erweisen. Statt vieler, MünchKommBGB/*Wagner,* § 824 Rd. 9. mit weiteren Nachweisen zur Rechtsprechung.

116 MünchKommBGB/*Wagner,* § 824 Rd. 11.

117 MünchKommBGB/*Wagner,* § 824 Rd. 22, 44.

118 Die Eignung zur Kreditgefährdung ist ein Aspekt, der durch „Basel II" nicht nur theoretischer Natur ist. Kreditgefährdung ist die Beeinträchtigung wirtschaftlicher Interessen, Palandt, 65. Aufl. 2006, § 824 Rd. 8. Als Komponente des operationellen Risikos fließt die Qualität der IT-Sicherheit in die Einschätzung und Bewertung von Banken- und Versicherungsrisiken und damit in die Bemessung der Eigenkapitalvorsorge ein.

119 MünchKommBGB/*Wagner,* § 823 Rd. 196.

120 MünchKommBGB/*Wagner,* § 823 Rd. 197. Wegen Art. 5 GG sei bei geschäftsschädigenden Werturteilen ein großzügiger Maßstab anzulegen. Ein Unternehmen muss sich Äußerungen bis an die Grenze der so genannten Schmähkritik gefallen lassen, a.a.O., Rd. 197 mit Hinweisen auf die Rechtsprechung.

breitung (ruf- und geschäftsschädigender) wahrer Tatsachen muss ein Unternehmen hinnehmen, auch wenn sie in der Konsequenz die gleichen negativen Folgen wie die Behauptung unwahrer Tatsachen haben kann.[121] Eine Grenze soll allerdings auch bei (wahren) Tatsachenbehauptungen bei so genannter „Prangerwirkung" bestehen.[122] Diese ist bei einer reinen Information über Sicherheitslücken allerdings kaum denkbar. Teilweise soll den Informationsinteressen der Allgemeinheit gegenüber unternehmerischen Interessen tendenziell der Vorrang eingeräumt werden.[123] Kriterium sei hier die Bedeutung der Information für die Öffentlichkeit.[124]

Schranken der Veröffentlichung von Sicherheitslücken sind auch dem Wettbewerbsrecht zu entnehmen, wenn also ein Konkurrent den Gegenbeweis antreten wollte, dass die Herstellerangaben bezüglich der Sicherheitsgarantie nicht den Tatsachen entsprechen (vgl. § 4 Nr. 8 UWG). Ob dem Konkurrenten allerdings daraus – in den urheberrechtlichen Grenzen - ein eigenes Recht zur Veröffentlichung des Gegenbeweises erwächst, ist im Einzelfall zu prüfen. Der Umkehrschluss aus § 4 Nr. 8 UWG indiziert zwar, dass wahre Tatsachenbehauptungen zulässig sind. Einschränkend gilt allerdings im Wettbewerb, dass die Verbreitung wahrer Tatsachen nur zulässig ist, soweit die angesprochenen Verkehrskreise ein sachlich berechtigtes Informationsinteresse haben.[125] Grundsätzlich ist demnach eine Interessenabwägung erforderlich. Diese könnte bei Informationen über Sicherheitslücken mit dem Aspekt der Eigenverantwortung zugunsten des Rechts zu informieren zu bejahen sein.

Festzuhalten ist, dass Informationen über Sicherheitslücken sich primär als Tatsachenbehauptung qualifizieren lassen. Die Verbreitung ruf- und geschäftsschädigender wahrer Tatsachen muss ein Unternehmen grundsätzlich hinnehmen. Für Hersteller und Anbieter können sich zusätzlich Beschränkungen durch das Wettbewerbsrecht ergeben, soweit die Offenbarung der Sicherheitslücken im Interesse der Nutzer ist, ist ein Recht des Mitbewerbers jedoch anzunehmen.

---

121 Soergel/*Beater*, § 823 Anh V Rd. 43; MünchKommBGB/*Wagner,* § 823 Rd. 198, mit dem einschränkenden Hinweis auf das Wettbewerbsrecht. Außerhalb des Wettbewerbsrechts überwiege das Informationsinteresse der Öffentlichkeit, so dass bei der inkriminierenden Behauptung von wahren Tatsachen größte Zurückhaltung geboten sei, a.a.O., Rd. 198.

122 Erman-*Schiemann,* § 823 Rd. 71; MünchKommBGB/*Wagner,* § 823 Rd. 198.

123 Soergel/*Beater*, § 823 Anh V Rd. 44. Das Recht des Arbeitnehmers zu informieren ist differenzierter zu beurteilen, vgl. Kapitel 5 B V.

124 So BVerfG, Beschluss v. 25.01.1984 - 1 BvR 272/81, BVerfGE 66, 116 (139), im Rahmen der Abwägung bei widerrechtlich beschafften Informationen; Soergel/*Beater*, § 823 Anh V Rd. 44.

125 Baumbach/Hefermehl-*Köhler,* § 4 UWG Rd. 16.

b) Aspekt der Ausnutzung durch ein Exploit

Soweit die Offenbarung der Sicherheitslücken Basis für ein Exploit sein kann, welches Rechtsgüter Dritter verletzt, kann diese im Rahmen des § 823 Abs. 1 BGB ein begrenzender Faktor sein. Als Frage, inwieweit man verpflichtet ist, andere vor Schäden zu bewahren,[126] ist die Möglichkeit eines schädlichen Exploits im Rahmen einer Verkehrssicherungspflicht zu berücksichtigen und ist soweit im Ergebnis mit der Begrenzung der Pflicht zu informieren identisch. Daher ist hier auf die Ausführungen unter Kapitel 5 C III. 2. b) cc) zu verweisen.

IV. Informationsrecht des Staates – Szenario 1

Dem folgenden Abschnitt wird das in Kapitel 1 dargelegte Szenario 1 zu Grunde gelegt. In diesem geht es um die Frage der Rechtmäßigkeit einer Warnung von Bundesregierung, Bundesamt für Sicherheit in der Informationstechnik (BSI) und des Landesdatenschutzbeauftragten[127] über die Sicherheitslücken in einem Browser.

Die Rechtsprechung und Literatur jahrzehntelang beschäftigt haben Warnungen im Bereich des Umweltschutzes, der Lebensmittel und der Glaubensgemeinschaften; vgl. die jüngsten Entscheidungen des BVerfG zu *„Glykol"* und *„Osho-Bewegung"*[128]. Im Zentrum der Erörterung steht neben der Kompetenz die Frage, ob und in welche Grundrechte die Warnung eingreift und ob deswegen ein Gesetzesvorbehalt besteht.[129] Anhand dieser Punkte sollen für die Frage nach der Rechtmäßigkeit von derartigen staatlichen „Verbraucherwarnungen" typische Problemfelder aufgezeigt und für das Szenario 1 diskutiert werden.

---

126 Eine allgemein Pflicht andere vor Schäden zu bewahren gibt es nicht, vgl. Koch, Haftung für die Weiterverbreitung von Viren, in: NJW 2004, 801 (803); Spindler, Verantwortlichkeit und Haftung, in: MMR 2002, 495 (499).

127 Dem Szenario liegt eine Warnung des Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig-Holstein zu Grunde. Das ULD warnt in seinem 26. Tätigkeitsbericht vor dem Browser eines führenden Herstellers und setzt sich gleichzeitig mit Alternativen konkret auseinander, ohne jedoch einen bestimmten Browser zu empfehlen. Eine ausführliche Diskussion und die Empfehlung namentlich genannter alternativer Browser findet sich im 26. Tätigkeitsbericht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein 2004, Landtagsdrucksache vom 06.05.2004, 15/3300, S. 141 f.

128 BVerfG „Glykol", Beschluss v. 26.06.2002, 1 BvR 558/91, NJW 2002, 2621; BVerfG „Osho-Bewegung" Beschluss v. 26. 6. 2002, 1 BvR 670/91, NJW 2002, 2626.

129 Zur „Eingriffsproblematik": Voitl, Behördliche Warnkompetenz, 1993, S. 14, mit weiteren Hinweisen in Fn. 20.

1. Kompetenz

Hier soll der Frage nachgegangen werden, ob und welche öffentliche Stelle im Szenario 1 die Kompetenz besaß, Informationen über den Browser an die Nutzer weiterzugeben. Grundsätzlich ist zwischen horizontaler staatlicher Regierungskompetenz und administrativer Verwaltungskompetenz und der vertikalen Kompetenz auf Bundes- und Landesebene zu unterscheiden.

a) Bundesregierung

Mit dem Bundesverfassungsgericht ergibt sich die Rechtsgrundlage für Verbraucherwarnung aus der Regierungskompetenz. Daneben könnte sie als Annexkompetenz oder Kompetenz kraft Natur der Sache begründet werden, soweit sie nicht als Kompetenz spezialgesetzlich normiert ist oder für gar nicht existent gehalten wird.[130] Dieser Aufriss soll genügen. Eine weitergehende Auseinandersetzung mit der verfassungsrechtlichen Grundlage staatlicher (nicht administrativer) Warnkompetenz erscheint für diesen Zweck nicht gegeben, da das Feld mittlerweile tief durchdrungen ist[131] und das BVerfG sich in den jüngsten Entscheidungen[132] erneut für eine Kompetenz des Staates zu Warnungen aus der Staatsleitung ausgesprochen hat. Aus der in der Verfassung verankerten Befugnis der Regierung zur verantwortungsvollen Leitung des Staates ergebe sich das Recht der Regierung,

> *„zur Abwehr schwerwiegender Gefahren für wichtige Gemeinschaftsgüter die Öffentlichkeit umfassend über die gegebene Sachlage zu informieren.“*[133]

---

130 Gegen eine Kompetenz aus Art. 65 GG spricht, dass Art. 65 die Kompetenzverteilung normiert und selbst keine Kompetenz begründet. Insgesamt ablehnend, Voitl, Behördliche Warnkompetenz, 1993, S. 158 ff.

131 Die Rechtsprechung findet sich in den angrenzenden Fußnoten immer wieder zitiert, aus der Literatur kann auf folgenden Ausschnitt verwiesen werden: Gröschner, Öffentlichkeitsaufklärung, in: DVBl. 1990, 619; Gusy, Verwaltung durch Information, in: NJW 2000, 977; Kloepfer, Staatliche Informationen, 1989, S. 24 ff.; Leidinger, Hoheitliche Warnungen, Empfehlungen und Hinweise, in: DÖV 1993, 925; Voitl, Behördliche Warnkompetenz, 1993.

132 BVerfG „Glykol“, Beschluss v. 26.06.2002 - 1 BvR 558/91, NJW 2002, 2621; BVerfG „Osho-Bewegung“ Beschluss v. 26. 6. 2002 - 1 BvR 670/91, NJW 2002, 2626.

133 BVerfG „Glykol“, Beschluss v. 26.06.2002 - 1 BvR 558/91, Absatz-Nr. 14 (findet sich nur im Volltext, http://www.bverfg.de/entscheidungen.html (30.05.2006)); in diesem Sinne bereits BVerwG „Glykol“, Urteil v. 18.10.1990 - 3 C 2/88, NJW 1991, 1766 (1769); BVerwG „TM-Bewegung“, Urteil v. 23.05.1989 - 7 C 2/87, NJW 1989, 2272 (2273); BVerfG „TM-Bewegung“, Beschluss v. 15.08.1989 - 1 BvR 881/89, NJW 1989 3269 (3270); BVerwG „Osho-Bewegung“, Beschluss v. 13.03.1991 - 7 B 99/90, NJW 1991, 1770 (1772).

Das BVerfG verneint in der „Glykol" Entscheidung eine Zuordnung zu einer exekutiven Tätigkeit, da die Regierung nicht lediglich zur Gefahrenabwehr tätig geworden sei, sondern zur Bewältigung einer komplexen Krise.[134] Des Weiteren dient die Warnung dem Ziel *„dem Vertrauen und der Erwartungshaltung zu entsprechen und (…) den Weinmarkt zu stabilisieren."*[135]

Soweit oben die Informationsverwertung vornehmlich als Aufgabe der Gefahrenabwehr (grundsätzlich Verwaltungstätigkeit) einzustufen ist, ist eine Kompetenz der Regierung fraglich, jedoch im Bereich der Sicherheitslücken nicht ausgeschlossen, da diese Auswirkungen bei vielfältigen, öffentlichen Tätigkeiten haben können (entsprechend den vielfältigen Projekten des E-Government) – soweit sie Informations- und Kommunikationsangebote für den Bürger bereithalten. Diese beruht letztendlich auf der *„funktionsbedingten Befugnis zur Öffentlichkeitsarbeit*[136]*"* da sie durch den Einsatz von IT-Systemen in der Unterstützung ihrer Regierungsarbeit die Überwachung der IT-Systeme – und Aufdeckung von Sicherheitslücken – ebenfalls in ihrer spezifischen Regierungsfunktion wahrnehmen. Insofern unterscheidet sich die Situation von jeder bisher diskutierten Verbraucherwarnungen, da sowohl die Bürger als auch der Staat in allen seinen Einrichtungen und Ebenen bei Bedrohungen der IT-Sicherheit betroffen ist und der Staat durch den Einsatz von IT-Systemen und das Angebot des E-Governments eine eigen Gefahrenquelle schafft, über die der Bürger zu informieren sein könnte.

In diesem Sinne kann jede staatliche Stelle, also auch die Bundesregierung, ihr in der eigenen Praxis erworbenes Wissen zur Gefahrenprävention an die Bevölkerung grundsätzlich weitergeben. Diese Weitergabe muss nicht zwingend in öffentlichen Einzelwarnungen ausgesprochen werden, sondern die staatlichen Stellen könnten, ihre Erfahrungen an geeigneter staatlicher oder privater Stelle (etwa CERTs) veröffentlichen.

---

134 Die Komplexität der Zielverwirklichung als Argument gegen eine Verwaltungstätigkeit zu verwenden, vermag jedoch angesichts der tatsächlichen Verwaltungsaufgaben nicht zu überzeugen. Zudem belegen normierte Warnungs- und Aufklärungsbefugnisse – etwa im § 8 Abs. 4 S. 3 GPSG oder § 2 Abs. 1 Nr. 2 UBAG (Gesetz zur Errichtung eines Umweltbundesamtes) - dass diese Informationstätigkeiten der Verwaltung zuzurechnen sein können.

135 Huber, Die Informationstätigkeit der öffentlichen Hand, in: JZ 2003, 290 (291).

136 Schatzschneider, Informationshandeln im Bundesstaat, in: NJW 1991, 3202 (3202).

b) BSI und Landesdatenschutzbeauftragte

Fraglich ist, ob dem BSI und dem Landesdatenschutzbeauftragten eine (parallele) administrative Kompetenz für die Verbraucherwarnungen wie im Szenario 1 zusteht.

Das Bundesverfassungsgericht will für Verbraucherwarnungen das Nebeneinander der Bundesstaatlichen und Länderkompetenzen sowie der administrativen Kompetenzen im Informationshandeln nicht grundsätzlich ausschließen.[137] Es wäre sogar unbedenklich, da das Informationshandeln der Bundesregierung

> *„weder das der Landesregierungen für ihren Verantwortungsbereich ausschließt oder behindert noch den Verwaltungsbehörden verwehrt, ihre administrativen Aufgaben zu erfüllen."*[138]

Eine weit verbreitete Ansicht in der Literatur tritt der Auffassung des BVerfG mit Art. 30, 83 GG entgegen, nach denen zuförderst die Länder zu einer Informationstätigkeit durch Warnungen befugt seien.[139] Fraglich ist, ob die informationsbehördliche Verwaltungsbefugnis beim Bund oder bei den Ländern angesiedelt ist.

Soweit Informationen über Sicherheitslücken im Internet einen Beitrag für die IT-Sicherheit leisten, könnte die Gesetzgebungskompetenz für die weiteren Überlegungen entscheidend sein.[140] In Betracht kommen Art. 73 GG Nr. 7 GG (Post und Telekommunikation)[141], Art. 74 Abs. 1 Nr. 11 GG (Wirtschaft)[142] sowie die (örtliche) Sicherheit und Ordnung aus Art. 70 GG. So wie die Errichtung des BSI aus Art. 87 Abs. 3 GG für eine Kompetenz der Bundesverwaltung im Bereich der IT-Sicherheit sprechen kann, so können das Nebeneinander von Bundes- und Landesdatenschutzgesetzen für eine Kompetenz von Bund- und Landesverwaltung sprechen. Da der Einsatz des Internets in allen gesellschaftlichen Bereichen denk-

---

137 BVerfG „Glykol", Beschluss v. 26.06.2002 - 1 BvR 558/91, NJW 2002, 2621 (2623).

138 BVerfG „Glykol", Beschluss v. 26.06.2002 - 1 BvR 558/91, NJW 2002, 2621 (2624).

139 Statt vieler: Schatzschneider, Informationshandeln im Bundesstaat, in: NJW 1991, 3202 (3202); Voitl, Behördliche Warnkompetenz, 1993, S. 111, explizit auch für die „gesetzesfreie hoheitliche Tätigkeit".

140 A. A. Schatzschneider, Informationshandeln im Bundesstaat, in: NJW 1991, 3202 (3202), der nicht von der Gesetzgebungsbefugnis auf eine informationsbehördliche Verwaltungsbefugnis schließen will.

141 Vgl. § 109 TKG, der als Norm des IT-Sicherheitsrechts dem TKG und damit der Kompetenz aus Art. 73 GG Nr. 7 GG unterfallen kann.

142 Der Gesetzesentwurf des BSIG stützt sich auf Art. 74 Abs. 1 Nr. 11 GG, vgl. Gesetzesentwurf des BSIG vom 23.02.1990, BR-Drs. 134/90, S. 17. Die Kompetenz für das BDSG (§ 9 BDSG) stützt sich auf Art. 74 Abs. 1, 11 und 12 GG, vgl. Gesetzesentwurf des BDSG vom 18.08.2000, BR-Drs. 460/00, S. 66.

bar ist, ist ebenso eine Regelung des Umgangs in allen Bereichen denkbar. Letztendlich verwischen die möglichen Sachkompetenzparallelen eine Abgrenzung zwischen Bundes- und Landesverwaltung.[143] Der ubiquitäre Einsatz von IT-Systemen in der Verwaltung indiziert eine ubiquitäre Kompetenz über Gefahren zu warnen, die aus dem Einsatz resultieren. Im diesem Sinne, das „Ob" einer Kompetenz der Verwaltung zur Informationen über Sicherheitslücken bejahend:

> *„Die Verbraucherinnen und Verbraucher dürfen von der von ihnen finanzierten und zu ihrem Schutz tätigen Verwaltung erwarten, dass sie über wesentliche Erkenntnisse unterrichtet werden."*[144]

In diesem Sinne nur die Frage der Kompetenz offen abschließend: Es

> *„stellt sich bei allen Krisen im Bereich des Verbraucherschutzes stets ein polyphones Konzert aus Informationen der EG-Kommission, der Bundesregierung, der Landesregierungen, nachgeordneten Behörden und zunehmend auch von Vertretern von NGOs ein."*[145]

Die Annahme einer klaren Trennung der Kompetenzen ist bei einem informationellen Verwaltungshandeln auch nicht schädlich, da keine Gefahr widersprechender Entscheidungen bestehe.[146]

Die Annahme von parallelen Kompetenzen erscheint sachgerecht, da die Regierungs- und Verwaltungspraxis im Umgang mit dem Internet unterschiedliche sicherheitsrelevante Informationen (über Sicherheitslücken) hervorbringen kann. Dies ist nicht zuletzt Ausfluss aus der Überlegung, dass IT-Sicherheit nur durch gemeinsames Wachsen und den Austausch aller Nutzer verbessert werden kann.

Festzuhalten ist, dass das BSI und der Landesdatenschutzbeauftragte grundsätzlich eine Kompetenz zu Verbraucherwarnungen im Bereich der IT-Sicherheit haben.

2. Ermächtigungsgrundlage

Eine Pflicht oder ein Recht des Staates zur Warnung – unter der Prämisse des mittelbar-faktischen[147] Grundrechtseingriffs der Warnung – erfordert auf Grundlage

---

143 Murswiek, Das Bundesverfassungsgericht und die Dogmatik mittelbarer Grundrechtseingriffe, in: NVwZ 2003, 1 (7); Gröschner will deshalb eine Informationstätigkeit des Bundes zur Gefahrenabwehr nur im Einzelfall über die Amtshilfe nach Art. 35 GG zulassen, Gröschner, Öffentlichkeitsaufklärung, in: DVBl. 1990, 619 (624 f.).

144 Knitsch, Die Rolle des Staates im Rahmen der Produktinformation, in: ZRP 2003,113 (117), der für eine gesetzliche Regelung der Verbraucherinformationen plädiert.

145 Huber, Die Informationstätigkeit der öffentlichen Hand, in: JZ 2003, 290 (296).

146 Lübbe-Wolff, Rechtsprobleme der behördlichen Umweltberatung, in: NJW 1987, 2705 (2708); a.A. Heintzen, der Bürger sei davor zu schützen, dass er nicht von mehren staatlichen *„Propagandaapparaten gleichzeitig"* überzogen werde, vgl. Heintzen, Hoheitliche Warnungen und Empfehlungen, in: NJW 1990, 1448 (1449).

der Lehre vom Gesetzesvorbehalt und der Wesentlichkeitstheorie[148] grundsätzlich eine einfachgesetzliche Ermächtigungsgrundlage.[149]

Daraus folgt, dass der Gesetzgeber alle Risken vor denen gewarnt werden könnte normativ zu regeln hätte. Deshalb wird teilweise die mangelnde Normierbarkeit mittelbar-faktischer Wirkungen angeführt,[150] und der Gesetzesvorbehalt für die staatliche Informationstätigkeit für überflüssig und als nicht zu beachtend erklärt.[151] Soweit angeführt wird, die Wirkung sei nicht steuerbar und damit auch nicht normierbar, kann entgegengehalten werden, dass nicht die Wirkung der Information den Grundrechtseingriff impliziert, sondern der Inhalt der Information ausschlaggebend ist (vgl. oben die Unterscheidung zwischen Produkttyp und Produkt), den die informierende Behörde steuern kann. Zudem belegt die Gesetzgebungspraxis, dass die Informationstätigkeit sich nicht grundsätzlich der Normierung entzieht, bzw. der Gesetzesvorbehalt im Bereich der faktisch-mittelbaren Eingriffe nicht aufgegeben werden muss.[152]

Soweit die Informationsverwertung eine administrative Tätigkeit ist, bedarf es auch nach dem BVerfG einer expliziten Ermächtigungsgrundlage.[153] Die allgemeine Befugnis einen Verwaltungsakt, etwa ein Verbot, erlassen zu können, soll nicht ausreichen, da die steuernde Wirkung der Informationstätigkeit schwer kalkulierbar sei.[154] Die grundrechtsbeeinträchtigende Wirkung der Warnung stellt die Regierungskompetenz an sich in Frage, da nicht überzeugend ist, warum nicht immer

---

147 Vgl. BVerfG „Osho-Bewegung", Beschluss v. 26.6.2002 - 1 BvR 670/91, NJW 2002, 2626 (2626), dieses nimmt eine mittelbar-faktische Grundrechtsbeeinträchtigung an.

148 Kloepfer, Informationsrecht, 2002, S. 105, Rd. 116.

149 Bejahend Murswiek, Das Bundesverfassungsgericht und die Dogmatik mittelbarer Grundrechtseingriffe, in: NVwZ 2003, 1 (6); ablehnend BVerfG „Glykol", Beschluss v. 26.06.2002 - 1 BvR 558/91, NJW 2002, 2621 (2622 f.); BVerfG „Osho-Bewegung", Beschluss v. 26.06.2002 - 1 BvR 670/91, NJW 2002, 2626 (2626).

150 BVerfG „Osho-Bewegung", Beschluss v. 26.06.2002 - 1 BvR 670/91, NJW 2002, 2626 (2629).

151 Huber, Die Informationstätigkeit der öffentlichen Hand, in: JZ 2003, 290 (294), m. w. H.

152 Ebenso Huber, a.a.O., (Fn. 151), 290 (295).

153 BVerfG „Glykol", Beschluss v. 26.06.2002 - 1 BvR 558/91, NJW 2002 2621 (2623), nennt exemplarisch - wohl nunmehr den einschlägigen - § 10 Abs. 2 GPSG. Weitere bereichsspezifische Ermächtigungsgrundlage in diesem Sinne sind etwa § 28 Abs. 4 Medizinproduktegesetz und § 69 Abs. 4 Arzneimittelgesetz.

154 Käß, Die Warnung als verwaltungsrechtliche Handlungsform, in: WiVerw 2002, 197 (206), der darauf hinweist, dass das Verwaltungshandeln durch Verwaltungsakte rechtlich steuer- und damit im Gegensatz zur Informationstätigkeit kalkulierbar ist. Dies kann etwa mit der Verselbständigung des Inhalts der Warnung und Empfehlung des BSI zu Browsern in der Aufbereitung durch die Medien belegt werden.

einer administrativen Informationstätigkeit mit der rechtlichen Absicherung über den Gesetzesvorbehalt der Vorzug zu geben ist.

a) Bundesregierung

Soweit es sich um eine Informationstätigkeit der Regierung handelt, schließt das BVerfG von der Aufgabe auf die Befugnis. Damit sei das Erfordernis einer Ermächtigungsgrundlage nicht gegeben.[155] Ohne Ermächtigungserfordernis muss die Informationstätigkeit allerdings zumindest allgemeinen Rechtmäßigkeitsanforderungen genügen.[156] Zu nennen ist hier das Übermaß- und Willkürverbot. Aus letzterem folgt das Gebot, Tatsachen sachlich zutreffend wiederzugeben.[157] Da die Warnung zutreffend ist, ist eine Ermächtigungsgrundlage nicht notwendig.

b) BSI

Im Errichtungsgesetz zum BSI findet sich keine Ermächtigungsgrundlage für Warnungen. Nach § 3 Abs. 1 Nr. 7 BSIG hat das BSI lediglich die Aufgabe zu beraten.

Kennzeichen der Beratung soll grundsätzlich eine gerichtete, individuelle und dialog-offene Informationstätigkeit sein.[158] Damit unterscheidet sie sich von der Warnung und Aufklärung, die an die Allgemeinheit gerichtet sind.[159] Wenn die Beratung nicht dialog-offen ist, d. h. nicht offen für Äußerungen und Fragen des Beratenden, handelt es sich begrifflich um Aufklärung oder Warnung.[160] Soweit das BSI sich mit Mailinglisten an die Bürger wendet, Informationsschriften herausgibt oder auf der Webpräsenz Informationen zu Sicherheitslücken und Schwachstellen der IT-Systeme veröffentlicht, fehlt der diskursive Charakter. Somit könnte diese Informationstätigkeit als Aufklärung und nicht als Beratung zu qualifizieren sein.

---

155 Nach dem BVerfG „Glykol", Beschluss v. 26.06.2002 - 1 BvR 558/91, NJW 2002, 2621 (2623) liegt *„in der Aufgabenzuweisung grundsätzlich auch eine Ermächtigung zum Informationshandeln"*.

156 Kloepfer, Informationsrecht, 2002, S. 105 f., Rd. 117.

157 BVerfG, „TM-Bewegung", Beschluss v. 15.08.1989 - 1 BvR 881/89, NJW 1089, 3269 (3270).

158 Oebbecke, Beratung durch Behörden, in: DVBl. 1994, 147 (150). Hier wird auf die Beratung rekurriert, obwohl sie als individuelle Informationstätigkeit für Informationen über Sicherheitslücken grundsätzlich als nicht geeignet zu bewertet ist.

159 Vgl. im SGB I wird etwa unterschieden die Bevölkerung aufzuklären (§ 13 SGB I) vgl. SGB I Kommentar, § 13 Rd. 5 und den Einzelnen zu beraten (§ 14 SGB I).

160 Oebbecke, a.a.O., (Fn. 158), 147 (150).

Nach der Begründung zum Gesetzesentwurf umfasst die Aufgabe des BSI

> *„insbesondere das Aufzeigen von Risiken bei der Anwendung der Informationstechnik sowie geeigneter Sicherheitsvorkehrungen. Das Bundesamt erfüllt die Aufgabe z. B. durch die Veröffentlichung von Informationsbroschüren und –schriften, die Durchführung von Lehrgängen, Seminare oder Kolloquien.“*[161]

Soweit sich die Gesetzesbegründung zum BSIG auf Informationsschriften bezieht, deutet dies auf eine breitere Massenwirkung der Beratung als das vorgenannte enge Verständnis – insbesondere auf die Initiative des BSI - hin.

Aus dem oben genannten Begriffsverständnis von Beratung würde sich in der Konsequenz ergeben, dass die tatsächliche Informationstätigkeit des BSI über die Beratung hinausgeht. Allerdings muss zugestanden werden, dass dieses Begriffverständnis von Beratung regelmäßig, aber nicht in jedem Fall mit dem Sprachgebrauch des Gesetzgebers übereinstimmt.[162]

Soweit die Informationstätigkeit des BSI über einen engen Begriff der Beratung in Form von Aufklärung oder Warnung hinausgeht, stellt sich die Frage nach der Ermächtigungsgrundlage.[163] Ob § 3 Abs. 1 Nr. 7 BSIG eine Ermächtigungsgrundlage für eine hier verstandene Aufklärung ist, ist eine Frage der Auslegung. In Anbetracht der Tatsache, dass das informale Verwaltungshandeln erst Ende der achtziger Jahre stärkeres juristisches Interesse gefunden hat,[164] erscheint es gerechtfertigt, nicht an dem engen Begriff haften zu bleiben, sondern die grammatische Auslegung durch die historische und teleologische zu ergänzen. Sinn und Zweck des BSI ist die Erhöhung der Sicherheit in der Informationstechnik. Zudem konstatiert der Gesetzgeber in der Begründung zum BSIG, dass ein gewisser Sicherheitsstandard den über Sicherheitsrisiken informierten Hersteller, Vertreiber und Anwender voraussetzt.[165] Somit könnte durch § 3 Abs. 1 Nr. 7 BSIG zumindest auch öffentlichkeitsbezogene Aufklärung abgedeckt sein.

---

161 Gesetzesentwurf des BSIG vom 23.02.90, BR-Drs. 134/90, S. 28.

162 Übereinstimmend §§ 13, 14 SGB I, § 26 Abs. 3 S. 1 BDSG, § 8 Abs. 2 BSHG, § 2 des Gesetzes zur Vermeidung und Bewältigung von Schwangerschaftskonflikten; Abweichend: § 25 VwVfG Beratung im Sinn von Belehrung; die Beratung und Information im Sinne des § 38 Abs. 1 Krw-/AbfG umfasst hingegen vielfältige Methoden, Gegenstände und Inhalte, auch die Warnung und Empfehlung sollen erfasst sein, Kunig/Paetow/Vestyl, Krw-/AbfG, 1998, § 38 Rd. 19.

163 Aus dem Rechtsstaats- und Demokratieprinzip ergebe sich eine Zuständigkeit der Behörde, die Öffentlichkeit im Rahmen ihrer ihr zugewiesen Sachaufgaben über die Aufgabenerfüllung und über aus der Aufgabenerfüllung angefallene Erkenntnisse von öffentlichem Interesse zu informieren, Lübbe-Wolff, Rechtsprobleme der behördlichen Umweltberatung, in: NJW 1987, 2705 (2707). Diese ist jedoch mit den Warnungen im Szenario 1 nicht tangiert.

164 Oebbecke, a.a.O., (Fn. 158), 147 (148).

165 Begründung zum Gesetzesentwurf des BSIG vom 23.02.1990, BR-Drs. 134/90, S. 13.

Ein Vergleich mit den normierten Aufgabenkatalogen anderer Bundesämter zeigt, dass dort die Informationstätigkeit wesentlich konkreter geregelt ist, vgl. etwa das Bundesinstitut für Arzneimittel und Medizinprodukte in Verbindung mit den Fachgesetzen (AMG und MPG). Dieses Institut ist zeitlich später im Rahmen der Neuordnung der Einrichtungen des Gesundheitswesens 1994 entstanden. Zum Zeitpunkt des Erlasses des BSIG war die Bedeutung der Informationstechnik noch nicht abzusehen. Das Internet findet explizit keine Erwähnung.[166] Das technische Entwicklungspotenzial der dem BSI zugewiesenen Aufgabe findet sich aber in einem Hinweis zur Informationsqualität wieder: Die Beratungen setzen voraus, dass der Wissenstand des BSI dem der Wissenschaft und Technik entspricht.[167]

Ein Vergleich mit anderen Ermächtigungsgrundlagen für administrative Informationstätigkeit zeigt, dass an die Warnung die allgemeinen Anforderungen aus dem entsprechenden Verwaltungsverfahrensrecht gestellt werden.[168] Spezialgesetzlich geregelt lassen sich solche Anforderungen exemplarisch dem GPSG entnehmen. Demnach hat die zuständige Behörde Befugnis zur Aufklärung des Sachverhaltes, § 8 Abs. 7 ff. GPSG. Darüber hinaus ist der betroffene Hersteller grundsätzlich anzuhören, § 10 Abs. 4 S. 2 GPSG. Schließlich ist stets eine Abwägung der Interessen geregelt.[169] Vor allem ist die Warnung - wie etwa der Subsidiarität der behördlichen Warnung nach § 8 Abs. 4 S. 3 GPSG zu entnehmen – als Ultima Ratio vorgesehen. Eine Warnung durch die Behörde ist nur vorgesehen, soweit Warnungen durch den Hersteller nicht oder nicht rechtzeitig getroffen werden.

Dieser Vergleich macht deutlich, dass die weitergehende Beeinträchtigung von Grundrechtspositionen durch Warnungen gesetzlich Berücksichtigung findet.

---

166 Allerdings findet sich bereits der Gedanke des Zusammenhangs zwischen ausreichenden Sicherheitsstandard und der Information über Bedrohungen und Risiken wieder, zum Gesetzesentwurf des BSIG vom 23.02.1990, BR-Drs. 134/90, S. 13.

167 Zum Gesetzesentwurf des BSIG vom 23.02.1990, BR-Drs. 134/90, S. 28.

168 Käß, Die Warnung als verwaltungsrechtliche Handlungsform, in: WiVerw 2002, 197 (207 ff.)

169 Vgl. Entwurf eines Verbraucherinformationsgesetzes vom 15.03.2002, BR-Drs. 210/02 (dieses Gesetz wurde in der 14. Legislaturperiode mangels Zustimmung des Bundesrates nicht verabschiedet.):
§ 6 des Entwurfs eines Verbraucherinformationsgesetzes *(1) Die Behörde kann die Öffentlichkeit unter Nennung des Erzeugnisses sowie derjenigen, die das Erzeugnis hergestellt oder in Verkehr gebracht haben, über im Interesse des Verbraucherschutzes liegende bedeutsame Sachverhalte informieren, soweit hieran ein besonderes Interesse der Öffentlichkeit besteht und dieses Interesse gegenüber den Belangen des Betroffenen überwiegt. (2) Ein besonderes Interesse der Öffentlichkeit liegt in der Regel vor, (…) 3. wenn hinreichende Anhaltspunkte dafür vorliegen, dass von einem Erzeugnis eine Gefährdung für die Sicherheit und Gesundheit ausgehen kann und aufgrund unzureichender wissenschaftlicher Erkenntnisse oder aus sonstigen Gründen die Unsicherheit nicht innerhalb der gebotenen Zeit behoben werden kann.*

Demnach kann dem BSIG zwar eine Befugnis zur Aufklärung, jedoch keine Befugnis zur Warnung/Empfehlung der Öffentlichkeit vor Sicherheitslücken entnommen werden. Soweit man die „Beratung" des § 3 Abs. 1 Nr. 7 BSIG in historischer und teleologischer Auslegung mit „Massenwirkung" versehen kann, ist darin allenfalls eine Befugnis zur Aufklärung im oben beschriebenen Verständnis zu sehen. D. h. die Befugnis zu einer Informationstätigkeit, die sich nicht auf konkret gefährliche Produkte bezieht.[170] Soweit die Informationstätigkeit in Grundrechte eingreift, ist eine entsprechend dem GPSG normierte Regelung der Informationstätigkeit erforderlich.

Für das Beispiel aus Szenario 1 heißt dies konkret, dass das BSI ohne gesetzliche Grundlage und damit rechtswidrig handelt.

c) Landesdatenschutzbeauftragte

Eine Ermächtigungsgrundlage des Landesdatenschutzbeauftragten Schleswig-Holstein (im Folgenden ULD) vor einem Browser zu warnen bzw. konkrete Alternativen zu empfehlen, könnte sich dem Datenschutzgesetz Schleswig-Holstein (DSG-SH) entnehmen lassen. An den Bürger gewandt kann es in Fragen zum Datenschutz und zur Datensicherheit beraten und informieren, § 43 Abs. 1 DSG-SH. Die offene Formulierung „informieren" bietet dem ULD vielfältige Informationsoptionen, die auch Warnungen und Aufklärungen umfassen können.

Die Äußerungen, auf die sich die Überlegungen beziehen, waren allerdings nicht an den Bürger, sondern als Tätigkeitsbericht § 39 Abs. 4 S. 2 DSG-SH an den Landtag gerichtet. Ein Tätigkeitsbericht muss seiner Natur nach inhaltlich umfassend informieren, da er Rechenschaft über die Arbeit abgibt und zudem ein Instrument der Informationsbeschaffung für die gesetzgeberische Tätigkeit des Landtages ist.[171] Als „staatsinterne" Informationstätigkeit fehlt ihm damit eine Qualität zur Verhaltensteuerung von Grundrechtsträgern, da die Adressaten als Mitglieder des Landtags lediglich „innenparlamentarische Öffentlichkeit" sind.[172] Insoweit kann § 39

---

170 Soweit das CERT des BSI in der Praxis eingehende Meldungen der Hersteller zu Schwachstellen und Sicherheitslücken bearbeitet, bewertet und veröffentlicht, ist mangels Freiwilligkeit und eigener Initiative der Hersteller eine Grundrechtsbeeinträchtigung abzulehnen. Vgl. http://www.bsi.de/certbund/infodienst/akt_adv.htm (30.05.2006).

171 Simitis u. a., BDSG/*Dammann,* § 26 Rd. 4 f., der auf die Funktion als Basis politischer oder gesetzgeberischer Korrekturen hinweist.

172 Eine indirekt steuernde Wirkung ergibt sich jedoch gerade im Hinblick auf die Parlamentsöffentlichkeit, Art. 42 Abs. 1 S. 1 GG. Allerdings liegt der Grad und der Umfang der

Abs. 4 S. 2 DSG-SH eine Legitimationsgrundlage auch für die mit der Möglichkeit der Verbreitung der Information (vgl. Art. 15 Abs. 1 S. 1 der Verfassung Schleswig-Holstein zur Parlamentsöffentlichkeit) verbundenen Grundrechtsverletzungen bieten.

Einem Urteil des VG Köln kann auch mangels Vergleichbarkeit nichts Gegenteiliges entnommen werden: Gegenstand der Entscheidung ist eine einstweilige Anordnung, mit der ein Hersteller einer Datenbank die Unterlassung einer Presseerklärung des Bundesbeauftragten (BfD) für Datenschutz begehrte.[173] Dieser beanstandete das Produkt des Herstellers, eine Software, mit der Bild-, Adress- und Telefondaten zu einer bestimmten Person zugeordnet werden können. Eine Grundrechtsbeeinträchtigung wurde vom Gericht – trotz Nicht-Nennung des Namens des Unternehmens durch den Datenschutzbeauftragten – angenommen. Das Gericht sah es als ausreichend an, dass in der anschließenden Diskussion in den Medien das Unternehmen namentlich erwähnt wurde.[174]

Zum Zeitpunkt des Urteils sah das BDSG keine Ermächtigungsgrundlage des BfD, die Öffentlichkeit zu informieren, vor. Das VG Köln verurteilte den BfD aufgrund der Unverhältnismäßigkeit der Äußerungen. Nach Ansicht des Gerichts war eine Ermächtigungsgrundlage nicht erforderlich, da hier eine *„eng einzugrenzende Modifikation des Grundsatzes des Vorbehaltes des Gesetzes"*[175] vorliege. In einer zeitlich nachfolgenden Gesetzesnovelle wurde erst Satz 2 in § 26 Abs. 1 BDSG eingefügt, der der Praxis des BfD, regelmäßig über den Tätigkeitsbericht hinaus die Öffentlichkeit zu informieren, eine gesetzliche Grundlage schuf. § 26 Abs. 1 S. 2 BDSG sieht einen allgemeinen Auftrag des Bundesdatenschutzbeauftragten (BfD) zur Unter-

---

Verbreitung in den Händen Dritter wie der Opposition, Medien, etc., vgl. auch Zöllner, Der Datenschutzbeauftragte, 1995, S. 102 f.

173 VG Köln, Beschluss v. 11.03.1999 – 20 L 3737/98, CR 1999, 557. Aus Anlass des Urteils des VG Köln wurde § 26 Abs. 1 S. 2 BDSG mit der Änderung des BDSG 2000 neu eingefügt, so Simitis u. a., BDSG/*Dammann,* § 26 Rd. 8a. Dies ist der Gesetzesbegründung vom 18.08.2000, BR-Drs. 461/00, S. 104, zur Änderung des BDSG zwar nicht zu entnehmen, jedoch erschien eine entsprechende Klarstellung aufgrund der langjährigen Praxis geboten.

174 VG Köln, Beschluss v. 11.03.1999 – 20 L 3737/98, CR 1999, 557 (558)

175 VG Köln, Beschluss v. 11.03.1999 – 20 L 3737/98, CR 1999, 557 (558); zustimmend Ehmann, Anmerkungen zu VG Köln Beschluss v. 11.03.1999 – 20 L 3737/98, in: CR 1999, 560 (561), der entsprechend dem VG Köln aus der Gesamtschau der Regelungen zum Bundesdatenschutzbeauftragten diesem eine Befugnis, Warnungen gegenüber der Öffentlichkeit auszusprechen, zuspricht. Dagegen Zöllner, Der Datenschutzbeauftragte, 1995 S. 102 f., der den Datenschutzbeauftragten in erster Linie als Zuarbeiter für Verfassungs- und Verwaltungsorgane sieht.

richtung des Deutschen Bundestages *und* der Öffentlichkeit vor und ist insoweit eine explizite Ermächtigungsgrundlage für die Information der Öffentlichkeit.[176]

Festzuhalten ist, für die Warnung des Landesdatenschutzbeauftragten im Szenario 1 gibt § 39 Abs. 4 S. 2 DSG-SH eine Ermächtigungsgrundlage.

3. Grundrechtseingriff

a) Grundrechtseingriff bei Verbraucherwarnungen

Für die Betrachtung, in welche Kommunikationsbeziehungen staatliche Informationstätigkeit im Bereich der Information über Sicherheitslücken eingreifen kann, soll zunächst allgemein auf die Voraussetzungen eines Grundrechtseingriffs durch Warnung eingegangen werden.[177] Vorangestellt werden die Kriterien für die Grundrechtseingriffsqualität des BVerwG und der Literatur bei Verbraucherwarnungen.

Die Eingriffsqualität der Warnungen liegt vor, wenn sie unter

> *„- Inanspruchnahme der staatlichen Autorität erfolgen und*
>
> *- auf die Verhaltenslenkung in dem geschützten Freiheitsbereich abzielen (Finalität)*
>
> *- oder die Lenkung des Verhaltens Dritter bezwecken, als dessen Kehrseite Nachteile im grundrechtlich geschützten Freiheitsbereich des Grundrechtssubjektes notwendig auftreten (Finalitätsäquivalent)"*[178].

Soweit die Maßnahmen nicht auf den geschützten Freiheitsbereich zielen, stellt sich die Frage des Finalitätsäquivalents. Bei der Frage der Richtung der Maßnahme ist die Alternative des Finalitätsäquivalents relevant. Ziel der Warnung ist nicht

---

176 Simitis u. a., BDSG/*Dammann,* § 26 Rd. 8c, der für den Fall von wahrheitswidrigen und „sonstigen geschäftsschädigenden" Äußerungen auf die allgemeinen Grundsätze der Amtshaftung verweist. Im Übrigen treffe den Datenschutzbeauftragten eine Sorgfaltspflicht, die abhängig von den negativen Auswirkungen auf den Geschäftsbetrieb des betroffenen Unternehmens sei. Bei möglicherweise gravierenden Folgen bedürfe es einer Verifizierung durch Anhörung des Betroffenen, a.a.O., Rd. 8d. Das heißt im Umkehrschluss, dass die Veröffentlichung zutreffender Tatsachen ohne weiteres Verfahren möglich ist.

177 Auf die Annahme des BVerfG ein Grundrechtseingriff liege bei einer staatlichen Informationstätigkeit nur dann vor, wenn eine (verfassungsrechtliche) Aufgabenzuweisung fehlt und die Zuständigkeitsordnung und Anforderungen an die Richtigkeit und Sachlichkeit von Informationen missachtet wurde soll hier (zunächst) nicht eingegangen werden., vgl. BVerfG „Glykol", Beschluss v. 26.06.2002 - 1 BvR 558/91, NJW 2002, 2621 (2622). Ausführliche Kritik an den Anforderungen des BVerfG: Huber, Die Informationstätigkeit der öffentlichen Hand, in: JZ 2003, 290 (292 ff.).

178 Murswiek, Das Bundesverfassungsgericht und die Dogmatik mittelbarer Grundrechtseingriffe, in: NVwZ 2003, 1 (2), die Literatur und die Rechtsprechung des BVerwG zusammenfassend.

zwingend, in die Kommunikationsbeziehung zwischen Hersteller und Verbraucher einzugreifen, der Nutzer soll nicht primär als Kunde ausbleiben. Das BVerfG verneint grundsätzlich eine steuernde Wirkung von Verbraucherwarnungen, da das eigentliche Ziel die Schaffung von Markttransparenz sei. Ein Ausgleich durch Verbraucherwarnungen sei geradezu indiziert, da Defizite in der Verfügbarkeit von Information die Steuerungskraft des Marktes bedrohe.[179] Ziel ist demnach lediglich, dem Nutzer Wissen als Handlungsgrundlage zu geben. Dieses Ziel bewirkt jedoch nicht notwendigerweise Nachteile in grundrechtlich geschützten Freiheitsbereichen Dritter (kein Finalitätsäquivalent). Damit ist die Grundrechtsrelevanz von Verbraucherwarnungen regelmäßig abzulehnen.

b) Grundrechtseingriff durch die Informationen im Szenario 1

Die folgenden Ausführungen beziehen sich gleichermaßen auf die Informationen der Bundesregierung, des BSI und des Landesdatenschutzbeauftragen. Als staatliche Maßnahmen unterliegen sie den Voraussetzungen des BVerwG für Verbraucherwarnungen.

Die Informationen erfolgen auch im Bereich der Information über Sicherheitslücken – soweit staatliche Stellen stets kraft Definition handeln – mit dem Stempel staatlicher Autorität, etwa des BSI.

Im Hinblick auf die Konstellation im Szenario 1, in dem die staatlichen und administrativen Stellen vor der Nutzung des Browsers eines führenden Herstellers warnen, kommen Nachteile für die unternehmerische Betätigung des Herstellers und somit Eingriffe in Art. 14 Abs. 1 und 2 Abs. 1 GG in Betracht.[180]

Im Zusammenhang mit Verbraucherwarnungen ist umstritten, welche Grundrechte der Unternehmen betroffen sein können. Die Entscheidung hängt von der Betonung der Wirkung ab. Soweit eine reputationsschädigend Wirkung der Nennung des Namens des Herstellers im Zusammenhang mit der Sicherheitslücke betont wird, könnte Art. 2 Abs. 1 GG tangiert sein.[181] Soweit über die reputationsschädi-

---

179 BVerfG „Glykol", Beschluss v. 26.06.2002 - 1 BvR 558/91, NJW 2002, 2621 (2622).

180 Auf Art. 12 GG soll nicht eingegangen werden, da der Browser nur ein kleiner Bereich nicht einmal ein Marktsegment des Herstellers ist und somit ein Eingriff in die berufliche Betätigungsfreiheit nicht ersichtlich ist.

181 Dreier qualifiziert rufschädigende Äußerungen der öffentlichen Verwaltung oder eine durch die Öffentlichkeitsarbeit der Regierung eintretende Rufschädigung als faktischen Eingriff in Art. 2 Abs. 1 GG, *Dreier*, in: Dreier (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 2. Aufl. 2004, Art. 2 I Rd. 84; regelmäßig keinen Eingriff durch staatliche Information und Aufklärung in

gende Wirkung die Absatzchancen miniert werden, könnten die Wirtschafts- und Unternehmergrundrechte[182] – namentlich Art. 14 Abs. 1 GG betroffen sein. Zunächst ist jedoch geboten sich den Inhalt der Information und ihre Wirkung zu verdeutlichen

Die Informationen über den Browser zielen zum einen auf Sicherheitslücken, die unabhängig von dem bestimmten Produkt eines Herstellers der Produktgattung zu eigen sind, zum anderen auf Sicherheitslücken des konkreten Produkts.

Soweit die Sicherheitslücken Modifikationen bei den Einstellungen von Produkten oder Systemen betreffen, die der Nutzer bereits besitzt, haben diese mehr eine gebrauchsanleitende und weniger eine das konkrete Produkt ablehnende Funktion. Soweit vor dem Einsatz von Java-Script gewarnt wird, dessen Funktion deaktiviert werden kann,[183] liegt keine Warnung, sondern eine Aufklärung vor, deren Eignung zur Grundrechtsbeeinträchtigung regelmäßig abgelehnt wird.[184] Ein Grundrechtseingriff liege bei Aufklärung nicht vor, soweit sie sich nicht auf bestimmte Produkte eines Herstellers, sondern auf den speziellen Produkttypen als solchen, beziehe.[185] Dies sei auch der Fall, wenn das Produkt regelmäßig nur von einem Monopolunternehmen vertrieben werde.[186] Allein die Information bezüglich Java-Script ist eine Aufklärung hinsichtlich eines Teiles eines Produkttypen und demnach „*grundrechtsneutral*“[187]. Verbunden mit weiteren Sicherheitslücken und der Ablehnung des konkreten Browsers kommt allerdings ein Eingriff in Art. 2 Abs. 1 GG in Betracht.

Art. 2 Abs. 1 GG nimmt dagegen Kunig an, v. Münch/Kunig (Hrsg.) Grundgesetz-Kommentar, Bd. 1, 5. Aufl. 2000, Art. 2 Rd. 18; Philipp, Staatliche Verbraucherinformationen, 1989, S. 181, misst den Ruf an Art. 14 Abs. 1 GG und lehnt einen Eingriff, mangels der Qualifizierung des Rufs als subjektives Recht, ab.

182 Vgl. Gröschner, Öffentlichkeitsaufklärung, in: DVBl. 1990, 619 (626). Unter Wirtschafts- und Unternehmergrundrechte können Art. 14 Abs. 1, 12 Abs. 1 und 2 Abs. 1 GG verstanden werden.

183 Soweit die Deaktivierung des Java-Script dazu führt, dass eine Webseite nicht mehr vollständig oder wie vorgesehen angezeigt wird, könnte allerdings an die Beeinträchtigung von Rechten aus Art. 12 oder 2 Abs. 1 GG des Anbieters der Seite gedacht werden.

184 Gröschner, Öffentlichkeitsaufklärung, in: DVBl. 1990, 619 (627).

185 Philipp, Staatliche Verbraucherinformationen, 1989, S. 158. Die Warnung bzw. die Empfehlung kann sich jedoch auch grundsätzlich absatzfördernd auswirken, wenn der Einsatz eines bestimmten Produkttyps (Firewall, Virenschutz) für erforderlich gehalten – und vor dem Fehlen demnach gewarnt wird – ohne ein spezifisches Produkt zu empfehlen.

186 A. A. Schmid, Strom- und Energiesparmarketing, 1997, S. 104: In eine Grundrechtsbetrachtung könnte einfließen, dass der Hersteller eines Produkts aufgrund der Marktpräsenz in jedem Fall stets zu nennen sei und genannt werde.

187 Gröschner, a.a.O., (Fn. 184), 619 (627), die Aufklärung sei „*grundrechtsneutral*“.

Gegen einen Eingriff in Art. 14 Abs. 1 GG spricht die Qualität des Browsers als Zugabe bzw. bei bestimmten Versionen von alternativen Browsern als Freeware. Der Browser ist nicht der eigentliche Vertriebsgegenstand (dieses ist regelmäßig das Betriebssystem), sondern nur eine (kostenlose bzw. im Preis inbegriffene) Zugabe. Damit kann ein Eingriff in eine Kaufentscheidung und damit in die Wirtschafts- und Unternehmergrundrechte – namentlich Art. 14 Abs. 1 GG – verneint werden, zumal die Browser anderer Hersteller auch mit dem Betriebssystem funktionieren.

Darüber hinaus kann die staatliche Information in das Recht des Unternehmens auf Selbstdarstellung aus Art. 2 Abs. 1 GG eingreifen. Durch Art. 2 Abs. 1 GG wird das Verhalten im Wettbewerb geschützt (Wettbewerbsfreiheit). Dieses Verhalten umfasst auch die Entscheidung des Unternehmens, wie es sich präsentieren will.[188] Diese ist auch dann tangiert, wenn die Äußerungen sich bloß auf produkttypische Teile beziehen.[189] Da der Hersteller selbst in Abständen auf die Sicherheitslücken hinweist und einen regelmäßigen Patchday zur Schließung von Lücken angekündigt hat, können die Äußerungen in die unternehmerische Entscheidung im Umgang mit den Sicherheitslücken eingreifen.

Neben den Grundrechten des Herstellers kann auch an eine Beeinträchtigung der Grundrechte des Nutzers gedacht werden. Durch den Stempel der staatlichen Autorität können die Verbraucherinformation in die allgemeine Handlungsfreiheit des Nutzers aus Art. 2 Abs. 1 GG eingreifen, der Warnung entsprechend handeln zu müssen (faktischer Zwang).[190] Diese Überlegungen gelten nur unter der Prämisse, dass dem Bürger die Warnungen „aufgedrängt" werden, sucht er in Eigeninitiative etwa spezielle Webseiten auf, so gelten diese Überlegungen nicht.[191] Mit dem BVerfG kann zusätzlich argumentiert werden, dass ja nicht das Verhalten der Nut-

---

188 Philipp, Staatliche Verbraucherinformationen, 1989, S. 155 f.: Dies sei nicht nur die Freiheit sich bestimmte Verhaltensweisen nicht vorschreiben zu lassen, es umfasse auch die Freiheit, in der Selbstdarstellung gegenüber Verbraucher und Wettbewerber nicht gestört zu werden.

189 A. A. Philipp, a.a.O., (Fn. 188), S. 156 f.: Dies gelte nur, wenn das konkrete Produkt betroffen sei. Vgl. VG Köln, Beschluss v. 11.03.1999 – 20 L 3737/98, CR 1999, 557 (558), bei dem Gegenstand ein individuelles Produkt (Datenbank) des Herstellers war.

190 Zur Problematik der Uferlosigkeit bei Annahme jeder mittelbaren, faktischen Beeinträchtigung in Art. 2 Abs. 1 GG als Eingriff, *Dreier*, in: Dreier (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 2. Aufl. 2004, Art. 2 I Rd. 51, der die Forderung nach besonderen qualifizierenden Kriterien unterstützt, allerdings anmerkt, dass solche allgemeinen Maßstäbe noch nicht gefunden seien.

191 Vgl. auch Mandelartz/Grotelüschen, Das Internet und die Öffentlichkeitsarbeit der Regierung, in: NVwZ 2004, 647 (650).

zer gelenkt werden, sondern die Steuerungsfähigkeit des Marktes hergestellt werden soll.[192]

Festzuhalten ist: Abhängig vom Verständnis der Reichweite des Art. 2 Abs. 1 GG und des faktischen Eingriffs wird hier eine Warnung, einen bestimmten Browser zu nutzen als rufschädigend qualifiziert und stellt damit mit dem BVerwG grundsätzlich einen Eingriff dar.[193] Ein Eingriff in Art. 14 Abs. 1 GG ist aber abzulehnen, da primäres Ziel die Realisierung von Wissen beim Nutzer ist, zumal der Einfluss auf die Kaufentscheidung (wettbewerbsrechtliches Verhalten der Verbraucher) aufgrund der „Zugabequalität" des Browsers in Frage gestellt werden kann. Allein die Information bezüglich Java-Script ist eine Aufklärung hinsichtlich eines Teiles eines Produkttypen und demnach nicht grundrechtsrelevant.

Soweit ein Eingriff bejaht wird, ist zu prüfen, ob die Informationstätigkeit gerechtfertigt ist.

c) Rechtfertigung des Grundrechtseingriffs im Szenario 1

Fraglich ist, ob der angenommene Eingriff gerechtfertigt ist. Hier ist eine Interessenabwägung im Sinne einer Verhältnismäßigkeitsprüfung vorzunehmen.

Obwohl beständig Sicherheitslücken des Browsers veröffentlicht werden, erhält die Information über diese durch den Stempel der staatlichen Autorität eine neue Qualität. Soweit sogar alternative Browser genannt werden, könnte eine zusätzliche Beschwer vorliegen.

Allerdings dienen die Äußerungen dazu, steuernd die Sicherheit in der Informationstechnik zu erhöhen und haben damit als Förderung einer kritischen Infrastruktur einen hohen Wert für die Gesellschaft.[194]

Dem steht gegenüber, dass die sicherheitsfördernde Wirkung angesichts der technischen Versiertheit und Programmierfreude einiger Nutzer stets fraglich sein kann. Die Schadensdynamik, die die Veröffentlichung der Sicherheitslücken im Fall Sasser hatte, ist nur ein prominentes Beispiel. Unter dem Aspekt der „sicheren

---

192 Vgl. BVerfG „Glykol", Beschluss v. 26.06.2002 - 1 BvR 558/91, NJW 2002, 2621 (2622).

193 Teilweise a. A. BVerfG: Mit dem BVerfG liegt kein Eingriff durch die Information der Bundesregierung vor, da unterstellt werden kann, dass eine (verfassungsrechtliche) Aufgabenzuweisung vorliegt und die Zuständigkeitsordnung und Anforderungen an die Richtigkeit und Sachlichkeit von Informationen nicht missachtet wurde, BVerfG „Glykol", Beschluss v. 26.06.2002 - 1 BvR 558/91, NJW 2002, 2621 (2622).

194 Vgl. Kapitel 2 B. II. 1. d).

Unsicherheit“[195] ist allerdings auch die Geheimhaltung kein zuverlässiger Garant, dass die Sicherheitslücke nicht Gegenstand vielfältiger Nutzungsinteressen werden kann. Letztendlich entscheidet über diese Fragen die Qualität der Sicherheitslücke im Einzelfall. Kriterien sind wohl die Verbreitung und die grundsätzliche Fehlerneigung sowie das Alter, respektive die Fortentwicklung neuer Versionen der Software.

Letztendlich wird eigenverantwortliches Handeln des Nutzers (Deinstallation, Modifikation in den Einstellungen oder Missachtung der Information) erst durch die Warnung ermöglicht und gefördert. Da die Wahrnehmung von Eigenverantwortung als allgemeine Handlungsfreiheit des Nutzers ebenfalls grundrechtlichen Schutz genießt,[196] ist die Veröffentlichung der Information regelmäßig vorzuziehen. Dies kann jedoch nur gelten, wenn nicht konkret ersichtlich ist, dass durch die Ermöglichung der Ausnutzung der Lücke wiederum Rechtsgüter Dritter gefährdet werden. Dies kann jedoch nur im Einzelfall und hier nicht abschließend bewertet werden.

Schlussendlich ist ersichtlich, dass die Informationen etwa durch die Art der Veröffentlichung gegen den Grundsatz der Verhältnismäßigkeit verstoßen. Selbst bei einer konzertierten und abgesprochen Aktion aller staatlicher und administrativer Warnungen, erhielten diese keine nennenswerte zusätzliche Beschwer, da der Hersteller selbst mit regelmäßigen Veröffentlichungen von Sicherheitslücken die Fehlerneigung seiner Produkte eingesteht.

Festzuhalten ist, dass der Eingriff in Art. 2 Abs. 1 GG des Herstellers durch die Warnung vor dem Browser gerechtfertigt ist.

4. Zusammenfassung

Bei staatlichen Informationen über Sicherheitslücken ist regelmäßig zu prüfen, ob ein Grundrechtseingriff in die Wirtschafts- und Unternehmergrundechte der Hersteller vorliegt. Soweit ein solcher zu bejahen ist, bedarf es zumindest bei der administrativen Informationstätigkeit einer Ermächtigungsgrundlage. Demnach kann das „polyphone Konzert“[197] mit Beteiligung der Verwaltung im Bereich der Infor-

---

195 Vgl. Kapitel 3 B.

196 Zu der Bedeutung des Art. 2 Abs. 1 für die Privatautonomie, *Dreier*, in: Dreier (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 2. Aufl. 2004, Art. 2 I Rd. 63.

197 S. o. Kapitel 5 B IV. 1. b).

mationstätigkeit über Sicherheitslücken nur erklingen, soweit eine konkrete Befugnisnorm und folglich eine eindeutige Zuweisung durch den Gesetzgeber vorliegt.

Für das Szenario 1 bleibt festzuhalten, dass parallele staatliche und administrative Kompetenzen für die Warnung vor dem Browser und die Aufklärung über JavaScript bestehen. Hinsichtlich der Ermächtigungsgrundlage gilt, dass bei der Bundesregierung von der Aufgabe auf die Befugnis geschlossen werden kann, der Landesdatenschutzbeauftragte mit § 39 Abs. 4 S. 2 DSG-SH eine besitzt und das BSI für die Warnung vor dem Browser seine Beratungsbefugnis aus § 3 Abs. 1 Nr. 7 BSIG überschreitet.

Darüber hinaus kann festgehalten werden, dass die Information bezüglich JavaScript eine Aufklärung ohne Grundrechtsrelevanz ist; die Warnung vor dem Browser zwar in Art. 2 Abs. 1 GG des Herstellers eingreift, allerdings gerechtfertigt ist.

V. Informationsrechte im Arbeitsverhältnis

1. Recht des Arbeitgebers sich zu informieren – Überwachung der Internetnutzung der Mitarbeiter

Die Nutzung des Internets am Arbeitsplatz – unabhängig ob zu dienstlichen oder privaten Zwecken – stellt eine potenzielle Gefahr für die Sicherheit des Unternehmensnetzwerkes aufgrund des Gefahrenpotenzials der Nutzung an sich und des „Faktors Mensch“ dar.

> *„Bedeutendster Gefahrenbereich bleibt "Irrtum und Nachlässigkeit eigener Mitarbeiter".*[198]

Im Folgenden soll betrachtet werden, inwieweit sich der Arbeitgeber über die Sicherheitslücke Mensch informieren darf.

Die Entscheidung über das „Ob“ und den Umfang der Nutzung des Internets am Arbeitsplatz trägt der Arbeitgeber als Eigentümer der Betriebsmittel.[199] Soweit der IT-Sicherheit im Rahmen des § 91 Abs. 2 AktG durch den Arbeitgeber Aufmerksamkeit geschenkt werden muss, könnte die Entscheidung über das „Ob“ der Überwachung der Internetnutzung am Arbeitsplatz damit normativ bereits getroffen sein.

---

198 Vgl. KES und Microsoft Sicherheitsstudie von 2004, S. 3, http://www.kes.info/archiv/-material/studie2004/kes-Microsoft-Studie2004-Sonderdruck.pdf (30.05.2006).

199 Däubler, Internet und Arbeitsrecht, 2004, Rd. 180; Dickmann, Inhaltliche Ausgestaltung von Regelungen zur privaten Internetnutzung, in: NZA 2003, 1009 (1010).

Soweit eine private Nutzung ausdrücklich – im Arbeitsvertrag, durch Betriebsvereinbarung insbesondere durch eine Internet-Policy – oder konkludent gestattet ist,[200] ist der Arbeitnehmer grundsätzlich gehalten, mit dieser in arbeitsverträglicher und verantwortungsvoller Weise umzugehen. Diese kann quantitativ an den Zeiten, an den aufgesuchten Seiten und an eventuell anfallenden Kosten gemessen werden.

Soweit eine Nutzung gestattet ist, ist der Arbeitgeber regelmäßig ein Dienstanbieter im Sinne des § 3 Nr. 6 lit. a) TKG, der zur Wahrung des Fernmeldegeheimnisses verpflichtet ist, § 88 Abs. 2 S. 1 TKG.[201] Dies unabhängig davon, ob er die Nutzung des Arbeitnehmers entgeltlich oder unentgeltlich erlaubt, da ein „geschäftsmäßiges Erbringen" im Sinn des TKG nur ein nachhaltiges Angebot und ausdrücklich keine zwingende Gewinnerzielungsabsicht voraussetzt, § 3 Nr. 10 TKG.

Die Kontrolle der Mitarbeiter – auch zu Zwecken der IT-Sicherheit – ist am strengeren Maßstab des Fernmeldegeheimnisses, der die Gestattung der privaten Nutzung mit sich bringt, zu messen. Das Fernmeldegeheimnis umfasst den Inhalt und die näheren Umstände der Telekommunikation, § 88 Abs. 1 S. 1 TKG. Die Umstände umfassen etwa die am Telekommunikationsvorgang beteiligten Personen und die Verkehrsdaten im Sinn des § 3 Nr. 30 TKG,[202] d. h. IP-Adresse, Internetdienst (Portnummer) und die Zuordnung zu einem Rechner/einer Person. Dies sind Daten, die für die Evaluierung der Sicherheit eines Systems erforderlich sind.

Regelmäßig wird bei der systematischen und ständigen Kontrolle durch technische Einrichtungen daher ein Eingriff in das Persönlichkeitsrecht des Arbeitnehmers nach Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG bejaht. Allerdings dürfen sich die Dienstanbieter Kenntnisse über die „Umstände der Telekommunikation" verschaffen, die der Schutz ihrer technischen Systeme erfordert, § 88 Abs. 3 S. 1 TKG.

Fraglich ist demnach, ob die Überwachung durch § 88 Abs. 3 S. 1 TKG gerechtfertigt ist und damit die präventive und ständige Kontrolle des Surfverhaltens der Arbeitnehmer gestattet ist. Ohne die Möglichkeit der Auseinandersetzung mit einem – noch nicht existierenden – § 88 Abs. 3 S. 1 TKG wurde regelmäßig eine Routinekontrolle des Surfverhaltens ohne erhebliche Verdachtsgründe für nicht verein-

---

200 Ernst, Der Arbeitgeber, die E-Mail und das Internet, in: NZA 2002, 585 (585).

201 Vgl. die Gesetzesbegründung zu § 85 TKG a. F.: Entwurf eines Telekommunikationsgesetzes vom 30.01.1996, BT-Drs. 13/3609, S. 53; in der Literatur etwa: Ernst, a.a.O., (Fn. 200), 585 (587). Ein Verstoß gegen das Fernmeldegeheimnis ist über § 206 StGB strafbewehrt.

202 Manssen-*Haß M.,* TKG § 85 Rd. 13, der noch Verbindungsdaten nach § 5 TDSV a. F. erwähnt, die durch die TKG-Novelle 2004 durch Verkehrsdaten ersetzt wurden.

bar mit dem Arbeitnehmerpersönlichkeitsrecht angesehen.[203] Andererseits wird festgestellt, dass es aus Gründen der Sicherheit unerlässlich sei, Zugriffe auf das Netz und den Aus- und Eingang von E-Mails zu protokollieren.[204] Die Einschränkung des Fernmeldegeheimnisses zum „Schutz der technischen Systeme" ist erst durch die Novelle des TKG im Jahr 2004 eingefügt worden.[205] In Ermangelung der Darlegung der Motivation in der Gesetzesbegründung,[206] kann nur auf die bisherigen Maßstäbe des § 85 Abs. 3 S. 1 TKG a. F. zurückgegriffen werden. Bis dato war eine Einschränkung lediglich in dem für die geschäftsmäßige Erbringung erforderlichen Maß erlaubt. Allerdings erfolgte in der Novelle nur eine deklaratorische Anpassung an das bisherige Verständnis in der Literatur: Die geschäftsmäßige Erbringung ist das nachhaltige Angebot von Telekommunikationsdiensten. Eine Überwachung der Verkehrsdaten kann etwa für den Zweck der Abrechnung dieses Angebotes oder aber auch zur Sicherstellung eines *„technisch einwandfreien Betriebsablaufs"*[207] erforderlich sein.[208] Die Grenze der zulässigen Überwachung ist der Inhalt der Kommunikation, dessen Kenntnis regelmäßig weder für die geschäftsmäßige Erbringung noch zum Schutz des technischen Systems erforderlich ist.[209]

Durch das Merkmal der Erforderlichkeit ist eine restriktive Auslegung geboten, d. h. Maßnahmen der Überwachung, auch zur Gewährleistung der IT-Sicherheit, sind nur zulässig, wenn kein anderes Mittel in Betracht kommt.[210] Dies ist eine technische Frage, die keine wirtschaftlichen Maßstäbe duldet.[211] Welche Maßnahmen in

---

203 Ernst, a.a.O., (Fn. 200), 585 (590). Mit Hinweis auf § 88 Abs. 3 (respektive § 85 Abs. 3 a. F.) TKG: Weißnicht, Die Nutzung des Internet am Arbeitsplatz, in: MMR 2003, 448 (449); Naujock, Internet-Richtlinien, in: DuD 2002, 592 (593).

204 Weißnicht, a.a.O., (Fn. 203), 448 (449).

205 Gesetzesentwurf zum Telekommunikationsgesetz vom 17.10.2003, BR-Drs. 755/03.

206 Vgl. die Gesetzesbegründung zur TKG-Novelle im Gesetzesentwurf vom 17.10.2003, BR-Drs. 755/03, S. 119, dort heißt es lapidar: *„Die Vorschriften zum Fernmeldegeheimnis werden unverändert übernommen."*

207 Manssen-*Haß M.,* TKG § 85 Rd. 17.

208 Manssen-*Haß M.,* TKG § 85 Rd. 17; Trute/Spoerr/Bosch-*Trute*, TKG § 85 Rd. 18 (inklusive Missbrauchsverhinderung und –abwehr).

209 Bisweilen unklar bleibt die Abgrenzung der Sicherstellung eines geregelten Ablaufs der Kommunikation zur Überwachung der Arbeitnehmer, die dem grundsätzlichen Verbot unterfällt, sich Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. So auch in einem aktuellen Kommentar zum TKG, der zwischen beiden Verhaltensweisen keine Grenze zu ziehen vermag, BerlKommTKG/*Klesczewski,* § 88 Rd. 23 ff.

210 Manssen-*Haß M.,* TKG § 85 Rd. 17.

211 Soweit ein Eingriff in den Telekommunikationsvorgang und damit in das Fernmeldegeheimnis zwar die kostengünstige Alternative etwa zur Beseitigung von technischen Störungen sei, aber andere Mittel, etwa eine Schulung der Mitarbeiter, zur Auswahl stünden, sei letztere zu wählen. Die technische Lösung wäre dann nicht erforderlich im Sinne des Geset-

Betracht kommen, ist eine Frage des konkreten Aspektes der Sicherheitslücke Mensch. In Betracht kommen proaktive Restriktionen, wie etwa eine Beschränkung auf die notwenigen Programme, Schulungen, Informationen über aktuelle technische Sicherheitslücken in der Software, etc.

Darüber hinaus verlangen auch gerade das Fernmeldegeheimnis und der Schutz des Systems vor unerlaubten Zugriffen *„angemessene technische Vorkehrungen"*[212], § 109 Abs. 1 TKG.[213] Nicht zuletzt kann dem Arbeitgeber ein Organisationsverschulden vorgeworfen werden, wenn er es versäumt, rechtswidrige Handlungen seiner Mitarbeiter durch eine angemessene Organisation zu verhindern.[214]

Die Überwachung wäre demnach in den Grenzen des § 88 Abs. 3 S. 1 TKG zulässig und nach § 109 Abs. 1 TKG sogar erforderlich, soweit sie als „angemessene technische Vorkehrung" bezeichnet werden kann.[215] Der Kommentierung zu § 87

---

zes, so Manssen-*Haß M.,* TKG § 85 Rd. 18; a. A.: Trute/Spoerr/Bosch-*Trute*, TKG § 87 Rd. 18 mit dem Hinweis auf den ebenfalls grundrechtlichen Schutz der Erbringung von Telekommunikationsdiensten.

212 Technische Vorkehrungen sind nach § 109 Abs. 2 S. 4 TKG angemessen, *„wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtung für die Allgemeinheit steht."* Im Falle der Protokollierung ist der Aufwand gering (etwa anderes könnte für die Auswertung gelten). Dieser ist mit dem Recht des Arbeitnehmers auf effektive Geschäftsführung und das Rechts sich, sein Eigentum und andere vor Gefahren zu schützen in Verhältnis zu stellen, vgl. Artikel 29 Datenschutzgruppe, Arbeitsdokument zur Überwachung der elektronischen Kommunikation von Beschäftigten vom 29.05.2002, S. 4, http://www.europa.eu.int/-comm/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_de.pdf (30.05.2006).

213 Die weiteren Schutzziele in § 87 Abs. 1 TKG a. F. sind nach § 109 Abs. 2 TKG nur bei Telekommunikationsdiensten für die Öffentlichkeit zu gewährleisten. Eine Konkretisierung der Maßnahmen aufgrund der gesetzlichen Schutzziele erfolgte in einem von der Regulierungsbehörde nach § 87 Abs. 1 S. 3 TKG a. F. erlassenen Katalog von Sicherheitsanforderungen mit Empfehlungscharakter. Vgl. BMPT, Katalog von Sicherheitsanforderungen, 1997, Banz. Nr. 208a vom 07.11.1997, abgedruckt bei Scheuerle/Mayen-*Zerres,* TKG Kommentar Anh zu § 87 (das Bundesministerium für Post und Telekommunikation (BMTP) nahm bis zum 31.12.1997 die Aufgaben der Regulierungsbehörde war). Der Schutz vor unerlaubten Zugriffen nach § 109 Abs. 1 Nr. 2 TKG umfasst interne und externe Gefährdungen, denen etwa mit Zugriffrechten, Authentisierungsverfahren, Firewalls und Protokollierungen begegnet werden können, vgl. Trute/Spoerr/Bosch-*Trute*, TKG § 87 Rd. 11 mit Hinweis auf BMPT, Katalog von Sicherheitsanforderungen, 1997, Anlage 2.

214 Hilber/Frik, Rechtliche Aspekte der Nutzung von Netzwerken, in: RdA 2002, 89 (90). Rechtswidrige Handlungen können etwa in Verletzung von Urheberrechten oder im Download von kinderpornografischen Inhalten bestehen.

215 So auch Hilber/Frik, a.a.O., (Fn. 214), 89 (94). § 109 Abs. 1 TKG ist in diesem Sinne auch eine Spezialvorschrift, die § 9 BDSG präzisiert und teilweise erweitert, aber nicht verdrängt, vgl. Scheuerle/Mayen-*Zerres,* TKG Kommentar § 87 Rd. 4.

Abs. 1 TKG a. F.[216] ist zu entnehmen, dass technische Maßnahmen alle Maßnahmen sind, die sich auf die Funktionsweise der Anlage beziehen. Sonstige Maßnahmen i.S.d. § 87 Abs. 1 TKG a. F. sind organisatorischer Natur.[217] Überwachungsmaßnahmen sind organisatorische Maßnahmen, die durch den Einsatz der Technik realisiert werden. Eine organisatorische Vorkehrung zum Schutz des § 109 Abs. 1 Nr. 2 TKG ist etwa die Protokollierung von Daten.[218] Inwieweit solche Maßnahmen erforderlich und zulässig sind, ist eine Frage der Verhältnismäßigkeit. Soweit § 109 Abs. 2 S. 4 TKG von angemessenen Vorkehrungen spricht, ist die Angemessenheit des technischen und wirtschaftlichen Aufwands in Relation zur Bedeutung der Anlage für die zu schützenden Rechte und die Infrastruktur zu setzen. Da Überwachungsmaßnahmen nur im Rahmen ihrer Erforderlichkeit nach dem Gesetz auch zulässig sein können, sind Überwachungsmaßnahmen in Abhängigkeit der Infrastrukturbedeutung für das Unternehmen einzusetzen. Gleiches gilt auch für die Art der Überwachungsmaßnahme.

Soweit eine private Nutzung nicht gestattet ist, gilt die Grenze einer Überwachung nach § 88 Abs. 2 S. 1 TKG nicht, da keine Telekommunikationsleistungen an Dritte erbracht werden, § 88 Abs. 2 S. 1 i.V.m. § 3 Nr. 6 lit. a) und 10 TKG.

Allerdings ist – unabhängig von (gestatteter) privater oder dienstlicher Nutzung – eine Überwachung und Kontrolle am (subsidiären) Bundesdatenschutzrecht zu messen. In der Regel liegt eine Erhebung personenbezogener Daten vor, §§ 3 Abs. 3 BDSG. Für diese gelten die §§ 13 und 28 BDSG.[219] Die Überwachung ist dann stets in den Grenzen der §§ 13 Abs. 1 und 28 Abs.1 Nr. 2 BDSG „zur Erfüllung der Aufgaben“ und zur „Wahrung berechtigter Interessen“ zulässig. Diese Begriffe lassen sich mit den ausgeführten Überlegungen füllen. Deshalb wird vertreten, dass das Loggen des Surfverhaltens des Mitarbeiters gegen die informationelle Selbstbe-

---

216 Dieser weicht von seinem Nachfolger, § 109 Abs. 1 TKG, insoweit ab, als er weitergehend neben dem Schutz des Fernmeldegeheimnisses und des Datenschutzes in Nr. 1 und den Schutz vor unerlaubten Zugriffen in Nr. 2 darüber hinaus vor Störungen, die zur Beeinträchtigung des Netzes (Nr. 3) führen können, und das System gegen äußere Angriffe und Katastrophen (Nr. 4) geschützt wissen will. Die letzten Schutzziele sind im § 109 Abs. 2 TKG nur den Betreibern aufgegeben, die Dienste für die Öffentlichkeit anbieten.

217 Scheuerle/Mayen-*Zerres,* TKG Kommentar § 87 Rd. 16.

218 BMPT, Katalog von Sicherheitsanforderungen, 1997, Anlage 2, abgedruckt bei Scheuerle/Mayen-*Zerres,* TKG Kommentar Anh zu § 87.

219 § 13 gilt grundsätzlich für öffentliche Stellen des Bundes (soweit öffentliche Stellen der Länder ihre Mitarbeiter überwachen sind die entsprechenden Landesdatenschutzgesetze zu beachten), § 28 für nicht öffentliche Stellen.

stimmung des Mitarbeiters verstoße und daher nur mit Einwilligung oder bei Vorliegen ernsthafter Sicherheits- oder Verdachtsgründe zulässig sei.[220]

Darüber hinaus sind Kontrolleinrichtungen jedweder Art mitbestimmungspflichtig, dies ergibt sich aus der Fürsorgepflicht des Arbeitgebers. Soweit vorhanden ist der Betriebsrat einzuschalten, § 87 Abs. 1 Nr. 6 BetrVG (entsprechend im öffentlichen Dienst der Personalrat nach § 75 Abs. 3 Nr. 17 BPersVG). An die technische Einrichtung sind keine besonderen Anforderungen zu stellen,[221] auch Programme sollen als digitale technische „Einrichtung" die Mitbestimmungspflicht auslösen. Hierbei soll die objektive Eignung ausreichen, auf einen zielgerichteten oder tatsächlichen Einsatz zur Überwachung komme es nicht an.[222] Die Mitbestimmung soll bereits dann ausgelöst werden, wenn eine Verhaltens- oder Leistungskontrolle auch nur in Verknüpfung mit anderen Daten möglich werde.[223] Demnach ist etwa auch das Führen von Firewall-Protokollen mitbestimmungspflichtig. Eine Mitbestimmung könnte allerdings durch eine Anonymisierung der Daten ausgeschlossen werden, § 3 Abs. 6 BDSG.[224] Ob anonymisierte Protokolle einen Beitrag zur IT-Sicherheit leisten können, bleibt der Einschätzung der Technik, respektive der des Administrators, überlassen.

Festzuhalten ist, der Arbeitgeber kann sich im gesetzlichen Rahmen begrenzt über Gefahren für die IT-Sicherheit, respektive die Einhaltung von IT-Sicherheitsmaßnahmen und damit über menschliche IT-Sicherheitslücken informieren. Eine Grenze findet sich in der durch § 88 Abs. 3 S. 1 TKG gebotenen Erforderlichkeit. Ob dieser gesetzliche Rahmen gerade im Hinblick auf kollidierende Überwachungspflichten aus § 91 Abs. 2 AktG ausreicht, bleibt abzuwarten. Zumindest auf europäischer Ebene gibt es Bestrebungen, den Arbeitgeber in seinen Informationsrechten zu beschränken.[225]

---

220 Bier, Internet und E-Mail am Arbeitsplatz, in: DuD 2004, 277 (279 f.).

221 Fitting/Kaiser/Heither/Engels, BetrVG, § 87 Rd. 219.

222 Fitting/Kaiser/Heither/Engels, BetrVG, § 87 Rd. 230.

223 Fitting/Kaiser/Heither/Engels, BetrVG, § 87 Rd. 230. Darüber hinaus findet sich ein Hinweis auf technische Schutzmaßnahmen nach § 9 BDSG in a.a.O., Rd. 239; a.E.; Hanau/Hoeren, Private Internetnutzung durch den Arbeitnehmer, 2003, S. 81.

224 Hanau/Hoeren, Private Internetnutzung durch den Arbeitnehmer, 2003, S. 90, mit dem Hinweis, dass die Einrichtung, das Programm, ausschließlich mit anonymisierten Daten arbeiten müsse und unter keinen Umständen ein Rückschluss zu personenbezogenen Daten möglich sein dürfe.

225 Zu den Überlegungen auf EU-Ebene im Überblick, Barton, Risiko-Management und IT-Sicherheit, in: K&R 2004, 305 (310 ff.).

2. Recht des Arbeitnehmers zu informieren kontra Geheimhaltungspflicht und arbeitsvertragliche Loyalität – Szenario 2

Ein Informationsrecht der (IT-)Mitarbeiter eines Unternehmens ist hier von Interesse, da diese grundsätzlich als Insider einen Einblick in die Sicherheitslücken und Schwachstellen des IT-Systems haben.[226] Der Staat könnte einen Beitrag dieser zur IT-Sicherheit de lege ferenda unterstützen, indem gesetzliche Regelungen die Folgen (Kündigung) möglicher arbeitsrechtlicher Illoyalität beseitigen (Kündigungsschutz). Entsprechende gesetzliche Maßnahmen wurden etwa bei der Gefahrenstoffverordnung (GefStoffVO) und im ArbSchG getroffen. Nach § 21 Abs. 6 der GefStoffVO darf eine Anzeige des Arbeitnehmers bei der Überwachungsbehörde nach Ausschöpfung der innerbetrieblichen Möglichkeiten nicht zu seinem Nachteil gereichen.[227] In § 17 Abs. 2 ArbSchG wurde die Rechtsposition des Arbeitnehmers sogar verstärkt. Eine Ausschöpfung aller innerbetrieblichen Beschwerdemöglichkeiten bedarf es nicht. Einer vergleichbaren Vorschrift für die IT-Sicherheit steht die mit der Regelung verbundene Privilegierung des Arbeitnehmers entgegen. Soweit dessen Sicherheit und der Schutz seiner Gesundheit am Arbeitsplatz nicht gewährleistet werden, tangiert dies primär seine Interessen. Die Durchsetzung dieser Interessen rechtfertigt eine Privilegierung. Soweit Sicherheitslücken und Schwachstellen des IT-Systems gefunden werden, sind dagegen widerstreitende Interessen Dritter betroffen. Fraglich ist, ob diese Privilegierung zur Durchsetzung von Interessen Dritter, die von der Offenbarung der Sicherheitslücke profitieren, sich über die arbeitsrechtliche Treupflicht hinweg setzen kann.

Inwieweit ein Recht des Arbeitnehmers besteht, den Staat oder die Öffentlichkeit zu informieren, ist folglich den allgemeinen (arbeitsrechtlichen) Bestimmungen zu entnehmen.

Neben den ausführlich zu diskutierenden (individual)arbeitsrechtlichen Bestimmungen können sich Geheimhaltungspflichten aus § 79 Abs. 1 S. 1 BetrVG (Per-

---

226 Zu dem arbeitsrechtlichen Konflikt zwischen Information über Sicherheitslücken und den Interessen des Arbeitgebers und Herstellers in einem Fall aus der Praxis, http://-www.heise.de/newsticker/meldung/65789 (30.05.2006).

227 § 21 Abs. 6 GefStoffVO: *„Wird die maximale Arbeitsplatzkonzentration oder die Technische Richtkonzentration oder der Biologische Arbeitsplatztoleranzwert nicht unterschritten und hilft der Arbeitgeber der dagegen erhobenen oder veranlassten Beschwerde nicht unverzüglich ab, so kann sich der einzelne Arbeitnehmer nach Ausschöpfung der innerbetrieblichen Möglichkeiten unmittelbar an die für die Überwachung zuständigen Stellen wenden. Besteht durch die Überschreitungen nach Satz 1 eine unmittelbare Gefahr für Leben oder Gesundheit, hat der einzelne Arbeitnehmer das Recht, die Arbeit zu verweigern. Aus der Ausübung der in den Sätzen 1 und 2 genannten Rechten dürfen dem Arbeitnehmer keine Nachteile entstehen."*

sonalrat, § 10 Abs.1 S. 1 BPersVG) ergeben. Für Betriebsratsmitglieder, die bestimmte sicherheitsrelevante Prozesse im Betrieb genehmigen müssen, und damit kennen, ergeben sich hieraus Geheimhaltungspflichten für Betriebs- und Geschäftsgeheimnisse, die sich zeitlich auf die Zeit nach Zugehörigkeit zum Betriebsrat ausdehnen. Zivilrechtlich können §§ 823, 824, 826 BGB das Recht der Arbeitnehmer zu informieren begrenzen (siehe oben). Soweit Arbeitnehmer Betriebs- und Geschäftsgeheimnisse unbefugt offenbaren, können sie nach § 203 Abs. 1 Nr. 6 StGB und § 17 Abs. 1 UWG strafrechtlich zur Verantwortung gezogen werden, dies gilt auch für ehemalige Arbeitnehmer.[228]

Fraglich ist jedoch, wie die bereits oben erwähnte Abwägung der arbeitsrechtlichen Treuepflicht mit dem Schutz des Einzelnen bei IT-Sicherheitslücken zu lösen ist, wenn Mitarbeiter über Sicherheitslücken und Schwachstellen des IT-Systems des Unternehmens informieren wollen. Unter dem Stichwort des „whistleblowing" soll im Folgenden der Meinungstand zu den Informationsrechten des Arbeitnehmers über Missstände (Sicherheitslücken) im Betrieb dargelegt werden, bevor dieser auf das Szenario 2 übertragen wird. Zunächst soll jedoch in einer grundsätzlichen Einschätzung dargelegt werden, ob IT-Sicherheitslücken als Betriebs- und Geschäftsgeheimnis der Geheimhaltung unterliegen.

a) Geheimhaltung von Sicherheitslücken als Betriebs- und Geschäftsgeheimnis

Soweit Betriebs- und Geschäftsgeheimnisse etwa verfassungsrechtlich geschützt sein können,[229] ist dies relevant für die Bestimmung von Informationsrechten, da eine Feststellung der verfassungsrechtlichen Grenzen Maßstab für die Bestimmung von Informationsrechte und -pflichten der Anbieter und Hersteller sein könnte.[230]

---

228 Vgl. BGH, Urteil v. 15.06.1993 - 9 AZR 558/91, NZA 1994, 502 (505).

229 In einer jungen Entscheidung will das BVerfG den verfassungsrechtlichen Schutz aus Art. 12 und 14 GG abhängig von der Qualität des Betriebs- und Geschäftsgeheimnisses im Einzelfall bewerten, BVerfG, Entscheidung v. 05.02.2004 - 1 BvR 2087/03, http://www.bverfg.de/entscheidungen/rk20040205_1bvr208703.html (30.05.2006). Regelmäßig sollen Betriebs- und Geschäftsgeheimnisse jedoch dem Schutz aus Art. 12 und 14 GG unterfallen, BVerwG, Beschluss v. 15.08.2003 – 20 F 8/03, http://www.bundesverwaltungsgericht.de/ (30.05.2006). Gegen einen Schutz nach Art. 14 GG: Wolff, Der verfassungsrechtliche Schutz der Betriebs- und Geschäftsgeheimnisse, in: NJW 1997, 98 (100 f.), der bei Betriebs- und Geschäftsgeheimnissen keine rechtliche Zuordnung zu einem Rechtsinhaber für erforderlich hält, da es auf eine tatsächliche Zuordnung und dem Schutz vor Offenbarung ankomme.

230 Diese Bedeutung will etwa Taeger zuschreiben, Taeger, Die Offenbarung von Betriebs- und Geschäftsgeheimnissen, 1988, S. 53.

Es erscheint daher sinnvoll zunächst zu klären, ob IT-Sicherheitslücken als Betriebs- und Geschäftsgeheimnisse qualifiziert werden können.

Der Begriff der Betriebs- und Geschäftsgeheimnisse ist nicht legal definiert. Betriebs- und Geschäftsgeheimnisse liegen gemeinhin vor, wenn

> *„(1) Tatsachen in Zusammenhang mit einem Geschäftsbetrieb, (2) nur einem eng begrenzten Personenkreis bekannt und (3) nicht offenkundig sind, (4) nach dem ausdrücklichen oder konkludent erklärten Willen des Betriebsinhabers (5) auf Grund eines berechtigten wirtschaftlichen Interesses geheimgehalten werden sollen.“*[231]

Im Folgenden soll anhand der Definition untersucht werden, ob IT-Sicherheitslücken grundsätzlich als Betriebs- und Geschäftsgeheimnis verstanden werden können.

(1) Eine Sicherheitslücke ist eine den Hersteller oder Anbieter betreffende Tatsache im Zusammenhang mit dem Geschäftsbetrieb.

(2) Es entspricht vermutlich der Realität, dass das eine Sicherheitslücke in einem Unternehmen, wenn überhaupt, nur einem eng begrenzten Personenkreis – etwa dem Administrator – bekannt ist. Die Kenntnis soll unter dem Punkt der Nichtoffenkundigkeit berücksichtigt werden.

(3) Eine Tatsache ist offenkundig, wenn sie der Öffentlichkeit bekannt ist oder ohne größere Schwierigkeiten in Erfahrung gebracht werden kann.[232] Die Offenkundigkeit setzt demnach nicht zwingend Kenntnis voraus, es genügt bereits die Möglichkeit der Kenntniserlangung.[233] Ob eine Sicherheitslücke offenkundig ist, hängt von der Verbreitung und Qualität der Lücke im Einzelfall ab. So könnte etwa die grundsätzliche Schwäche eines Servers, für DoS Angriffe missbraucht zu werden, offenkundig sein. Soweit zum Entdecken einer Sicherheitslücke in der Software regelmäßig zunächst der Quellcode zu prüfen ist, kann eine Offenkundigkeit verneint werden. Bei einer Sicherheitslücke durch den „menschlichen Faktor“, etwa

---

[231] Fezer/Rengier UWG § 17 Rd. 7, mit weiteren Hinweisen auf die Rechtsprechung (des BGH). In jüngster Zeit bestätigt durch BGH, Urteil v. 7.11.2002 - I ZR 64/00, GRUR 2003, 356 (358); Richters/Wodtke, Schutz von Betriebsgeheimnissen aus Unternehmersicht, in: NZA-RR 2003, 281 (281); Baumbach/Hefermehl-*Köhler* § 17 UWG Rd. 3. Die Differenzierung nach Betriebs- und Geschäftsgeheimnis kann aufgrund ihres übereinstimmenden rechtlichen Schutzes dahingestellt bleiben. Grundsätzlich werden Geschäftsgeheimnisse dem kaufmännischen und Betriebsgeheimnisse dem technischen Bereich zugeordnet und können als Wirtschafts- oder Unternehmensgeheimnis zusammengefasst werden, vgl. Fezer/Rengier UWG § 17 Rd. 8 f.; zustimmend, Breuer, Schutz von Betriebs- und Geschäftsgeheimnissen im Umweltrecht, in: NVwZ 1986, 171 (172).

[232] Richters/Wodtke, a.a.O., (Fn. 231), 281 (281); BGH, Urteil v. 17.12.1981 - X ZR 71/80, NJW 1982, 937 (937); Fezer/Rengier UWG § 17 Rd. 12.

[233] Fezer/Rengier UWG § 17 Rd. 13; Richters/Wodtke, a.a.O., (Fn. 231), 281 (282).

bei einer technisch ungenügenden Passwortauswahl, kann das Passwort so einfach sein, dass eine theoretische Möglichkeit der Kenntniserlangung gegeben ist. Eine Offenkundigkeit ist wohl trotzdem abzulehnen, da regelmäßig das Passwort erst mithilfe eines Programms „geknackt" wird.[234] Ist das Passwort „geknackt", hängt die Offenkundigkeit von den weiteren Umständen des Einzelfalls ab. Die Offenkundigkeit wurde etwa bei einem entschlüsselten Programm verneint, dessen illegales Auswertungsprogramm noch nicht weit verbreitet ist.[235]

(4) Soweit die Sicherheitslücke durch den Hersteller oder Anbieter nicht ausdrücklich offen gelegt wird, ist ein Geheimhaltungswille wohl regelmäßig zu unterstellen. Dies gilt jedenfalls, wenn die Offenbarung sich schädlich auf die Reputation (in einer bestimmten Branche) auswirken kann.

(5) Das berechtigte wirtschaftliche Interesse an der Geheimhaltung liegt vor, wenn die Offenbarung *„spürbare wirtschaftliche Auswirkungen auf die Wettbewerbsfähigkeit des Unternehmens"*[236] hat. Das berechtigte Interesse ist im Hinblick auf die strafrechtlichen Sanktionen des Geheimnisverrats objektiv zu beurteilen.[237] Ein wirtschaftliches Interesse an der Geheimhaltung der Sicherheitslücke ist regelmäßig anzunehmen, da sich die Offenlegung zumindest auf den Ruf des Unternehmens auswirkt. Das berechtigte Interesse könnte indes entfallen, wenn die Sicherheitslücke ein „illegales Geheimnis" ist. Als „illegales Geheimnis"[238] wird regelmäßig die Geheimhaltung von bewussten und unbewussten Gesetzesverstößen bezeichnet. Zunächst ist bereits strittig, ob grundsätzlich ein berechtigtes Interesse an der Geheimhaltung „il-

---

234 So stehen auch die Fälle von „Social Engineering" nicht einer Offenkundigkeit gleich. Mit „Social Engineering" wird die Methode bezeichnet, durch Kommunikation mit dem Passwortträger, von diesem das Passwort zu erlangen. So wird etwa gegenüber neuen Mitarbeitern die Identität eines IT-Mitarbeiters vorgegeben, um zu „Wartungszwecken" das Passwort zu erhalten.

235 BayObLG, Urteil v. 28.08.1990 - RReg 4 St 250/89, GRUR, 1991, 694 (696), in der Sache ging es um ein Programm zur Steuerung von Geldspielautomaten, das in einer Zeit von 70 Stunden und einem Einsatz von 5000 DM Spielgeld entschlüsselt werden konnte.

236 Richters/Wodtke, a.a.O., (Fn. 231), 281 (282); vgl. auch Baumbach/Hefermehl-*Köhler* § 17 UWG Rd. 9.

237 Richters/Wodtke, a.a.O., (Fn. 231), 281 (282); Breuer, Schutz von Betriebs- und Geschäftsgeheimnissen im Umweltrecht, in: NVwZ 1986, 171 (172 f.). Die Frage nach dem „berechtigten Interesse" impliziere eine Abwägung mit anderen Interessen. Bei Gesetzesverstößen verlangen etwa die Interessen an einem effektiven Rechtsschutz eine Offenlegung.

238 Rützel, Illegale Unternehmensgeheimnisse?, in: GRUR 1995, 557 ff. Als „illegale Unternehmensgeheimnisse" bezeichnet Rützel, die Geheimhaltung von bewussten und unbewussten Gesetzesverstößen in einem Unternehmen. Als Beispiel nennt Rüzel etwa Straftaten gegen die Umwelt, a.a.O., (557).

legaler Geheimnisse“ besteht.[239] Im Einzelfall ist des Weiteren zu prüfen, ob die Sicherheitslücke einen Gesetzesverstoß darstellt. Im Falle von ungeschützten (personenbezogenen) Kundendaten könnte etwa ein Verstoß gegen § 9 BDSG vorliegen. Dann entfällt in einer engen Auslegung das berechtigte Interesse und es liegt kein Betriebs- und Geschäftsgeheimnis vor. Soweit man eine weite Auslegung des berechtigten Interesses favorisiert,[240] bleibt die Bewertung dem Zivil- und Strafrecht überlassen.

(6) Im Ergebnis gilt: Grundsätzlich sind Schwachstellen in einem Unternehmen vor Offenbarung zu schützen.[241] Sicherheitslücken stellen grundsätzlich Betriebs- und Geschäftsgeheimnisse dar und sind damit regelmäßig vor Offenbarung geschützt. Ein Schutz besteht soweit gesetzliche und (nach)vertraglichen Schutzpflichten reichen. Fraglich ist jedoch, wie etwa die arbeitsvertragliche Treuepflicht zu bewerten ist, wenn die Sicherheitslücke ein „illegales Unternehmensgeheimnis“ und damit nicht – so hier vertreten – als ein Betriebs- und Geschäftsgeheimnis geschützt ist.

b) Rechtsprechung und Literatur zum „whistleblowing“

In der bisherigen Praxis der Rechtsprechung und in der Literatur wurde die arbeitsrechtliche Bedeutung der Informationen von Arbeitnehmer über strafbares, rechtswidriges oder aus sonstigen Gründen kritikwürdiges Verhalten des Arbeitgebers bisher – im Gegensatz zu der US-amerikanischen rechtlichen Auseinandersetzung mit dem „whistleblowing“ – nicht ausgiebig diskutiert.[242] Dem US-

---

239 Fezer/Rengier UWG § 17 Rd. 21 mit Darstellung des Meinungsstandes.

240 Für die Einbeziehung von „illegalen Geheimnissen“ etwa: Fezer/Rengier UWG § 17 Rd. 21; Baumbach/Hefermehl-*Köhler* § 17 UWG Rd. 9.

241 Generell die Schwachstellen des Unternehmens zu den Betriebs- und Geschäftsgeheimnissen zählend, Fezer/Rengier UWG § 17 Rd. 23.

242 Zum deutschen und US-amerikanischen Recht, Graser, Whistleblowing, 2000; vgl. auch die ausführliche Einleitung bei Müller, Whistleblowing, in: NZA 2002, 424 (424 f.), der die dünne Auseinandersetzung u.a. mit der gesellschaftlichen Rezeption solcher Informationen in Deutschland (Denunziant, Nestbeschmutzer) begründet. Müller weist aber auch auf erste Ansätze für eine Veränderung hin, etwa die Informationsseite für Arbeitnehmer http://www.whistleblower.de (30.05.2006) hin. Unterstützt von der EU will dieses Projekt entsprechend der rechtlichen Verpflichtung in den USA nach dem Sarbanes-Oxley Act ein System für anonyme Hinweise schaffen. Nach Sec. 310 (1) B und Sec. 806 des Sarbanes-Oxley Act müssen alle an einer US-Börse notierten Unternehmen ein Hinweissystem einrichten, um whistleblower zu schützen. Hintergrund ist, das Vertrauen in den Kapitalmarkt und dessen Unternehmen (wieder) zu stärken und wirtschaftskriminelle und sonstige schädigende Verhaltensweisen von Mitarbeitern in Unternehmen unterbinden zu können.

amerikanischen Modell entsprechend soll im Folgenden unter dem Stichwort des „whistleblowing" im Allgemeinen das Recht des Arbeitnehmers diskutiert werden, über Straftaten und Rechtsverstöße des Arbeitgebers zu informieren,[243] bevor die Bewertung des Szenarios 2 im Besonderen vorgenommen wird.

Wie oben bereits angedeutet, besteht eine nebenvertragliche Pflicht des Arbeitnehmers auf die geschäftlichen Interessen seines Arbeitgebers Rücksicht zu nehmen und sie im zumutbaren Umfang zu wahren. Dies folgt aus § 242 i.V.m. § 241 Abs. 2 BGB.[244] Diese Pflicht konkretisiert sich in nicht immer trennscharfen Fallgruppen in einer Verschwiegenheitspflicht, Loyalitätspflicht oder Interessenwahrungs- und Schadensabwendungspflicht.[245] Bei der Information über Sicherheitslücken könnte sich die so begründete Pflicht auf Tatsachen und Vorgänge, deren Geheimhaltung im Interesse des Arbeitgebers liegen[246] oder deren Offenbarung den Arbeitgeber schädigen könnte,[247] beziehen. Diese Pflichten können auch grundsätzlich die Beendigung des Arbeitsverhältnisses überdauern.

Soweit Gegenstand der Information ein Betriebs- und Geschäftsgeheimnis ist, ist an die strafrechtliche Beschränkung des „whistleblowing" aus § 17 Abs. 1 UWG zu denken. Arbeitsrechtlich ist es allerdings grundsätzlich unerheblich, ob man Sicherheitslücken als Betriebs- und Geschäftsgeheimnisse qualifizieren kann, da sich die arbeitsrechtliche Rücksichtnahmepflicht über diese hinaus erstreckt.[248]

Das Informationsrecht des Arbeitnehmers ist mangels gesetzlicher Regelung aus dem Umfang und der Reichweite der Pflicht zur Rücksichtnahme des Arbeitnehmers zu entwickeln. Soweit der Arbeitnehmer zur Rücksicht verpflichtet ist, sind ihm Informationsrechte grundsätzlich nur im Einverständnis mit dem Arbeitgeber eingeräumt.

---

243 Vgl. Müller, Whistleblowing, in: NZA 2002, 424; Richters/Wodtke, a.a.O., (Fn. 231), 281 (282); BAG, Urteil v. 03.07.2003 - 2 AZR 235/02, NZA 2004, 427.

244 Vgl. BAG, Urteil v. 03.07.2003 - 2 AZR 235/02, NZA 2004, 427 (429) mit weiteren Hinweisen; Henssler/Willemsen/Kalb-*Thüsing* § 611 BGB Rd. 348.

245 Herbert/Oberrath, Schweigen ist Gold?, in: NZA 2005, 193 (195).

246 Müller, Whistleblowing, in: NZA 2002, 424 (429): Die Verschwiegenheitspflicht umfasse die Geheimhaltung betrieblicher Vorgänge oder Tatsachen, die im Interesse des Arbeitgebers liegen. Die Loyalitätspflicht verpflichte den Arbeitnehmer, Interessen des Arbeitgebers nicht zu verletzen. Der Arbeitnehmer solle nach der Interessenwahrungs- und Schadensabwendungspflicht alles unterlassen, was den Arbeitgeber Schaden könne.

247 Schaub-*Linck* ArbR-Hdb., § 53 Rd. 15.

248 BAG, Urteil v. 03.07.2003 - 2 AZR 235/02, NZA 2004, 427 (429). Strafrechtlich besitzt die Qualifizierung der Sicherheitslücke als Betriebs- oder Geschäftsgeheimnis allerdings durchaus Relevanz, vgl. § 203 StGB.

Regelmäßig werden die Grenzen und die Konkretisierung der Rücksichtnahmepflicht des Arbeitnehmers unter Heranziehung von Grundrechten begründet. Über die Generalklausel in § 242 BGB entfalten die Grundrechte Drittwirkung für das Arbeitsverhältnis.[249] Letztendlich sind der Umfang und das Ausmaß der Rücksichtnahmepflicht aus einer einzelfallbezogenen Güterabwägung zwischen den Grundrechten und den rechtfertigenden Interessen ihrer Einschränkung sowie dem Grundrecht des Arbeitgebers aus Art. 12 Abs. 1 S. 2 GG zu ermitteln.[250]

Insbesondere setzt die Meinungsfreiheit nach Art. 5 Abs. 1 S. 1 GG Maßstäbe zur Beurteilung der Nebenpflicht und damit des whistleblowings. Allerdings ist fraglich, ob das whistleblowing vom Schutzbereich des Art. 5 Abs. 1 GG erfasst wird. Erfasst werden von Art. 5 Abs. 1 S. 1 GG grundsätzlich nur Werturteile und Tatsachenbehauptungen insoweit, als sie Voraussetzung der Bildung von Meinungen sind.[251] Hier kann auf die oben dargelegte Unterscheidung[252] zwischen Tatsachenbehauptung und Werturteil verwiesen werden. Soweit die Information über Sicherheitslücken und Schwachstellen als Tatsachenbehauptung einzustufen ist, ist das whistleblowing, das diese Information zum Gegenstand hat, über Art. 5 Abs. 1 S. 1 GG geschützt.

In Betracht kommt im Fall der Information über Sicherheitslücken auch die Berücksichtigung der beruflichen Interessen des Arbeitnehmers aus Art. 12 Abs. 1 S. 2 GG. Im besonderen Fall des IT-Administrators stehen bei Bekanntwerden und Realisierung der Gefahren der Sicherheitslücke nicht nur die Reputation des Unternehmens, sondern auch die Reputation des Arbeitnehmers – etwa bei Wechsel des Arbeitgebers – auf dem Spiel, da nicht auszuschließen ist, dass die Folgen der Schwachstelle als fachliche Schwäche des Administrators interpretiert werden.

---

249 Ständige Rechtsprechung, statt vieler BVerfG, Urteil v. 15.01.1958, BVerfGE 7, 198 (205); BVerfG, Beschluss 23.04.1986, BVerfGE 73, 261 (269); BAG, Urteil v. 03.07.2003 - 2 AZR 235/02, NZA 2004, 427 (429); BAG, Urteil v. 10.10.2002 - 2 AZR 472/01, NZA 2003, 483 (486). Die Drittwirkung hat für eine Gesellschaftsordnung, in der der Einzelne nicht nur vor staatlicher, sondern auch wirtschaftlicher und sozialer Machtausübung zu schützen ist, besondere Bedeutung, Müller, Whistleblowing, in: NZA 2002, 424 (429).

250 Herbert/Oberrath, Schweigen ist Gold?, in: NZA 2005, 193 (195).

251 Vgl. BVerfG, das klargestellt, dass Tatsachenbehauptungen insoweit dem Schutzbereich unterfallen, als sie mit Werturteilen verbunden sind oder sonst für die Meinungsbildung relevant sind. Damit wird der Schutzbereich weit definiert. Zum Begriff der Tatsachenbehauptung: BVerfG, Beschluss v. 09.10.1991 - 1 BvR, NJW 1992, 1439 (1440); BVerfG, Beschluss v. 11.01.1994, BVerfGE 90, 1 (15)

252 Kapitel 5 B III. 2.

Eine weitere Einschränkung könnte sich aus Art. 2 Abs. 1 i.V.m. 20 Abs. 3 GG ergeben. Aus der staatsbürgerlichen Pflicht und dem Recht an einem Strafverfahren teilzunehmen, könnte sich auch ein Recht ergeben ein solches Verfahren mittels Anzeige einzuleiten (§ 158 Abs. 1 StPO).[253] Diese Konstellation ist jedoch nur im Ausnahmefall der strafrechtlichen Relevanz der Sicherheitslücke eine Grundlage der Einschränkung der Rücksichtnahmepflicht. Eine Regel lässt sich hieraus sicherlich nicht ableiten.

Die Wertentscheidung der Grundrechte gilt allerdings auch nicht uneingeschränkt, sondern ist wiederum am Grundsatz der Verhältnismäßigkeit zu messen. Im Hinblick auf die Konkretisierung der Rücksichtnahmepflicht sollen demnach zumutbare und verhältnismäßige Maßnahmen des Arbeitnehmers die Meinungsäußerungsfreiheit einschränken.[254] Einer Informierung Externer durch den Arbeitnehmer könnten durch die Verhältnismäßigkeitsanforderungen bestimmte Maßnahmen vorgeschaltet sein. Indizien für ein unverhältnismäßiges Verhalten können etwa die Motivation des Arbeitnehmers oder eine fehlende innerbetriebliche Informierung (des Arbeitgebers) sein.[255] Ob solche Indizien vorliegen, ist regelmäßig an den Umständen des Einzelfalls zu messen.

Anknüpfend an die Voraussetzungen des Betriebs- und Geschäftsgeheimnisses könnte die Rücksichtnahmepflicht eingeschränkt werden. Aus der Rücksichtnahmepflicht ergebe sich zumindest, dass der Arbeitnehmer „illegale Geheimnisse" offenbaren darf, wenn keine Abhilfe im Betrieb erreicht werden kann und öffentliche Interessen berührt werden.[256] Es wurde bereits ausgeführt,[257] dass hier das „berechtigte Interesse" des Arbeitgebers an Geheimhaltung verneint wird, wenn der Gegenstand der Geheimhaltung illegale Tatsachen und Vorgänge im Unternehmen betrifft.

Nach den dargelegten Grundsätzen kann der Arbeitnehmer nicht nur berechtigt, sondern sogar verpflichtet sein, über Sicherheitslücken zu informieren. Diese Pflicht ergibt sich, soweit nicht vertraglich vereinbart, ebenfalls aus der Rücksichtnamepflicht des Arbeitnehmers.[258] Fraglich sind allerdings Reichweite und Umfang

---

253 Müller, Whistleblowing, in: NZA 2002, 424 (430).

254 BAG, Urteil v. 03.07.2003 - 2 AZR 235/02, NZA 2004, 427 (430).

255 BAG, Urteil v. 03.07.2003 - 2 AZR 235/02, NZA 2004, 427 (430).

256 Schaub-*Linck* ArbR-Hdb., § 54 Rd. 5.

257 Vgl. Kapitel 5 B V. 2. a).

258 Insoweit sind Informationspflichten nur ein kleiner sehr spezieller Teil der Pflicht des Arbeitnehmers zum sachgemäßen Umgang mit dem Internet. Über den Umfang und die Reichweite des sachgemäßen Umgangs mit dem Internet gibt es bisher kaum Rechtspre-

dieser Pflicht. Nicht zuletzt setzt eine solche ein entsprechendes Sicherheitsbewusstsein voraus und kollidiert in der Praxis mit dem Sicherheitsrisiko „Faktor Mensch". Mit anderen Worten ist der Mitarbeiter nicht nur gehalten, selbst sicherheitsbewusst zu agieren, will er sich unter Umständen nicht schadensersatzpflichtig machen, sondern muss in bestimmtem Maße durch Informationsweitergabe zur Abwendung einer Sicherheitslücke beitragen.

Inwieweit bei Unterlassen ein arbeits- oder haftungsrechtlicher Vorwurf zu machen ist, ist im Einzelfall zu prüfen. Soweit dem Arbeitnehmer lediglich ein fahrlässiges Verhalten vorgeworfen werden kann, ist nach den spezifischen Grundsätzen der Arbeitnehmerhaftung[259] eine anteilige Haftung nur bei mittlerer und eine volle Haftung nur bei grober Fahrlässigkeit begründet.

Arbeitsrechtlich stellt sich in letzter Konsequenz die Frage, inwieweit ein verhaltensbedingter Kündigungsgrund gegeben sein kann. Nach einer Ansicht sind bei „*fahrlässiger Falschbedienung"* des PC keine Kündigungen oder Ersatzansprüche gerechtfertigt.[260] Ein Ergebnis, das zumindest bei durchgeführten Schulungen[261] kaum mit der Pflicht zur Rücksichtnahme für den sensiblen Bereich der IT-Sicherheit, die auch den PC des Mitarbeiters umschließt, zu vereinbaren ist.

Aus der arbeitsgerichtlichen Praxis sollen abschließend Fälle aus der Rechtsprechung zum whistleblowing bemüht werden, aus denen sich Kriterien für den Umfang und die Art und Weise der zulässigen Information für das Szenario 2 ableiten lassen.

---

chung. Dies ist nicht zuletzt den spezifischen Regelungen zur Arbeitnehmerhaftung geschuldet, nach denen der Arbeitnehmer nur im Fall der mittleren Fahrlässigkeit anteilig und bei grober Fahrlässigkeit und Vorsatz voll haftet. So hat die Rechtsprechung im Fall der Computersabotage etwa die eigenmächtige Änderung der Hauptpasswörter beschäftigt, vgl. HessLAG, Urteil v. 13.05.2002 – 13 Sa 12 68/01, RDV 2003, 148. Das HessLAG hob zudem die Bedeutung einer funktionierenden EDV hervor, *die „selbst in kleinen Betrieben (…) das Herzstück der betrieblichen Organisation ist."*, a.a.O., 148. Nach Däubler kann etwa die Weitergabe des Passworts im Einzelfall wegen Gefährdung der Vertraulichkeit eine Abmahnung rechtfertigen, Däubler, Internet und Arbeitsrecht, 2004, Rd. 203.

259 Däubler, Internet und Arbeitsrecht, 2004, Rd. 205.

260 Däubler, Internet und Arbeitsrecht, 2004, Rd. 205a.

261 So sieht etwa die „Richtlinie für die Bereitstellung und Nutzung von Internet/Intranet Zugängen" des Finanzsenats Bremen in Nr. 3 Abs. 3 die Teilnahme an Schulungen vor. Diese Richtlinie ist im Amtsblatt der Freien Hansestadt Bremen, Brem.ABl. Nr. 20 vom 10.02.2004, S. 77 ff., veröffentlicht. Zu einer Verdachtskündigung gegen einen Administrator wegen Einschleusung eines Virus als „Arbeitsbeschaffungsmaßnahme", vgl. LAG Saarland, Urteil v. 01.12.1993 – 2 Sa 154/92, BB 1994, Beilage 7, S. 14.

Im Falle der Information eines Strahlenschutzbeauftragten entschied das BAG, dass Arbeitnehmer, denen die Sicherheit als Aufgabe obliegt, Sicherheitsbedenken auch bei zuständiger Stelle vorbringen können.[262] Eine darauf folgende Kündigung sei unwirksam.

Dem Schutz der öffentlichen Interessen ist in einer Entscheidung des LAG Baden-Württemberg der Vorrang eingeräumt worden, die die Information der zuständigen Lebensmittelkontrolle über die Handhabung und Vermengung von altem und frischem Hackfleisch in einer Metzgereiabteilung zum Gegenstand hatte.[263] Grundsätzlich sei das Verhalten geeignet einen Kündigungsgrund darzustellen, aufgrund des öffentlichen Interesses an der Information allerdings abzulehnen.

In einer anderen Entscheidung des LAG Köln war Gegenstand der Information die Verkehrsuntüchtigkeit eines LKW. Nachdem der Arbeitnehmer vergeblich versuchte den Arbeitgeber zur Herstellung der Verkehrstüchtigkeit zu veranlassen, informierte er die Polizei.[264] Eine darauf folgende Kündigung sei unwirksam.

In einer jüngsten Entscheidung des BVerfG[265] ging es um den „Belastungseifer" eines Arbeitnehmers. Dieser übergab in einem strafrechtlichen Ermittlungsverfahren gegen den Arbeitgeber der Ermittlungsbehörde aus freien Stücken Unterlagen. Das BVerfG sah darin eine zulässige Wahrnehmung staatsbürgerlicher Rechte.

Diesen Fällen ist das öffentliche Interesse an der Information gemein. Soweit Sicherheitslücken Interessen Privater tangieren, ist eine Übertragung fraglich, allerdings aufgrund der vergleichbaren Breitenwirkung durch die Ubiquität von Sicherheitslücken und des Internets als kritische Infrastruktur wohl anzunehmen.[266]

Aus diesen Entscheidungen lassen sich folgende Kriterien entnehmen, die den Abwägungsvorgang präzisieren und die für den Fall der Information über Sicherheitslücken relevant sein können. Die Information (1) ergeht an eine (externe) zu-

---

262 BAG, Entscheidung v. 14.12.1972 – 2 AZR 115/72, DB 1973, 675.

263 LAG Baden-Württemberg, Urteil v. 03.02.1987 - 7 (13) Sa 95/86, NZA 1987, 756.

264 LAG Köln, Urteil v. 23.02.1996 – 11 (13) Sa 976/96, BB 1996, 2411.

265 BVerfG, Beschluss v. 02.07.2001 - 1 BvR 2049/00, NZA 2001, 888; vgl auch BAG, Entscheidung v. 03.07.2003 2003 - 2 AZR 235/02, NZA 2004, 427.

266 Dies ist bedingt durch die Qualität und Gefährdung des Schutzobjektes. Soweit die Sicherheitslücke Auswirkungen auf Rechtsgüter Dritter oder der Allgemeinheit hat, kann auch deren Veröffentlichung im Interesse der Allgemeinheit oder Dritter sein. Im Einzelfall ist allerdings zu entscheiden, welche Form der Veröffentlichung im Interesse Dritter oder der Allgemeinheit ist. Nicht im Interesse ist eine Veröffentlichung, die die Möglichkeiten des Ausnutzens der Lücke fördert.

ständige staatliche Stelle,[267] (2) die Information liegt im Interesse und dient dem Schutz der Öffentlichkeit oder Dritter und (3) die Information ergeht erst, nachdem interne Schadensbegrenzungsversuche fehlgeschlagen sind (Abhilfebemühen[268]). Zusätzlich soll als weiteres Kriterium (4) die Motivation des Arbeitnehmers für die Veröffentlichung genannt werden.[269]

c) Ergebnis für das „whistleblowing" in Szenario 2

Die vielfältigen Kriterien zur Beurteilung des whistleblowings zwingen zu einer Begrenzung des Untersuchungsgegenstandes. Dieser wird durch Szenario 2 konturiert. Gegenstand ist der Arbeitnehmer, der eine Sicherheitslücke mit Auswirkung auf die Wahrung des Fernmeldegeheimnisses Dritter (Kunden) entdeckt. Nach Informierung des Arbeitgebers will dieser keine personellen Mittel zum Schließen der Lücke einsetzen, die Lücke geheim halten und auf die „sichere Unsicherheit"[270] vertrauen. Der Arbeitnehmer postet daraufhin (mittlerweile nicht mehr bei dem Arbeitgeber beschäftigt) die Information in entsprechende Internetforen und verständigt die betroffenen Kunden.

Zunächst kann festgehalten werden, dass durch die Sicherheitslücke Nachrichten des Kunden offenbart werden können, mithin die Wahrung des Fernmeldegeheimnisses nach § 109 Abs. 1 Nr. 1 TKG verletzt sein könnte. Dieses wäre der Fall, wenn der Arbeitgeber angemessene technische Vorkehrungen nicht getroffen hätte. Hierbei ist der erforderliche technische und wirtschaftliche Aufwand in ei-

---

267 Eine bloße Anzeige bei einer Behörde gilt als weniger einschneidend für den Arbeitgeber, dem etwa durch die Information der Medien eine irreparable Schädigung des Rufes droht. Vgl. auch Herbert/Oberrath, Schweigen ist Gold?, in: NZA 2005, 193 (198 f.), der eine Veröffentlichung im Internet als Ultimo Ratio ansieht.

268 Selbst im der IT-Sicherheit „verwandten" Datenschutzrecht findet sich nur eine Anzeigevorschrift, die Interessen Dritter wahren soll. § 4g BDSG sieht im Zweifelsfall eine Anzeige des betrieblichen Datenschutzbeauftragten an die zuständige Aufsichtsbehörde vor. Eingeschränkt wird dieses durch ein vorheriges internes Bemühen um Abhilfe, Simitis u. a., BDSG/*Simitis*, § 4g Rd. 23.

269 Weitere Differenzierungskriterien zur Eingrenzung können sein: der Status des Anzeigenden (Beamter/sonstiger Arbeitnehmer), Qualität des angezeigten Verhaltens (strafbar/gefährlich, moralisch verwerflich, kritikwürdig), Status des Anzeigeempfängers (extern/intern) und Verursacher des angezeigten Verhaltens (Arbeitgeber/Kollegen), Müller, Whistleblowing, in: NZA 2002, 424 (426). Darüber hinaus wurde im vorliegenden Szenario mit der Abhilfe-Reaktion des Arbeitnehmers (Schadensbegrenzung/Ignoranz) ein weiteres Kriterium aufgestellt. Darüber hinaus kann ein Kriterium der rechtlichen Bewertung die Qualität des Gegenstandes (Betriebs- und Geschäftsgeheimnis/sonstiger Betriebs- und Geschäftsgegenstand) sein.

270 Vgl. Kapitel 3 B.

nem angemessenen Verhältnis zur Bedeutung des zu schützenden Rechts zu stellen, § 109 Abs. 2 S. 4 TKG. Das Fernmeldegeheimnis genießt als in Art. 10 Abs. 1 GG verfassungsrechtlich geschützte Position einen hohen Stellenwert. Dem kann nicht entgegen gehalten werden, dass die Ausnutzung der „sicheren Unsicherheit“[271] sehr unwahrscheinlich ist. Als Unternehmer der IT-Branche kann dem Arbeitgeber unterstellt werden, dass er über entsprechenden technischen und personellen Sachverstand verfügt, die Sicherheitslücke zu schließen. Somit liegt ein Verstoß gegen § 109 Abs. 1 Nr. 1 TKG vor und die Sicherheitslücke ist als ein illegales Unternehmensgeheimnis zu qualifizieren und damit nicht als Betriebs- und Geschäftsgeheimnis geschützt.

Aus dem oben Dargestellten ergibt sich Folgendes: Den (Ex-)Arbeitnehmer trifft grundsätzlich eine vertragliche und nachvertragliche Rücksichtnahmepflicht, die ihm Schweigen über die Sicherheitslücke gebietet. Allerdings könnte sich aus Art. 5 und 12 GG etwas anderes ergeben. Soweit die berufliche Reputation des Arbeitnehmers beeinträchtigt ist, könnte ihm grundsätzlich ein Recht zu informieren zustehen. So eingegrenzt bleiben dennoch die oben dargestellten Kriterien zur Abwägung der Offenbarung der Sicherheitslücke.

(1) Die betroffenen Kunden wurden nach Information des untätig gebliebenen Arbeitgebers als externe Stellen informiert, nicht aber die zum Einschreiten berechtigte Bundesnetzagentur als Aufsichtsbehörde nach § 126 TKG.[272] Die Information besitzt damit externe Massenwirkung anstatt die Chance auf ein „stilles“ Aufsichtsverfahren zu nutzen. Andererseits können damit die Interessen der Nutzer effektiver und schneller gewahrt werden als durch ein Aufsichtsverfahren. Auf jeden Fall erscheint das zusätzliche Posten der Information in Internetforen als unverhältnismäßig, da es nicht den Interessen der Nutzer dient und sogar gefahrerhöhend sein kann, da die Lücke von Dritten ausgenutzt werden kann.

(2) Die Information dient dem Kundeninteresse an der Wahrung des Fernmeldegeheimnisses.

(3) Die Information erfolgte auch erst nach fehlgeschlagenen internen Versuchen, die Sicherheitslücke zu beheben. Überlegungen, ob der Arbeitnehmer nicht entgegen der Anweisung des Arbeitgebers die Lücke hätte beseitigen müssen, sind auf-

---

271 Vgl. Kapitel 3 B.

272 Soweit keine angemessenen technischen Vorkehrungen zum Schutz der Nachrichten getroffen werden, liegt ein Verstoß gegen § 109 Abs. 1 Nr. 1 TKG vor, der die Bundesnetzagentur zum ordnungsrechtlichen Einschreiten (Anordnungen nach § 126 Abs. 1 TKG) veranlassen kann.

grund des bestehenden Weisungsrechts des Arbeitgebers wohl im Ergebnis abzulehnen.

(4) Aus der Tatsache, dass der Arbeitnehmer aus dem Unternehmen ausgeschieden ist, lässt sich durch die Informierung der Kunden alleine keine negative Motivation den Arbeitgeber zu schaden ableiten. Durch den zusätzlich herbeigeführten Crash des Servers lässt sich diese jedoch vermuten.

Festzuhalten ist, grundsätzlich stünde dem Arbeitnehmer im Szenario 2 ein Recht die Nutzer und oder die Bundesnetzagentur zu informieren zu, allerdings nicht in der durchgeführten Art und Weise.

C Informationspflichten bei Sicherheitslücken

Die Betrachtung von Informationsrechte war in den vorangegangenen Ausführungen geprägt von der Suche nach den Schranken ihrer Ausübung. Informationspflichten müssen durch Gesetz oder vertraglich begründet werden. Somit orientieren sich die Ausführungen an einem bestehenden Regelungsrahmen. Ein IT-Sicherheitsrecht[273] besticht bisher durch wenig spezifische (gesetzliche) Regelungen, die Basis für eine Analyse der Pflichten im Allgemeinen und der Informationspflichten im Besonderen sein können. Zu nennen sind hier etwa der bereits mehrfach zitierte § 9 BDSG, § 109 TKG und §§ 8 Abs. 4 S. 3 und 5 Abs. 2 GPSG. Explizite Regelungen der Informationspflichten könnten allerdings negative Folgen (Reputationsverluste) der Information ebnen, wenn alle Konkurrenten den gleichen expliziten Pflichten unterworfen wären.[274]

Mit den §§ 33 BDSG, § 4 Abs. 4 PTSG und § 15 Abs. 1 S. 1 WpHG sollen zunächst bereichsspezifische Gesetze als mögliche Grundlage für Informationspflichten dargestellt werden. Diese wurden ausgewählt, da sie als kritische Infrastrukturen und mit Bezug zum Finanzmarkt aus Bereichen stammen, die eine besondere Abhängigkeit von den IT-Infrastrukturen aufweisen, bzw. mit personenbezogenen Kundendaten im E-Commerce ein besonderes Angriffsziel bieten.

Im Anschluss werden die allgemeinen (deliktischen) Sorgfaltspflichten in ihrer Ausprägung als Informationspflichten untersucht. Diese werden differenziert nach

---

273 Grundlegend zum IT-Sicherheitsrecht: Holznagel, Recht der IT-Sicherheit, 2003.

274 Chang, Computer Hacking: Making the Case for a National Reporting Requirement, S. 28, http://cyber.law.harvard.edu/home/2004-06 (30.05.2006).

Produktbeobachtungspflichten (der Hersteller) sowie Verkehrssicherungs- und Amtspflichten der Anbieter.

Soweit die Wirkung der Information – als Schutz oder Sicherheitslücke[275] – Einfluss auf die Bestimmung der Informationspflicht hat, soll hier von einer *„unpredictable Full-Disclosure"*[276] ausgegangen werden.

I. Bereichsspezifische Informationspflichten

1. Informationspflicht des Anbieters bei Offenbarung von Kundendaten

a) Pflicht nach § 33 Abs. 1 S. 1 BDSG – Versandshop im Szenario 3

Da bei der Offenbarung von personenbezogenen Kundendaten der Datenschutz betroffen ist, könnte das BDSG – so die These – bereichspezifische Informationspflichten regeln.

Den folgenden Ausführungen wird Szenario 3 zu Grunde gelegt. Hierbei gilt es die Frage zu beantworten, ob der Betreiber des Versandshops die Kunden von der „sicheren Unsicherheit"[277] informieren muss. Eine so verstandene Information über Sicherheitslücken beweckt nicht primär das Schließen der Lücke, sondern dient der Schadensminimierung und gibt dem Betroffenen Transparenz über die Verfasstheit und Integrität seiner Daten. Insbesondere soll sie verhindern, dass offen gelegte Daten missbraucht werden können.

Eine Pflicht des Anbieters über Sicherheitslücken zu informieren könnte sich aus §§ 19a, 33 BDSG ergeben. Diese sehen vor, dass bei Datenbeschaffung ohne Kenntnis des Betroffenen dieser hierüber zu unterrichten ist. Dies ist die Normierung einer verfahrensrechtlichen Folge einer unzulässigen Datenbeschaffung.[278] Faktisch zwingen sie die Daten beschaffende Stelle zu widersprüchlichem Verhal-

---

275 Vgl. Kapitel 2 B V. 3.

276 Vgl. Kapitel 3 B.

277 Vgl. Kapitel 3 B.

278 Zulässig ist die Datenerhebung grundsätzlich nur mit Einwilligung oder aufgrund einer Rechtsgrundlage, § 4 BDSG. Grundsätzlich soll jeder Betroffene also Kenntnis haben, bei wem welche Daten gespeichert sind. Bei der Erhebung aufgrund Gesetz kann dies zumindest vermutet werden, da andernfalls die Ausnahme von der Benachrichtigungspflicht nach § 33 Abs. 2 Nr. 4 BDSG kontraproduktiv wäre.

ten. Einerseits darf sie nach dem Gesetz (vgl. § 4 BDSG) grundsätzlich nur mit Kenntnis des Betroffenen Daten erheben.[279] Verstößt sie gegen das Gesetz, indem sie ohne Kenntnis Daten erhebt, so soll sie gesetzmäßigerweise initiativ-aktiv den Betroffenen davon unterrichten.

Alternativ könnte eine Pflicht des Anbieters über Sicherheitslücken zu informieren aus §§ 19, 34 BDSG begründet werden. Im Unterschied zu der Benachrichtigung verlangt der Auskunftsanspruch ein initiativ-aktives Handeln des Betroffenen. Damit ist er kaum geeignet, einen Beitrag zur Vermeidung oder Minimierung von konkreten Sicherheitslücken zu leisten, von deren Bestehen er keine Kenntnis hat. Dies würde ein Auskunftsverlangen „ins Blaue" erfordern.[280] Die Benachrichtigungspflicht aus §§ 19a und 33 BDSG versetzt den Betroffenen vielmehr erst in die Lage, seine Rechte aus §§ 19 und 34 BDSG wahrnehmen zu können.[281] Eine entsprechende Informationspflicht lässt sich demnach nicht aus §§ 19 und 34 BDSG begründen.

§§ 19a, 33 BDSG sind nahezu inhaltsgleich.[282] § 33 Abs. 1 S. 1 BDSG:

> *„Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen."*

Eine Differenzierung in zwei Regelungen einer Benachrichtigungspflicht ergibt sich aus der Systematik des BDSG, das zwischen öffentlichen und nicht-öffentlichen Stellen trennt (§ 1 Abs. 2 BDSG). Im Folgenden ist § 33 BDSG einschlägig, da der Betreiber des Versandshops eine nicht-öffentliche Stelle im Sinn von § 1 Abs. 2 Nr. 3 BDSG ist.[283]

---

279 Dies spiegelt sich auch der Benachrichtigungspflicht nach § 4 Abs. 3 BDSG wieder. Hier ist die Kenntnis des Betroffenen von der Tatsache der Datenerhebung zu unterstellen, da die Daten bei ihm selbst erhoben werden.

280 Vgl. Kapitel 4 A II. 2. b) am Ende.

281 Simitis u.a., BDSG/*Mallmann*, § 19a Rd. 3.

282 § 19a Abs. 1 S. 1 BDSG: *"Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung zu unterrichten."* Das wesentliche Unterscheidungskriterium ist die erstmalige Speicherung. Die Erstmaligkeit meint, dass bisher noch keine Daten von dem Betroffenen gespeichert sind und schließt einen Benachrichtigungsanspruch beim Zuspeichern von weiteren, gleichartigen Daten aus, Schaffland/Wiltfang, BDSG § 19a Rd. 2; a. A. Simitis u. a., BDSG/*Mallmann*, § 33 Rd. 9.

283 Im Folgenden soll Frage nach der Benachrichtigungspflicht als Pflicht zu informieren ausschließlich anhand von § 33 BDSG diskutiert werden. Die so gewonnenen Ergebnisse können auf § 19a BDSG erstreckt werden, soweit es um die Frage geht, ob eine Benachrichtigungspflicht auch durch eine erforderliche Information über Sicherheitslücken ausgelöst wird.

Der Betreiber des Versandshops hat die Kundendaten mit Kenntnis des Betroffenen gespeichert, da der Betroffene die Registrierungsoption selbst wahrgenommen und seine Daten online eingegeben hat. Fraglich ist, ob durch die Speicherung durch Frau Anonym und potenzieller Hacker – unzweifelhaft ohne Kenntnis des Betroffenen – eine Benachrichtigungspflicht des Betreibers nach § 33 Abs. 1 BDSG ausgelöst wird. Liest man § 33 Abs. 1 S. 1 BDSG, so könnte den Betreiber eine Benachrichtigungspflicht treffen, zumal § 33 Abs. 1 BDSG den Normverpflichteten nicht klar benennt. Mit der Gesetzessystematik ist der Verpflichtete § 27 Abs. 1 BDSG i.V.m. § 3 Abs. 7 BDSG zu entnehmen.[284] Verpflichtete könnte demnach der Betreiber als verantwortliche Stelle nach § 3 Abs. 7 BDSG sein, da er die Daten der Kunden speichert. Allerdings speichert er die Daten mit Mithilfe und somit nicht ohne Kenntnis der Kunden. Somit erfüllt er nicht den Tatbestand des § 33 Abs. 1 S. 1 BDSG.

Prüft man jedoch § 33 Abs. 1 S. 3 BDSG, so könnte der Betreiber des Versandshops trotzdem nach § 33 Abs. 1 S. 1 BDSG analog die Kunden von der Sicherheitslücke benachrichtigen müssen:

> *„Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss."*

Eine Ausweitung der Datenverarbeitung – nach Satz 3 ist eine weitere Übermittlung der (bereits gespeicherten) Daten vorgesehen – kann allerdings das gefundene Ergebnis nicht verändern, da Satz 3 sich auf den Verpflichteten aus Satz 1 bezieht.

Zudem ergibt sich aus einer Gesamtschau mit § 4 Abs. 3 BDSG[285], dass der Betreiber des Versandshops nicht von § 33 Abs. 1 BDSG analog erfasst werden kann, wenn dieser bereits nach § 4 Abs. 3 BDSG verpflichtet wäre – und somit keine Regelungslücke bestünde.[286] Eine Benachrichtigungspflicht des Betreibers nach beiden Normen wäre grundsätzlich in sich widersprüchlich. Zumal Beide Teile einer logischen „Architektur" datenschutzrechtlicher Pflichten sind.[287] Verpflichtete nach § 33 Abs. 1 S. 1 BDSG ist vielmehr grundsätzlich Frau Anonym und poten-

---

284 Vgl. Gola/Schomerus, BDSG, § 33 Rd. 3.

285 § 4 Abs. 3 BDSG: *„Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über 1. die Identität der verantwortlichen Stelle, 2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und 3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss, zu unterrichten."*

286 In dem Szenario scheidet eine Pflicht allerdings aus, da der Betroffene mit der eigenen Eingabe seiner Daten bei Registrierung auch Kenntnis von der Datenerhebung hat.

287 Bizer, Datenschutzrechtliche Informationspflichten, in: DuD 2005, 451 (451).

zieller Hacker, die die Sicherheitslücke entdeckt und Kundendaten gespeichert haben, denn hier liegt eine erstmalige Speicherung ohne Kenntnis den Betroffenen vor. Eine Benachrichtigungspflicht des Betreibers nach beiden Normen ist allerdings kein Widerspruch, da der Anwendung der Normen unterschiedliche Sachverhalte zu Grunde liegen. § 4 Abs. 3 BDSG findet Anwendung für die (erstmalige) Speicherung durch die online Registrierung. § 33 Abs. 1 BDSG auf die erstmalige Speicherung durch Frau Anonym und potenzieller Hacker.

Zudem könnte der Betreiber des Versandshops als verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG verpflichtet sein, über die Tatsache der Speicherung beim Hacker zu benachrichtigen.[288] Die Legaldefinition des § 3 Abs. 7 BDSG regelt nur eine verfahrenstechnische Zuordnung, nicht zwingend eine schützende Verantwortlichkeit im Sinne von Verantwortung für die Daten. Diese ergibt sich jedoch aus dem Zweck des Gesetzes.

Zweck der Norm ist, Transparenz bei der Datenverarbeitung zu schaffen und dem Betroffenen die Geltendmachung seiner Rechte zu erleichtern.[289] Es soll sicherstellt werden,

> *„dass der Betroffene von einer Verarbeitung seiner Daten auch dann erfährt, wenn sie nicht direkt bei ihm erhoben worden sind.‘*[290]

Als Mittel zur Sicherung des in Art. 2 Abs. 1 i.V.m. 1 Abs. 1 S. 1 GG verfassungsrechtlich verankerten Rechts auf informationelle Selbstbestimmung ist die Benachrichtigungspflicht weit auszulegen.[291]

Es ist mit dem Schutzzweck des Gesetzes nicht vereinbar, wenn dem Hacker eine Informationspflicht obliegt, aber derjenige, der für den Schutz der Daten originär verantwortlich und dem eine entsprechende Information des Betroffenen möglich ist, keine entsprechende Pflicht besitzt.

Wenn durch § 33 BDSG schon der Missbrauchsgefahr durch eine regelmäßige und (branchen)typische Speicherung von Daten – etwa bei Auskunfteien – durch eine

---

288 So Gola/Schomerus, BDSG, § 33 Rd. 3, mit dem Ergebnis, dass die Benachrichtigungspflicht des Empfängers entfällt, da der Betroffene nach § 33 Abs. 2 Nr. 1 BDSG auf andere Weise von der Speicherung erfahren hat.

289 Simitis u. a., BDSG/*Mallmann*, § 19a Rd. 3. Beispielhaft werden als solche Rechte genannt: *"Kontroll-, Abwehr- und Gestaltungsrechte wie diejenigen auf Benachrichtigung, Sperrung, Löschung und Widerspruch"*, Simitis u. a., BDSG/*Mallmann*, § 19 Rd. 1.

290 Bizer, Datenschutzrechtliche Informationspflichten, in: DuD 2005, 451 (452).

291 Die Benachrichtigung als „verfahrensrechtliche Schutzvorkehrung“ vgl. BVerfG „Volkszählungsurteil”, Entscheidung v. 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1 (46); Simitis u. a., BDSG/*Mallmann*, § 19a Rd. 4.

Benachrichtigungspflicht begegnet werden soll, so muss dies erst recht für eine atypische und unvorhergesehene Erhebung und Speicherung von Daten gelten, bei der eine Missbrauchsabsicht (etwa bei der Verschaffung eines unberechtigten Zugangs zu Kontodaten) sogar regelmäßig unterstellt werden kann.

Gegen die Ausweitung auf den unberechtigten Zugriff auf Daten könnte sprechen, dass die Benachrichtigungspflicht als Vorstufe zum Auskunftsanspruch primär diesen ermöglichen soll.[292] Dieser Auskunftsanspruch kann mangels Nennung des Empfängers nicht wahrgenommen werden. Für den Zweck der Transparenz über den „Aufenthaltsort" eigener Daten, genügt jedoch zunächst das Wissen um die Tatsache, dass ohne Kenntnis Daten erhoben wurden.

Gegen eine Ausweitung könnte zudem das Verhältnismäßigkeitsprinzip sprechen. Dieses konkretisiert sich an einigen Stellen in § 33 Abs. 2 BDSG, der Ausnahmen von der Benachrichtigungspflicht bestimmt. Diese besteht regelmäßig nicht, wenn die Benachrichtigung einen *„unverhältnismäßigen Aufwand erfordern würde"*[293] oder *„wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist"*[294]. Für eine Benachrichtigung könnte sprechen, dass ein Gesetzesverstoß – die mangelnde Zugriffskontrolle nach § 9 BDSG i.V.m. Nr. 3 der Anlage zu § 9 BDSG – den unberechtigten Zugang zu den Kundendaten erst möglich macht.[295] Gegen eine Benachrichtigung könnte sprechen, dass ein Missbrauch der Daten nicht erwiesen ist. Da bei den Kundendaten auch Kreditkartennummern abgelegt sind, und damit eine hohe Missbrauchsgefahr besteht, ist auch ein höherer Benachrichtigungsaufwand zumutbar, zumal eine Benachrichtigung formlos möglich ist.[296] Auch kann es auf einen möglichen Reputationsverlust des Unternehmens nicht ankommen, da eine Benachrichtigung dann regelmäßig ausgeschlossen wäre und dem Schutzzweck des Gesetzes so nicht Genüge getan werden könnte.[297] Letztendlich ist eine Benachrichtigung nicht unverhältnismäßig.

---

292 Simitis u. a., BDSG/*Mallmann*, § 33 Rd. 15.

293 § 33 Abs. 2 Nr. 2 BDSG.

294 § 33 Abs. 2 Nr. 7 a) BDSG.

295 Hier kann im Sinne einer Verkürzung der Argumentation auf das Wesentliche unterstellt werden, dass eine Verletzung von § 9 BDSG vorliegt.

296 Argumentum e contrario § 34 Abs. 3 BDSG, der grundsätzlich für die Auskunftspflicht die Schriftform vorsieht.

297 Auch indizieren die Ausnahmen aus § 33 Abs. 2 BDSG eine rein wirtschaftliche Betrachtung vor der Benachrichtigung und nicht wirtschaftlich mögliche Folgen in der Zukunft.

Für eine Ausweitung auf den vorliegenden Fall kann letztendlich der Gedanke des § 6 Abs. 2 BDSG[298] herangezogen werden. Diesem kann entnommen werden, dass Stellen die Daten über Betroffene gespeichert haben, diesem umfassend zur Hilfe bei der Suche nach dem „Aufenthaltsort" seiner Daten verpflichtet sind.

Problematisch ist allerdings der Zeitpunkt der Benachrichtigung.[299] Entsprechend dem Tatbestandsmerkmal der Speicherung ist eine Benachrichtigung noch nicht erforderlich, wenn die Sicherheitslücke zwar entdeckt, jedoch noch nicht erkennbar ausgenutzt, d. h. Daten durch den unberechtigten Zugriff erhoben wurden. Letztes zu beurteilen ist allerdings unter dem Gesichtspunkt der „sicheren Unsicherheit" – im Szenario 3 durch den Hinweis von Frau Anonym – regelmäßig jedoch nicht möglich.

Festgehalten werden kann, dass eine Pflicht zu informieren entsprechend § 33 Abs. 1 S. 1 und 3 BDSG grundsätzlich durch mehrere im BDSG getroffenen Wertungen indiziert ist. Ein Verstoß gegen § 33 BDSG stellt allerdings eine Ordnungswidrigkeit dar, die nach § 43 Abs. 3 mit einer Geldbuße bis zur 25.000 € geahndet werden kann. Da das Analogieverbot des Art. 103 Abs. 2 GG sich auf Ordnungswidrigkeiten erstreckt, verbietet sich eine entsprechende Anwendung von § 33 Abs. 1 BDSG.[300]

Festzuhalten ist, der Betreiber des Online-Versandshops ist nicht verpflichtet, entsprechend § 33 Abs. 1 S. 1 und 3 BDSG die Kunden von der Ausnutzung der Sicherheitslücke in Kenntnis zu setzen.

b) Online-Versandshop im US-amerikanischen Recht

Aufgrund der Parallelen zum Szenario 3 und dem vorangegangenen Punkt, soll folgend ein Überblick über die Informationspflichten in datenschutzrechtlichen Regelungen und die Entwicklungen in den USA bei der Offenbarung von Kundendaten gegeben werden.

---

298 § 6 Abs. 2 S. 1 und 2 BDSG: *„Sind die Daten des Betroffenen automatisiert in der Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten."*

299 Grundsätzlich soll mangels einer gesetzlichen Frist die Schutzfunktion des Gesetzes eine „unverzügliche" Benachrichtigung entsprechend § 121 BGB fordern, Gola/Schomerus, BDSG, § 33 Rd. 15.

300 Vgl. BVerfG „Anti-Atomkraftplakette", Beschluss v. 23.10.1985 - 1 BvR 1053/82, BVerfGE 71, 108.

In den USA werden drei „rechtliche Trends" im Bereich der *„information security"*[601] ausgemacht. Zum einen die Erkenntnis, dass „information security" eine (rechtliche) Pflicht der Unternehmen ist, zum anderen die Entwicklung rechtlicher Standards für „information security" und letztens die Betonung einer Pflicht Verletzungen der „information security" zu offenbaren.[302]

Im Folgenden sollen Entwicklungen bei den Offenbarungspflichten dargestellt werden. Eine geltende Regelung findet sich im Recht Kaliforniens in dem *„Security Breach Information Act"* [303]. Im Entwurfsstadium befindet sich im Bundesrecht der USA der "Personal Data Privacy And Security Act of 2005"[304]. Die dort niedergelegten Pflichten über Angriffe zu informieren sollen kurz dargestellt und ihre Vorbildfunktion für eine entsprechende Informationspflicht über Sicherheitslücken im deutschen Recht untersucht werden.

Mit Inkrafttreten des „Security Breach Information Act" in Kalifornien zum 01.07.2003, werden Behörden und Unternehmen verpflichtet, „Sicherheitsverletzungen des Systems"[305] den betroffenen Personen (schriftlich) zu offenbaren, wenn personenbezogene Daten[306] (eines Einwohners Kaliforniens) von einer nicht berechtigten Person erlangt wurden. Von dieser Pflicht ist der Betreiber nur befreit,

---

301 "Information Security" ist wohl umfassend im Sinn der hier verwendeten IT-Sicherheit zu übersetzen.

302 Smedinghoff, Trends in the law of information security, in: 829 PLI/Pat, 285 (289).

303 Der Security Information Act (Bill Number SB 1386) fließt in den Civil Code of California, Section 1798.29 und 1798.82 ein. Er soll insbesondere gegen den "Identity Theft" vorgehen. Dieser ist in den USA aufgrund der umfassenden Verwendung der „Sozialversicherungsnummer" als Identitätsnachweis möglich. Vgl. etwa eine Meldung bei heise news vom 13.04.2005 zum Identitätsdiebstahl bei LexisNexis, http://www.heise.de/newsticker/meldung/58523 (30.05.2006). Seit 2003 sind entsprechende Gesetzesvorhaben auch in anderen US-Bundesstaaten geplant. Einen Überblick über die einzelnen Vorhaben in den Bundesstaaten gibt, Rasch, Mark, Cleaning Up Disclosure, SecurityFocus 11.04.2005, http://www.securityfocus.com/columnists/316 (30.05.2006). Allerdings ist der funktionale Nutzen bei bundesweit operierenden Unternehmen, die unterschiedlichen Informationspflichten ausgesetzt sein können, anzuzweifeln.

304 Senat Bill vom 26.06.2005, S. 1332 des 109th Congress (2005-2006). Letzter Status: Placed on Senate Legislative Calendar under General Orders, Calendar No. 151 (30.05.2006).

305 Sec. 2 (d) Security Breach Information Act: *„Breach of the security of the system" means unauthorized acquisition of computerized data that compromise the security, confidentiality, or integrity of personal information maintained by the agency"*, (floss als Section 1798.29 (d) in den Civil Code California ein). Ebenso Sec. 4 (d) Security Breach Information Act für Unternehmen (floss als Section 1798.82 (d) in den Civil Code California ein).

306 Personenbezogene Daten im Sinne des Gesetzes sind der Name des Kunden in Kombination mit einer unverschlüsselten Sozialversicherungsnummer, Führerscheinnummer oder Kontodaten in Verbindung mit Zugangsdaten oder Passwort, vgl. Sec. 2 (e) Security Breach Information Act.

wenn er die Kundendaten durch Verschlüsselung geschützt hat.[307] Der Angriff auf die Kundendaten soll grundsätzlich unmittelbar nach Entdeckung den betroffenen Kunden in einer „angemessenen Frist" offenbart werden *(„in the most expedient time possible and without reasonable delay"*[608]). Diese Regelung soll den Kunden vor Missbrauch der offenbarten und erlangten Daten schützen.

Mit Bekanntwerden einiger unberechtigten Zugriffe auf Datenbanken im größeren Ausmaß – etwa der Zugriff auf über 40 Millionen Kreditkartendaten[309] – ist Ende Juni 2005 auch der US-Bundesgesetzgeber aktiv geworden. Am 29.06.2005 wurde mit dem "Personal Data Privacy and Security Act of 2005" ein Gesetzesvorschlag auf Bundesebene eingereicht. Dieser Act soll die Veröffentlichung, den Verkauf oder Erwerb personenbezogener Informationen (insbesondere in Verbindung mit der Sozialversicherungsnummer) verbieten und verhindern. Um dieses Ziel zu erreichen, ist neben der Etablierung von Standards zum Schutz von *„privacy and security"*[610] vorgesehen, dass die Betroffenen über den unbefugten Datenzugriff zu informieren sind. Dies deckt sich im Grundsatz mit den Informationspflichten im „Security Breach Information Act", ist inhaltlich aber detaillierter ausgeführt. So sind etwa zusätzlich neben den betroffenen Kunden (Einwohner der USA) auch Verbraucherschutzorganisationen[311] und ab einer kritischen Schwelle von 10000

---

307 Vgl. Sec. 2 (a) Security Breach Information Act: *"(…) whose unencrypted personal information (…)"*.

308 Vgl. Sec. 2 (a) Security Breach Information Act.

309 Vgl. der Zugang zu 40 Millionen Kreditkartendaten bei einem Dienstleister, der Transaktionen zwischen Händlern und Kreditkartenunternehmen durchführt, heise news vom 18.06.2005, http://www.heise.de/newsticker/meldung/60767 (30.05.2006); Zugang zu Kreditkartendaten durch Zugang zu den Datensätzen einer Bekleidungsfirma, heise news vom 14.04.2005, http://www.heise.de/newsticker/meldung/58591 (30.05.2006); bei LexisNexis, heise news vom 10.03.2005, http://www.heise.de/newsticker/meldung/57286 (30.05.2006). In der Regel ermöglichte eine Sicherheitslücke den Zugang zu den Daten. So etwa im Fall des Zugangs zu 40 Millionen Kreditkartendaten: Hier wurde eine Sicherheitslücke im Netzwerk ausgenutzt, um sich Zugang zu unverschlüsselten Daten zu verschaffen, heise news vom 20.06.2005, http://www.heise.de/newsticker/meldung/60810 (30.05.2006). Betroffene Kunden aus Deutschland wurden erst Ende Juni von diesem Vorfall im April schriftlich informiert und erhielten neue Kreditkarten, heise news vom 30.06.2005, http://-www.heise.de/newsticker/meldung/61288 (30.05.2006).

310 Sec. 401 ff. Personal Data Privacy And Security Act of 2005.

311 Sec. 421 (a) (2) Personal Data Privacy And Security Act of 2005: *"consumer reporting agency"*. Diese werden in 15 U.S.C. 1681 (a) (United States Code) definiert: *"Consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers"*.

Betroffenen[312] staatliche Behörden zu informieren und gegebenenfalls an der Aufklärung zu beteiligen.[313]

Abgesehen von der die Veröffentlichungspflicht ausschließenden Verschlüsselung der Daten ist es nicht relevant, in welchem Maße Schutzmaßnahmen gegen den unbefugten Zugang zum System getroffen wurden. Die Norm definiert keine Standards hinsichtlich Vorkehrungen, die getroffen werden müssten, um von dem Einbruch in das System Kenntnis zu erlangen.

In der (geplanten) Bundesregelung werden zu treffende Schutzmaßnahmen etwas konkreter angesprochen. So ist das Unternehmen (nicht aber die Behörde) von der Pflicht den Zugriff auf Daten zu melden befreit, wenn:

> *„the business entity utilizes a security program reasonably designed to block the use of the sensitive personally identificable information to initiate unautorized transaction before they are charged to the account of the individual".*[314]

Der „Security Breach Information Act" beträfe Fälle wie im Szenario 3 geschildert. Für das Unternehmen in Szenario 3 bestünde mit den Vorschriften des „Security Breach Information Act" eine Verpflichtung, die Kunden schriftlich („written notice" oder „electronic notice") über die Einsichtnahme in die Kundendaten zu informieren. Zu informieren wäre nicht über das Bestehen einer Schwachstelle, sondern darüber, dass die Datensicherheit und der Datenschutz verletzt worden sind.

Ob man Informationspflichten wie im „Security Breach Information Act" erst bei einem tatsächlichen Zugriff auf (personenbezogene) Daten annehmen soll, erscheint fraglich. Nicht zuletzt kann eine weitergehende Informationspflicht – die zeitlich früher mit Entdeckung einer Sicherheitslücke ausgelöst werden könnte – neben einem effektiveren Schutz des Betroffenen (Kunden/Bürger) vor Missbrauch der Daten weitere Funktionen erfüllen. So haben Informationspflichten eine die Anbieter disziplinierende Funktion. Nicht zuletzt können sie die Eigenverantwortung des Einzelnen nicht nur für eigene Sicherheitsvorkehrungen[315], sondern auch für die Entscheidung, wem Daten anvertraut werden können, d. h. wer erfor-

---

312 Sec. 421 (a) (1) Personal Data Privacy And Security Act of 2005: "*if the security breach impacts more than 10,000 individuals nationwide, impacts a database, networked or integrated databases, or other data system associated with more than 1,000,000 individuals nationwide, impacts databases owned or used by the Federal Government, or involves sensitive personally identifiable information of employees and contractors of the Federal Government".*

313 Sec. 421 (a) (1) (A) Personal Data Privacy And Security Act of 2005.

314 Sec. 424 (b) (2) Personal Data Privacy And Security Act of 2005.

315 Chang, Computer Hacking: Making the Case for a National Reporting Requirement, S. 29, http://cyber.law.harvard.edu/home/2004-06 (30.05.2006), "*Some customers misjudge the threat [because] intrusions are for the most largely undetected and unreported."*

derliche Sicherheitsmaßnahmen ergriffen hat und somit idealiter keine Sicherheitslücken und Schwachstellen aufweist, stärken.

2. Informationspflicht der Anbieter kritischer Infrastrukturen

Für kritische Infrastrukturen ergeben sich spezifische Pflichten aus gesetzlichen Regelungen, namentlich § 4 Abs. 4 PTSG und Art. 4 Abs. 2 der elektronischen Datenschutzrichtlinie.

Mit dem Post- und Telekommunikationssicherstellungsgesetz (PTSG)[316] wurde neben der teilidentischen und teilweise subsidiären Regelung in § 109 Abs. 2 S. 1 TKG (§ 87 Abs. 1 Nr. 3 und 4 TKG a. F.) ein Gesetz geschaffen, das vor unerlaubten Zugriffen auf ein Kommunikationssystem schützen soll.

Mit dem § 4 Abs. 4 PTSG haben Unternehmen Störungen, die erhebliche Auswirkungen auf die Kunden haben, dem Bundesministerium für Wirtschaft und Arbeit unverzüglich mitzuteilen. Eine Informationspflicht besteht jedoch nur für Störungen, die ein Ausmaß erreichen, das in einem Anwendungsfall des Gesetzes (vgl. § 1 PTSG) vertypisiert ist.[317] Eine Informationspflicht besteht demnach grundsätzlich nur bei Naturkatastrophen oder einem besonders schweren Unglücksfall. Ein schwerer Unglücksfall ist nicht bei einer bloßen individuellen Betroffenheit, auch wenn Schäden in Millionenhöhe, wie etwa durch prominente Viren in der Vergangenheit[318], anzunehmen. Die Störung muss vielmehr den Katastrophenschutz betreffende Auswirkungen für die Sicherheit und Ordnung haben.[319] Damit scheidet § 4 Abs. 4 PTSG als regelmäßige Pflicht der Unternehmen über „alltägliche" Sicherheitslücken und Schwachstellen in IT-Systemen zu informieren aus.

Art. 4 Abs. 2 der Elektronischen Datenschutzrichtlinie[320] (d. h. eine entsprechende Regelung sollte in allen Mitgliedstaaten existieren) begründet bei einem besonderen

---

316 Zur Entstehungsgeschichte, BT-Drs. 12/6718, S. 56 ff.; 12/7270 S. 19, 27; 12/8060, S. 124 ff.

317 Beck'scher TKG-Kommentar/*Ehmer* Anh § 87 § 4 PTSG Rd. 2.

318 Eine Übersicht über die Schäden finden sich bei Sonntag, IT-Sicherheit kritischer Infrastrukturen, 2005, S. 59. Solche IT-Sicherheitsvorfälle sollen durch die Versuche diese regelmäßig geheim zuhalten ein eigenes Bedrohungspotenzial besitzen.

319 Beck'scher TKG-Kommentar/*Ehmer* Anh § 87 § 1 PTSG Rd. 1.

320 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. Nr. L 201, vom 31.07.2002, S. 37. Frist zur Umsetzung der Richtlinie war nach Art. 17 der 31.10.2003.

Risiko der Verletzung der Netzsicherheit eine Informationspflicht der Betreiber.[321] Damit betrifft es zwar nicht ausdrücklich kritische Infrastrukturen. Allerdings sind diese wesentlich von der Gewährleistung der Netzsicherheit abhängig und damit kann Art. 4 Abs. 2 der Elektronischen Datenschutzrichtlinie als Schutz kritischen Infrastrukturen betrachtet werden Dieser sieht vor:

> *„Besteht ein besonderes Risiko der Verletzung der Netzsicherheit, muss der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes die Teilnehmer über dieses Risiko und – wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahmen liegt – über mögliche Abhilfen, einschließlich der voraussichtlich entstehenden Kosten, unterrichten."*

Die elektronische Datenschutzrichtlinie wurde mit der Novelle des TKG 2004 umgesetzt.[322] Da sich im TKG keine Art. 4 Abs. 2 entsprechende Regelung findet, kann vermutet werden, dass der inhaltlich engere § 4 Abs. 4 PTSG eine Umsetzung entbehrlich machen sollte. Allerdings regelt dieser bei einem inhaltlichen Vergleich nicht die Vorgaben der Richtlinie. Soweit sich im deutschen Recht keine entsprechende Regelung findet, könnte Art. 4 Abs. 2 im Wege der richtlinienkonformen Auslegung im deutschen Recht zu berücksichtigen sein[323] – etwa bei der Bestimmung und Konkretisierung von Verkehrssicherungspflichten – und damit eine Informationspflicht der Anbieter begründen.

3. Ad-hoc-Informationspflicht börsennotierter Unternehmen

Soweit Ausmaß und Folgen einer Sicherheitslücke geeignet sind, den Börsenpreis der Wertpapiere eines Unternehmens zu beeinflussen, könnte eine Veröffentlichungspflicht eines börsennotierten Unternehmens nach § 15 Abs. 1 S. 1 WpHG[324] im Wege der Ad-hoc-Mitteilung bestehen. Diese Informationspflicht besteht personell nur für Emittenten von Finanzinstrumenten, die zum Handel an einer deutschen Börse zugelassen sind. Zudem muss eine Sicherheitslücke eine Insiderinformation darstellen. Insiderinformationen sind Umstände, die nicht öffentlich be-

---

321 Auf Szenario 3 findet Art. 4 c) keine Anwendung, da dieses die Datensicherheit und nicht die Netzsicherheit betrifft.

322 Telekommunikationsgesetz, BGBl. 2004, I Nr. 29, 25.06.2004, S. 1190; vgl. Gesetzesentwurf eines Telekommunikationsgesetzes vom 17.10.2003, BR-Drs. 755/03, S. 5; Gesetzesentwurf vom 09.01.2004, BT-Drs. 13/2316, S. 5 und 55.

323 Soweit eine horizontale Direktwirkung, d. h. eine unmittelbare Wirkung zwischen Privaten, abgelehnt wird, könnte Art. 4 Abs. 2 in die richterliche Auslegung und Bewertung der deliktischen Schutzpflichten einfließen. Zu den Voraussetzungen der Direktwirkung im Europarecht, vgl. Gundel, Neue Grenzlinien für die Direktwirkung nicht umgesetzter EG-Richtlinien unter Privaten, in: EuZW 2001, 143 ff.

324 Wertpapierhandelsgesetz.

kannt und geeignet sind, den Börsen- und Marktpreis erheblich zu beeinflussen, § 13 Abs. 1 S. 1 WpHG.

Vorangestellt sei jedoch, dass die Norm nicht den Individualinteressen der Anlieger/Nutzer, sondern ausschließlich der Sicherung und Funktionsfähigkeit des Kapitalmarktes dient.[325] Nach § 15 Abs. 1 WpHG publizitätspflichtige Sachverhalte sind Umstände, die den Emittenten ummittelbar betreffen und die geeignet sind, den Börsen- oder Marktpreis erheblich zu beeinflussen. Hierunter können auch *„technische Probleme, die mit Qualitätseinbußen der Produkte verbunden sind"*[626] fallen. Maßstab für die Eignung zur erheblichen Kursbeeinflussung ist, ob ein verständiger Anleger eine Kauf- oder Verkaufsentscheidung aufgrund der Information treffen würde, § 13 Abs. 1 S. 2 WpHG. Mithin ist eine Informationspflicht schwerpunktmäßig für börsennotierte Unternehmen der Branche IT-Sicherheit relevant, aber auch für jedes börsennotierte Unternehmen, dessen Geschäftstätigkeit auf eine funktionsfähige IT angewiesen ist, denkbar.

Hervorgehoben werden soll allerdings das Konkurrenzverhältnis zwischen der Adhoc-Publizitätspflicht und der IT-Sicherheit. Unterstellt, dass Sicherheitslücken der Produkte oder Schwachstellen des IT-Systems des Unternehmens kurserheblich sind, sind diese unverzüglich zu veröffentlichen. Die *„Zeitgerechtigkeit"*[627], d. h. die nützliche Frist für die Offenbarung von Sicherheitslücken ist grundsätzlich nicht beachtlich. Die Publizität als *„insiderrechtliche Präventivmaßnahme"*[628] schützt nur vor Missbrauch durch Marktteilnehmer mit Informationsvorsprung, nicht aber vor Missbrauch durch Ausnutzung der publizitätspflichtigen Tatsache. Die Norm schützt grundsätzlich nur die Interessen des Kapitalmarktes, nicht aber die des Unternehmens oder die Interessen gefährdeter Dritter. Allerdings ist der Emittent von der Pflicht zur Veröffentlichung nach § 15 Abs. 3 S. 1 WpHG

> *„solange befreit, wie es der Schutz seiner berechtigten Interessen erfordert, keine Irreführung der Öffentlichkeit zu befürchten ist und der Emittent die Vertraulichkeit der Insiderinformation gewährleisten kann."*

Unterstellt, die Sicherheitslücke ist eine Insiderinformation mit kurserheblicher Qualität, d. h. grundsätzlich veröffentlichungspflichtig, ist nach § 15 Abs. 3 S. 1

---

325 *Assmann,* in: Assmann/Schneider (Hrsg.), WpHG, 4. Aufl. 2006, § 15 Rd. 27.

326 Assmann/Schneider, WpHG/*Kümpel*/*Assmann*, 3. Aufl. 2003, § 15 Rd. 95.

327 Der Begriff ist entnommen bei: Druey, Information als Gegenstand des Rechts, 1995, S. 246. Zeitgerechtigkeit bedeutet, dass die Information in nützlicher Frist erfolgen muss. Übertragen auf Sicherheitslücken, ist die Veröffentlichung mit dem Schließen der Lücke abzuwägen.

328 *Assmann,* in: Assmann/Schneider (Hrsg.), WpHG, 4. Aufl. 2006, § 15 Rd. 32.

WpHG für den Zeitpunkt der Veröffentlichung durch den Emittenten folgendes abzuwägen:

Zum einen ist zu diskutieren, ob die berechtigten Interessen des Emittenten eine Beseitigung der Sicherheitslücke vor einer Veröffentlichung indizieren. Die berechtigten Interessen des Emittenten ergeben sich aus einer Interessenabwägung zwischen den Interessen des Emittenten an der „vorübergehenden Geheimhaltung" und dem Informationsinteresse der Marktteilnehmer, wobei die Interessen des Emittenten überwiegen.[329] Dies kann wohl für Sicherheitslücken angenommen werden, deren Beseitigung in kurzer Frist möglich ist, oder für die Zeit, die nötig ist, um mögliche Vorsichtsmaßnahmen zum Schutz vor Ausnutzen der Lücke treffen zu können – etwa um im Fall des Szenarios 3 die Adressierung des Zugangs der Nutzer anders zu gestalten. Keinesfalls kann es dazu führen, dass der Emittent die Beseitigung und damit die Veröffentlichung unangemessen hinauszögert, zumal § 15 Abs. 3 S. 1 WpHG nur einen zeitlichen Aufschub der Veröffentlichung gewährt („solange"). Regelmäßig wird allerdings das berechtigte Interesse an der (vorübergehenden) Geheimhaltung der Sicherheitslücke abzulehnen sein.

Zum anderen ist zu diskutieren, inwieweit tatsächlich die Vertraulichkeit der Information gewährleistet werden kann (Aspekt der „sicheren Unsicherheit"[330]). Angesichts der technischen Fähigkeiten mancher Hacker oder Cracker könnte man argumentieren, nie. Allerdings würde mit einer solch engen Auslegung gleichsam Unmögliches vom Emittenten gefordert. Vorzuziehen ist demnach ein am technisch Machbaren orientierter Ansatz. Der Tatbestand ist dahingehend auszulegen, dass der Emittent, das was in seiner Sphäre organisatorisch und technisch möglich ist, vornehmen muss. Etwa könnten betroffene Teile oder das ganze System zeitweise vom Netz genommen werden.

Festzuhalten ist, IT-Sicherheitslücken oder Schwachstellen im IT-System können Insiderinformationen sein und eine Veröffentlichungspflicht nach § 15 Abs. 1 WpHG begründen, wobei allerdings eine Einzelfallbetrachtung erforderlich ist.

II. Informationspflichten als Produktbeobachtungspflichten

Die Pflichten der Hersteller als Produzenten von Soft- und Hardware sind im Rahmen des § 823 Abs. 1 BGB unter der durch Richterrecht entwickelten Fall-

---

329 *Assmann,* in: Assmann/Schneider (Hrsg.), WpHG, 4. Aufl. 2006, § 15 Rd. 155.

330 Vgl. Kapitel 3 B.

gruppe der Produzentenhaftung als Konstruktions-, Fabrikations-, Instruktions- und Produktbeobachtungspflichten konturiert.[331] Fraglich ist, ob sich diese Pflichten auf die Anbieter von Webseiten übertragen lassen. Zur Vorbereitung werden zunächst die Produzentenpflichten für die Hersteller von Software vorangestellt. Soweit IT spezifische Besonderheiten bestehen, werden diese dargelegt.

1. Pflicht der Hersteller sich und den Nutzer zu informieren

Hier soll die Produzentenpflicht konkretisiert auf die Produktbeobachtungspflicht dargestellt werden. Voraussetzung ist jedoch, dass die Komponenten des Internets, namentlich die Hard- und Software als Produkt im Sinne der deliktischen Produzentenhaftung verstanden werden können. Während sich das Produkthaftungsgesetz in § 2 ProdHaftG auf bewegliche Sache beschränkt,[332] ist die Frage der Verkörperung für die deliktische Produzentenhaftung nicht relevant, die auf die innewohnende Gefahr für Rechtsgüter abstellt.[333] Durch Sicherheitslücken in Software kann etwa bei Absturz der Software der Datenbestand auf dem Rechner gelöscht werden. Insoweit wäre das Eigentum als in § 823 Abs. 1 BGB geschütztes Rechtsgut verletzt.[334]

Da es als gefestigt angesehen werden kann, dass Software und Programme neben der Hardware – letztere unzweifelhaft als bewegliche Sache – als Produkt der Produzentenhaftung unterliegt,[335] soll hier nur auf die Besonderheiten der Ausprägungen der Produktbeobachtungspflichten für Software eingegangen werden.[336]

---

331 Zur Produzentenhaftung: MünchKommBGB/*Wagner,* § 823 Rd. 547 ff.; Palandt, 65. Aufl. 2006, § 823 Rd. 165 ff.; Erman-*Schiemann*, § 823 Rd. 108. Konzentriert auf die Produktbeobachtung: Michalski, Produktbeobachtung und Rückrufpflicht, in: BB 1998, 961.

332 Soweit die Elektrizität erfasst wird, stellt dies eine nicht analogiefähige Ausnahme dar, vgl. Ausführungen bei Beckmann/Müller, Online übermittelte Informationen, in: MMR 1999, 14, (15 f.).

333 Spindler, Verschuldensabhängige Produkthaftung im Internet, in: MMR 1998, 23 (24).

334 Die Löschung von Daten auf der Festplatte wird gemeinhin als Eigentumsverletzung qualifiziert, statt vieler: Libertus, Zivilrechtliche Haftung bei Computerviren, in: MMR 2005, 507 (508).

335 Taeger, Produkt- und Produzentenhaftung, in: CR 1996, 257 (266 ff.); Spindler, a.a.O., (Fn. 333), 23 ff.; zuletzt: Spindler, Haftung und Verantwortlichkeit im IT-Recht, in: CR 2005, 741 (741 f.) m.w.N.

336 So sind etwa die Anforderungen, die an Konstruktionspflichten, d. h. die Sorgfalt der Programmierung gestellt werden können, abhängig vom Einsatzgebiet des Programms: Taeger, a.a.O., (Fn. 335), 257 (268). Daraus kann aber nicht zwingend gefolgert werden, dass ein Programm, dass von der Mehrheit der Nutzer verwendet wird, wie etwa der Browser eines

Die Produktbeobachtungspflicht ist als Konkretisierung der Verkehrssicherungspflicht in § 823 Abs. 1 BGB begründet. Die Verkehrssicherungspflicht ist Ausfluss der Idee, Schädigungen Dritter zu verhindern.[337] Durch eine unterlassene Produktbeobachtung alleine kann allerdings niemandem ein Schaden entstehen. Die Produktbeobachtungspflicht ist demnach lediglich Basis für ein Spektrum von Pflichten, die sich als Konsequenz aus der Produktbeobachtung ergeben und die von der Informationssammlung über Warnungen bis zu Rückrufaktionen reichen können.[338] Im Rahmen der Informationssammlung lässt sich zwischen der aktiven und passiven Produktbeobachtung unterscheiden. Ob die Pflicht darauf beschränkt ist, Beschwerden von Kunden entgegenzunehmen (passiv) oder ob Informationen initiativ generiert werden müssen (aktiv), ist eine Frage des Gefahrenpotenzials des Produkts (Grad der drohenden Gefahr, neues/bewährtes Produkt).[339] Soweit eine aktive Pflicht gefordert ist, kann sich diese in laufenden Überwachungen durch Produkttests, Literaturrecherche, Unfallanalysen, etc. niederschlagen.[340]

Im Folgenden konzentriert sich die Ausführung zunächst auf die Produktbeobachtungspflichten der Hersteller von Soft- und Hardware als potenzielle Pflichten, sich und den Nutzer zu informieren. Im Anschluss daran wird zur Pflicht zum Rückruf durch Patches Stellung genommen.

Eine Warnung kommt als geeignete Reaktion für bereits verkaufte Produkte in Betracht, wenn dem Nutzer Gesundheitsschäden oder erhebliche materielle Einbußen drohen.[341] Grundsätzlich sind die Nutzer über drohende Gefahren in Kenntnis zu setzen, damit sie in Eigenverantwortung handeln und die Gefahrensteuerung übernehmen können.[342]

---

führenden Herstellers, besonders hohen Sorgfaltsanforderungen genügen muss. Eine solche Annahme würde primär die Quantität der Rechtsgutsverletzungen berücksichtigen, im Einzelfall muss aber die Qualität der Rechtsgutsverletzungen festgestellt werden.

337 MünchKommBGB/*Wagner,* § 823 Rd. 230; Erman-*Schiemann*, § 823 Rd. 119.

338 MünchKommBGB/*Wagner,* § 823 Rd. 597.

339 MünchKommBGB/*Wagner,* § 823 Rd. 599. Die Entscheidung basiert auf den allgemeinen Regeln der Bewertung des Umfangs und Inhalts der Verkehrssicherungspflichten, Kriterien sind hierbei das *„Ausmaß der drohenden Schäden"* und der *„Grad der Realisierbarkeit",* vgl. a.a.O., Rd. 249.

340 Erman-*Schiemann*, § 823 Rd. 119; Michalski, Produktbeobachtung und Rückrufpflicht, in: BB 1998, 961 (963 f.).

341 Erman-*Schiemann*, § 823 Rd. 119.

342 MünchKommBGB/*Wagner,* § 823 Rd. 603 mit Hinweisen auf die Rechtsprechung. Konkret zu den Anforderungen an Warnhinweise bei Softwarefehler: Spindler, Das Jahr 2000-Problem, in: NJW, 1999, 3737, (3739 f.).

Zeitlich abgestuft kann die Pflicht bereits bei Verdacht einer Sicherheitslücke bestehen, als sie auch erst bei Wissen um die Gefahr entstehen kann.[343] Die Art und Weise einer solchen Warnung muss grundsätzlich geeignet sein, die entsprechenden Verkehrskreise anzusprechen.[344] Der Hersteller ist demnach grundsätzlich gehalten, die Nutzer über mehrere Wege zu informieren (Computerzeitschriften, Foren, Webseite, Kundentelefon, etc.).[345] Für den Jahr 2000-Fehler wird explizit festgestellt:

> *„Warnungen in den wichtigsten Computerzeitschriften und über das Internet sind notwendig."*[346]

Das Ausmaß und der Zeitpunkt der Warnung bemesse sich an der Möglichkeit des Nutzers, (noch) Maßnahmen zur Risikovermeidung treffen zu können.[347] Teilweise wird an die zu benutzenden Medien zahlenmäßig eine hohe Anforderung gestellt.[348]

Soweit die Sicherheitslücken durch eigene Tests des Herstellers in Erfahrung gebracht worden sind, soll ihm ein Ermessen zustehen, ob er eine öffentliche Warnung ausspricht oder versucht die Lücke durch Patches zu beseitigen.[349] Dem kann entgegen gehalten werden, dass sich dies zum einen nicht ausschließt, sondern dem Hersteller kumulativ obliegen kann. Zum anderen kann die hier als „sichere Unsicherheit"[350] bezeichnete exklusive Kenntnis über die Sicherheitslücke kaum eingeschätzt und in eine Ermessensabwägung eingestellt werden. Es muss vielmehr darauf abgestellt werden, die Art und Weise der Veröffentlichung so zu gestalten („unpredictable disclosure"), dass die Sicherheitslücke nicht ausgenutzt werden kann. Hierüber entscheidet mehr das „Wie" als das „Ob" der Veröffentlichung.

Neben der Pflicht ex post zur Warnung als Ausfluss der Produktbeobachtungspflicht und Pflicht bei Sicherheitslücken den Nutzer zu informieren, unterliegen Software und Programme auch ex ante den Instruktionspflichten. Diese erstrecken sich auf die Gefahren, die bei bestimmungsgemäßer Benutzung auftreten können

---

343 Differenzierend nach der Rechtsgutverletzung: Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3147), der bei Gefahr für Leib und Leben einen ernst zu nehmenden Verdacht ausreichen lässt, während bei Sachschäden und nicht akuter Bedrohung abgewartet werden könne.

344 Spindler, Haftung und Verantwortlichkeit im IT-Recht, in: CR 2005, 741 (743).

345 Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3147).

346 Bartsch, Software und das Jahr 2000, 1998, S. 148. Die Warnung beruht nach Bartsch auf der Produktbeobachtungspflicht.

347 Bartsch, a.a.O., S. 148 f.

348 Vgl. Übersicht bei Marly, Softwareüberlassungsverträge, 4. Aufl. 2004, Rd. 1311.

349 Spindler, Haftung und Verantwortlichkeit im IT-Recht, in: CR 2005, 741 (743).

350 Vgl. Kapitel 3 B.

und auf den vorhersehbaren Fehlgebrauch.[351] Bei Sicherheitslücken in der Software ist die Abgrenzung, ob eine Gefahrneigung des Produkts vorliegt – somit Instruktionspflichten bestehen – oder eine nachträglich auftretende Gefahr eine konkrete Warnung erforderlich macht, nicht immer trennscharf möglich.[352] Dies lässt sich am Beispiel des Java-Scripts (vgl. Szenario 1) verdeutlichen. Die Eignung mittels Java-Script vom Nutzer unbemerkt Programme auf dem Client auszuführen, ist eine Funktion, die ex ante eine Instruktionspflicht erforderlich machen könnte. Soweit ein spezielles Exploit kursiert, das auf Java-Skript basiert, ist dies ein Ereignis, dass eine Warnung aufgrund der Produktbeobachtung nach sich ziehen sollte.

Ob und unter welchen Umständen den Hersteller darüber hinaus eine Pflicht zum Rückruf trifft, ist strittig. Zum Teil wird eine solche abgelehnt, da die Warnung zur Gefahrensteuerung ausreiche und eine Anerkennung einer Rückrufpflicht mit den Wertungen des Gewährleistungsrechts kollidiere.[353] Überwiegend wird eine solche Pflicht anerkannt, jedoch nach Umfang und Ausmaß differenziert.[354] Teilweise wird vertreten, eine solche Pflicht sei nur geboten, wenn Warnhinweise zur Schadensvermeidung nicht ausreichen.[355]

Fraglich ist, ob diese Pflicht zum Rückruf durch das Angebot von Updates und Patches erfüllt werden können. Da dieser eine adäquate und marktgerechte Reaktion auf fehlerhafte Software ist, kann der Hersteller damit seine Pflichten erfüllen.[356] Soweit vertreten wird, dass die Rückrufpflicht erst ab einem bestimmten Schadensausmaß in Betracht kommt, spricht dagegen, dass im Bereich der Sicherheits-

---

351 MünchKommBGB/*Wagner,* § 823 Rd. 588; Spindler, Verschuldensabhängige Produkthaftung im Internet, in: MMR 1998, 23 (27): Konkret müsse der Nutzer im Rahmen der Instruktionspflicht etwa auf die Erforderlichkeit von Anti-Viren-Programmen hinwiesen werden.

352 Die Differenzierung der Pflichten soll sich in der Beweislastverteilung auswirken. Während für die Instruktionspflichten eine Beweislastumkehr gelte, müsse den Verstoß gegen die Produktbeobachtungspflicht der Geschädigte beweisen, MünchKommBGB/*Wagner,* § 823 Rd. 611; a. A. Erman-*Schiemann*, § 823 Rd. 122.

353 Brüggemeier, Produkthaftung, in: ZHR 152 (1988), 511 (525 f.).

354 Erman-*Schiemann*, § 823 Rd. 119; MünchKommBGB/*Wagner,* § 823 Rd. 603 f. mit weiteren Hinweisen zu Literatur und Rechtsprechung. Im Weiteren legt MünchKommBGB/*Wagner,* a.a.O., Rd. 605 dar, dass die Rückrufpflicht im Zusammenhang mit der Erfüllung der Konstruktions- und Fabrikationspflichten zu beurteilen sei. Soweit diese verletzt sind, sei der Hersteller zu Rückruf und Reparatur auf eigene Kosten verpflichtetet.

355 MünchKommBGB/*Wagner,* § 823 Rd. 605.

356 So auch Taeger, Produkt- und Produzentenhaftung, in: CR 1996, 257 (270). Ob ein Zur-Verfügung-Stellen durch Downloadangebote auf der Webseite des Herstellers genüge, oder eine Kontaktaufnahme mit dem einzelnen Nutzer erforderlich ist, hänge von den Umständen des Einzelfalls ab.

lücken eine Warnung lediglich Vorstufe ist und Ziel der Produktbeobachtungspflichten letztendlich stets der Rückruf, mithin das Patch sein muss.[357] Diese Modifikation der Produzentenhaftung ist den Eigenheiten des Produktes Software geschuldet. Letztendlich wird die Gefahrensteuerung damit in die Hände der Nutzer gelegt, die Updates regelmäßig in (Eigen)Verantwortung installieren müssen. Allerdings soll der Hersteller nach einer Ansicht nicht darauf vertrauen können, dass der Nutzer bei der Installation der Software gleichzeitig der aktuelle Patch einspielt.[358] Dies kann allerdings nur dann gelten, wenn der Fehler vor dem In-Verkehr Bringen bekannt war, andernfalls ist diese Ansicht abzulehnen, da dem Hersteller eine unzumutbare Verkehrssicherungspflicht aufgebürdet würde. Soweit die Produktbeobachtungspflichten die allgemeinen Verkehrssicherungspflichten konkretisieren, schadet die (Eigen)Verantwortung des Nutzers nicht, zumal der Umfang der Verkehrssicherungspflichten auch durch *„Sorgfaltsvorkehrungen des Opfers"*[359] bestimmt werden. Zu den Kriterien und dem Zeitrahmen, in dem ein Patch bereitgestellt werden muss, vgl. Kapitel 3 D I.; Kriterien sind die Qualität der Rechtsgutsgefährdung, der mögliche Schadensumfang sowie die Vorteilsziehung des Herstellers.

Diese Pflichten sind an der Sicherheitserwartung der Durchschnittsverbraucher bzw. der konkreten Zielgruppe auszurichten.[360] Soweit ein durchschnittlicher Nutzer nicht feststellbar ist,[361] sind an den Sorgfaltsaufwand hohe Anforderungen zu stellen, da er am Schutz der *„am wenigstens informierten und damit nach der gefährdetsten Benutzergruppe"*[362], *„deren Angehörige zur eigenverantwortlichen Gefahrensteuerung am wenigsten in der Lage sind"*[363], zu orientieren ist.

Die obigen Ausführungen setzen voraus, dass die Information über die Sicherheitslücke sicherheitserhöhendes Potenzial hat. Die Entwicklung bei dem Inter-

---

357 Noch offen gelassen: Spindler, Haftung und Verantwortlichkeit im IT-Recht, in: CR 2005, 741 (743).

358 Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3147).

359 MünchKommBGB/*Wagner,* § 823 Rd. 251.

360 MünchKommBGB/*Wagner,* § 823 Rd. 574 f.; Taeger, a.a.O., (Fn. 356), 257 (269).

361 Vgl. Kapitel 3 C I.

362 V. Westphalen, Produzentenhaftung, in: v. Westphalen/Langheid/Streitz (Hrsg.), Der Jahr 2000 Fehler, 1999, S. 269, Rd. 803.

363 MünchKommBGB/*Wagner,* § 823 Rd. 574, konkret ist dies wohl der Nutzer, der sich ohne technisches Know-how auf die voreingestellte Funktionsfähigkeit der Software verlässt und keine eigenen Konfigurationen etwa bei den Sicherheitseinstellungen vornimmt. Dagegen steht Spindler bei uneinheitlichen Verbrauchererwartungen dem Hersteller ein *„Anpassungsermessen bei Wandel des Gefahrenbewusstseins und bei neuen technischen Entwicklungen"* zu, Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3147).

netwurm Sasser zeigt, dass mit der Veröffentlichung der Sicherheitslücke auch kontraproduktiv herausgefordert werden kann, dass diese ausgenutzt wird. Diese Wirkung ist bei der konkreten Bestimmung der Verkehrssicherungspflicht im Einzelfall abzuwägen.[364] Abzuwägen sei, ob eine öffentliche Warnung erforderlich oder individuelle Warnungen der Nutzer möglich oder die Hinweise Dritter sich auf die Lücke mehren.[365] Dabei wird nicht auf die Frage eingegangen, welche Pflichten den Hersteller treffen, wenn kein Patch erstellt werden kann. In diesem Fall ist mit der sicheren Unsicherheit[366] zu vertreten, dass der Verbraucher in jedem Fall in Kenntnis zu setzen ist.

Abschließend kann festgehalten werden, dass den Herstellern von Soft- und Hardware mit der Produktbeobachtungspflicht – gerade wegen der *„objektiven Unvermeidbarkeit von Programmierungsfehlern (…) eine Pflicht (…) zur besonders sorgfältigen Produktbeobachtung"*[367] – eine Pflicht zur Warnung und zum Rückruf (Patch) treffen kann. Zusätzlich kann ihm ex ante eine Instruktionspflicht für spezifische Gefahren beim Einsatz einer bestimmten Software obliegen. Im Folgenden soll nun diskutiert werden, inwieweit sich die so bestimmte Produktbeobachtungspflicht des Herstellers von Hard- und Software auf IT-Systeme und damit die Anbieter[368] übertragen lässt.

2. Pflicht der Anbieter sich und den Nutzer zu informieren?

Fraglich ist, ob Anbieter einer Webpräsenz und von interaktiven Webseiten sich entsprechend der Produktbeobachtungspflicht aus § 823 Abs. 1 BGB über Sicherheitslücken informieren müssen. Hätte etwa der Inhaber des Online-Versandshops im Szenario 3 eine Produktbeobachtungspflicht gehabt, seinen Webauftritt auf Sicherheitslücken laufend zu untersuchen und zu kontrollieren?

Könnte man die Produzentenhaftung auf den Anbieter im Internet übertragen, so könnte man auf ein von der Rechtsprechung fortentwickeltes Pflichtenkonzept – insbesondere die Konturierung der Produktbeobachtungspflichten und die etab-

364 Vgl. auch Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3147).

365 Spindler, a.a.O., (Fn. 364), 3145 (3147).

366 Vgl. Kapitel 3 B.

367 Spindler, a.a.O., (Fn. 364), 3145 (3147), der im Weiteren ausführt, dass bei Gefahren für Leib und Leben sogar ein ernst zu nehmender Verdacht ausreiche, um eine Warnpflicht auszulösen.

368 Vgl. Kapitel 2 B III. 1. b).

lierten Erleichterungen der Beweislastverteilung zugunsten des Nutzers[369] – zurückgreifen.

In der Literatur wird die Frage der Produzentenhaftung für das Produkt Informationen im Internet diskutiert und bejaht; insofern wird die Produzentenhaftung auf Software und Programme erstreckt.[370] Soweit Programme als Produkt qualifiziert werden, könnte sich dieses auch auf die Daten der Übertragung als Information erstrecken und die Übertragung somit als Produkt betrachtet werden.[371]

Adressat der Produzentenhaftung ist primär der Hersteller.[372] Hier ist aber die mögliche Pflicht des Anbieters von Interesse. Dem Anbieter von Webseiten fällt allerdings – etwa im Fall eines Online-Shops – mehr die Rolle des Händlers als die des Herstellers zu. Diesen mit dem Hersteller gleichzusetzen, bedeutet dem Verkauf über das Internet einen derart eigenständigen Charakter einzuräumen, die es erlaubt, dieser Verkaufsmodalität produktgleich eine eigenständige Qualität zuzugestehen. Soweit dem Händler (ausnahmsweise) Produkthaftungspflichten – etwa Produktbeobachtungspflichten – auferlegt sind, so erstrecken sie sich auf das Produkt und nicht auf die Verkaufmodalität.[373] Die Verkaufmodalität ist auch nicht entsprechend einer Verpackung mit dem Produkt gleichzusetzen.[374] Allerdings können Verkaufsmodalität und Produkt verschmelzen. Bei dem Online-Verkauf von Software sind die Daten der Übertragung (Verkaufsmodalität) und das Produkt identisch. So ist es für den Nutzer unerheblich, ob ein Virus im Produkt Software übertragen wird oder dieser als Zusatz durch die Übertragung von Daten auf seinen Rechner gelangt. Das Ergebnis ist das gleiche. Im Fall des Online-Versandshops ist die Verkaufsmodalität online jedoch trennscharf von dem eigentlichen Produkt zu unterscheiden.

---

369 MünchKommBGB/*Wagner,* § 823 Rd. 608, mit weiteren Hinweisen. Im Kern werde dem Nutzer die Darlegungs- und Beweislast hinsichtlich Unternehmensinterna abgenommen.

370 Vgl. Kapitel 5 C II. 1.

371 Gesetzliche Wertungen indizieren allerdings eine Differenzierung: Die gesetzliche Wertung des Teledienstegesetzes indiziert eine Differenzierung nach inhaltlichem Angebot (Teledienst nach § 2 Abs. 2 TDG) und Übertragungsmodalität (§ 2 Abs. 4 Nr. 1 TDG).

372 MünchKommBGB/*Wagner,* § 823 Rd. 556 ff.

373 Spindler, Verschuldensabhängige Produkthaftung im Internet, in: MMR 1998, 23 (28), mit weiteren Nachweisen.

374 Diese Gleichsetzung wird für die Diskette angenommen, vgl. Beckmann/Müller, Online übermittelte Informationen, in: MMR 1999, 14, (15). In Betracht kommt eher eine Gleichsetzung mit einer (zusätzlichen) Dienstleistung, die der Anbieter eines Webauftritts erbringt. Dienstleistungen werden von der Produzentenhaftung nicht erfasst, MünchKommBGB/*Wagner,* § 823 Rd. 554.

Allerdings lässt sich der grundsätzlich auf Sachen zugeschnittene Fehlerbegriff der Konstruktions-, Fabrikations-, Instruktionsfehler auf das Angebot einer interaktiven Webseite übertragen: Soweit der (interaktive) Webauftritt mit besonderen Programm-Features gestaltet oder dieser einem Provider übertragen ist, könnte die Verantwortung für diesen arbeitsteiligen Webauftritt dem Verantwortlichen für die Seite entsprechend einer Konstruktions- und Fabrikationspflicht obliegen.[375]

Argumentativ ließe sich damit eine Produktbeobachtungspflicht der Anbieter begründen. Ergebnisorientiert stellt sich jedoch die Frage, ob die Konsequenzen der Produzentenhaftung für Anbieter erwünscht sind:

Wäre die Gestaltung und Programmierung eines Webauftritts mit der Konstruktion eines Produktes gleichzusetzen, so träfe den Anbieter eine Konstruktionspflicht mit der Folge der entsprechenden Beweislastumkehr. Er würde für Folgen von Sicherheitslücken seiner Webangebote haften, wenn er nicht beweisen könnte, dass er diese nicht verhindern konnte.[376] Findet diese Beweislastumkehr auf alle Anbieter Anwendung, so ist jeder gehalten, IT-Sicherheit nachweislich zu organisieren. Ein Ergebnis, dass zwar zu begrüßen ist, allerdings im Widerspruch zu getroffenen gesetzlichen Regelungen steht.

Bestehende gesetzliche Regelungen sehen vor, Organisationspflichten für IT-Sicherheit bisher nur komplexer verfassten Unternehmen aufzuerlegen,[377] vgl. § 91 Abs. 2 AktG und § 109 Abs. 3 TKG. Nach § 109 Abs. 3 TKG haben Betreiber von Telekommunikationsanlagen, die Telekommunikationsdienste für die Öffentlichkeit erbringen, ein Sicherheitskonzept zu erstellen. Telekommunikationsanlagen sind in § 3 Nr. 23 TKG definiert. Da dieser jedwede technische Einrichtung umfasst, die der Telekommunikation dient,[378] fällt hierunter auch der Server im Szenario 3, auf dem die Kundendaten gespeichert werden. Regelmäßig wird der Speicherplatz für die Daten des interaktiven Webauftritts bei einem Provider „ange-

375 MünchKommBGB/*Wagner,* § 823 Rd. 557 f.

376 Statt vieler: MünchKommBGB/*Wagner,* § 823 Rd. 609; Palandt, 65. Aufl. 2006, § 823 Rd. 184; BGH, Urteil v. 11.06.1996 – VI ZR 202/95, VersR 1996, 1116 (1117); BGH, Urteil v. 08.12.1992 – VI ZR 24/92. NJW 1993, 528; Michalski, Produktbeobachtung und Rückrufpflicht, in: BB 1998, 961 (962). NJW 1999, 1028. A:A: für die Verletzung der Produktbeobachtungspflicht nach Auslieferung des Produkts: diese hat der Geschädigte zu beweisen, v. Westpahlen, Das neue Produkthaftungsgesetz, in: NJW 1990, 83 (86), mit Hinweis auf: BGH, Urteil v. 17.03.1981 – VI ZR 191/79, NJW 1981, 1603; ebenso MünchKommBGB/*Wagner,* § 823 Rd. 611.

377 Im Gegensatz hierzu wird die Produzentenhaftung unterschiedslos großen und kleinen Herstellern auferlegt, MünchKommBGB/*Wagner,* § 823 Rd. 533.

378 BerlKommTKG/*Säcker,* § 3 Rd. 37.

mietet".[379] Die Erstellung des Sicherheitskonzepts obliegt demnach dem Provider und nicht dem Online-Versandshop. Ein Ergebnis, dass zu begrüßen ist, andernfalls würde wahrscheinlich – angesichts der komplexen formalen und inhaltlichen Anforderungen aus § 109 Abs. 3 S. 2 TKG[380] und der Aussicht einer Geldbuße bis zu € 1.000.000 nach § 149 Abs. 1 S. 21 und Abs. 2 S. 1 TKG – jeder Webauftritt im Keim erstickt.

Die Übertragung der Produktbeobachtungspflicht auf den Anbieter von Webseiten ist demnach abzulehnen. Aus der Ablehnung der Übertragung der Produzentenhaftung folgt allerdings nicht, dass dem Anbieter grundsätzlich keine Verkehrssicherungspflichten obliegen. Diese werden im Folgenden unter dem Aspekt der Verkehrssicherungspflicht diskutiert.

III. Informationspflichten der Anbieter als Verkehrssicherungs- und Amtspflicht

Im Folgenden soll zunächst das „Ob" einer möglichen Verkehrssicherungspflicht aus § 823 Abs. 1 BGB für staatliche und gewerbliche Anbieter gleichermaßen diskutiert werden.[381] Auf eine Verkehrssicherungspflicht der Hersteller wird nicht eingegangen, da die Produzentenhaftung als „lex specialis" insoweit als abschließend betrachtet wird.

Im darauf folgenden Punkt wird auf spezifische Aspekte staatlicher Informationspflichten als Amtspflicht eingegangen. Zu Grunde gelegt wird hierbei das Szenario 4.

Zunächst ist jedoch zu prüfen, ob eine deliktische Informationspflicht der Anbieter nicht durch die Haftungsprivilegierung des § 8 Abs. 2 TDG grundsätzlich ausgeschlossen ist.

---

379 Ohne näher auf den schuldrechtlichen Vertrag eingehen zu wollen, wird diese Leistung regelmäßig durch einen Hosting Provider erbracht.

380 Zu den Anforderungen im Einzelnen etwa BerlKommTKG/*Klesczewski,* § 109 Rd. 25 ff.

381 Ebenso für eine Gleichstellung von Unternehmen und Behörden hinsichtlich der Verkehrssicherungspflichten beim Versenden von E-Mails: Libertus, Zivilrechtliche Haftung bei Computerviren, in: MMR 2005, 507 (510); Koch, Haftung für die Weiterverbreitung von Viren, in: NJW 2004, 801 (807).

1. Haftungsprivilegierung des § 8 Abs. 2 TDG als abschließende Regelung?

Fraglich ist, ob die Haftungsprivilegierungen der Diensteanbieter in §§ 8 ff. TDG respektive §§ 6 ff. MDStV[382] eine Diskussion der Pflicht der Anbieter sich über Sicherheitslücken zu informieren von vorneherein verbietet.[383] In Betracht kommt § 8 Abs. 2 TDG:

> *„Diensteanbieter im Sinne der §§ 9 bis 11 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen (…)"*

Damit haben Anbieter für fremde Information keine Pflicht einer allgemeinen Kontrolle übermittelter oder gespeicherter fremder Informationen. Würde im Fall des Szenarios 4 die Verantwortung und Administration für die Webseiten einem externen Provider übertragen, so wäre dieser aufgrund der Privilegierung des § 8 Abs. 2 TDG nicht verpflichtet, Informationen zu überwachen.[384] Fraglich ist, ob dies auch Informationen über Sicherheitslücken erfasst.

Das TDG umfasst mit Information sämtliche „*Angaben, die im Rahmen des jeweiligen Teledienstes übermittelt oder gespeichert werden*"[385]. Erfasst sind demnach auch die Daten, die nur der Übermittlung dienen, unabhängig vom kommunikativen Inhalt und der Erkennbarkeit für den Nutzer.[386]

Die Haftungsprivilegierung soll den Anbieter angesichts seiner automatisierten Tätigkeit vor einer Kontrolle eines jeden fremden Inhalts bewahren und befreit von einer „*proaktive Suchpflicht*"[387]. Sie soll ihn hingegen nicht von Sorgfaltspflichten be-

---

382 Da für den Kern der folgenden Diskussion die Differenzierung in Tele- und Mediendienste nicht entscheidend ist, und das TDG und der MDStV insoweit inhaltsgleich sind, wird im Folgenden stellvertretend nur das TDG diskutiert.

383 Zur so genannten Vorfilterfunktion der Verantwortlichkeitsregeln im TDG: Hoffmann, Zivilrechtliche Haftung im Internet, in: MMR 2002, 284 (285); Podehl, Internetportale, in: MMR 2001, 17 (19).

384 Die Überwachungspflicht des § 8 Abs. 2 S. 1 TDG ist eine gesetzlich normierte Verteilung der Sorgfaltspflicht, Volkmann, Der Störer im Internet, 2005, S. 141. D. h. der Gesetzgeber hat die Übernahme der Sorgfaltspflicht für die Provider für einen bestimmten Bereich gesetzlich ausgeschlossen.

385 Vgl. Begründung des Entwurfs eines Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr vom 17.05.2001, BT-Drs. 14/6098, S. 23.

386 Spindler/Schmitz/Geis-*Spindler*, TDG § 8 Rd. 23; Hoffmann: Zivilrechtliche Haftung im Internet, in: MMR 2002, 284 (288); Freytag, Providerhaftung, in: CR 2000, 600 (603).

387 Freytag, Providerhaftung, in: CR 2000, 600 (606).

freien, die in seiner Sphäre liegen und ihm damit möglich sind.[388] Der sachliche Anwendungsbereich des § 2 Abs. 1 und 2 TDG indiziert zudem die Beschränkung der Überwachungsprivilegierung auf kommunikative Inhalte in Abgrenzung zu der Übermittlung des Anbieters gemäß dem § 2 Abs. 4 Nr. 1 TDG. Eine Pflicht das System auf Sicherheitslücken hin zu überprüfen, tangiert auch nicht die nicht vorzunehmende Überwachung nach § 8 Abs. 2 S. 1 TDG, da eine Überprüfung des Systems – mithin der Infrastruktur – nicht die Überprüfung und Überwachung der Inhalte impliziert.[389] Soweit Sicherheitslücken durch Mängel der Systemsicherheit entstehen, kann sich der Anbieter demnach nicht auf die Privilegierungen aus dem TDG berufen.

§ 8 Abs. 1 TDG ist für die Verantwortlichkeit von eigenen Inhalte nur von deklaratorischer Natur und gilt für Anbieter eigener und fremder Informationen.[390] Für die Diskussion von Verkehrssicherungspflichten bleibt demnach Raum, soweit Gefahren in der Sphäre des Anbieters betroffen sind, die sich aus weiteren Umständen aus dem Webauftritt an sich für andere Rechtsgüter ergeben, insbesondere für die *„Funktionstüchtigkeit und die Sicherheit der angebotenen Dienste"*[391].

2. Verkehrsicherungspflicht der staatlichen und privaten Anbieter

Die Verkehrssicherungspflichten sind als richterliche Steuerung der Gefahren einzustufen und stellen insoweit eine *„ernsthafte Handlungsanleitung"*[392] nach § 823 Abs. 1 BGB dar, die eine Verhaltenssteuerung „in operatione"[393] möglich werden lassen.

Voraussetzung für die Annahme einer Verkehrssicherungspflicht ist die Eröffnung eines Verkehrs.[394] Verkehrssicherungspflichten erfordern von jedem *„beim eigenen Tun*

---

388 Spindler/Schmitz/Geis-*Spindler*, TDG § 8 Rd. 25.

389 Insofern läuft die Annahme einer Pflicht sich über Sicherheitslücken zu informieren nicht auf eine allgemeine, unzulässige Überwachungspflicht hinaus, vgl. Spindler/Schmitz/Geis-*Spindler*, TDG § 8 Rd. 11.

390 Spindler/Schmitz/Geis-*Spindler*, TDG § 8 Rd. 1; bereits zum TDG alter Fassung: Koch, Anbieterhaftung, in: CR 1997, 193 (197).

391 Libertus, Zivilrechtliche Haftung bei Computerviren, in: MMR 2005, 507 (511); in diesem Sinne auch: Spindler/Schmitz/Geis-*Spindler*, TDG Vor § 8 Rd. 25; Soergel/*Krause*, § 823 Anh II Rd. 120, zu einer Verkehrssicherungspflicht für Computerviren; a. A. Schneider/Günther, Computervieren, in: CR 1997, 389 (391), allerdings in einer Bemerkung zum IuKDG-Entwurf.

392 Soergel/*Krause*, § 823 Anh II Rd. 11.

393 Vgl. Kapitel 4 A II. 2. b).

und Lassen die im Verkehr erforderliche Sorgfalt zu beachten."[695] Ziel ist letztlich die Kontrolle der Gefahrenquellen und Statuierung einer Fürsorgepflicht für bestimmte Rechtsgüter Dritter.[396] Anbieter schaffen durch die Bereitstellung und Nutzung der Infrastruktur des Internets eine Gefahrenquelle.[397]

Die Bestimmung der Verkehrssicherungspflicht ist die Aufgabe,

> *„in dem immer vorhandenen Netz sozialer Handlungszusammenhänge diejenigen Akteure zu identifizieren, die am Besten zur Steuerung bestimmter Gefahren in der Lage sind."*[398]

Demnach könnte den Anbieter eine Pflicht treffen, die von ihm angebotene Kommunikation im Internet als Gefahrenquelle zu steuern.[399] Beim Anbieten einer lediglich informativen Webpräsenz könnte eine Gefährdung für Rechtsgüter des Nutzers fraglich sein. Soweit personenbezogenen Daten in der Behörde oder in dem Unternehmen organisiert werden, genügt nur der Zugang eines Rechners des Behörden- oder Unternehmensintranetzes an das Internet um etwa personenbezogene Daten zu gefährden.[400] Ebenso ist bei dem Einsatz von Cookies, die auch Si-

---

394 Mit weiteren Entstehungsgründen für Verkehrspflichten über die klassischen aus Vertrag, Gesetz und Ingerenz hinaus: MünchKommBGB/*Wagner,* § 823 Rd. 223, etwa Beherrschung eines Sachbereichs, Inverkehrbringen von Sachen, Schaffung einer Gefahrenlage oder berufliche Sicherungsverantwortung.
Soweit der Anbieter Anwendungen anbietet, bei denen mit dem Datenaustausch auch die wechselseitige Gefahr besteht, von Sicherheitslücken und Schwachstellen im IT-System des anderen betroffen zu werden, eröffnet er einen Verkehr.

395 MünchKommBGB/*Wagner,* § 823 Rd. 220.

396 MünchKommBGB/*Wagner,* § 823 Rd. 223.

397 Volkmann, Der Störer im Internet, 2005, S. 142. Die (eigenverantwortliche) Nutzung dieser Gefahrenquelle scheint zwar sozialadäquat, vermag aber keinen Ausschlusstatbestand für die Annahme einer Sorgfaltspflicht des Anbieters zu begründen.

398 MünchKommBGB/*Wagner,* § 823 Rd. 225.

399 Die täglichen Virenmeldungen und Meldungen über Sicherheitslücken im Internet schließen die Sozialadäquanz der Gefahrenquelle nicht aus. Vielmehr belegen die Bemühungen um ein sicherer Internet, dass diese nicht tolerierbar ist.

400 Ein vollständiger Schutz der internen Daten vor Angriffe aus dem Internet ist nur gegeben, wenn diese in einem Intranet ohne Anbindung zum Internet geführt werden. Sobald auch „nur" eine administrative Schnittstelle des Systemadministrators zum Internet und damit ein Einfallstor besteht, ist diese „hundertprozentige" Sicherheit der Daten nicht mehr anzunehmen. Dies ist insbesondere beunruhigend, wenn keine Entscheidungsfreiheit hinsichtlich der Datenorganisation besteht. So, etwa wenn der Verbraucher keine freie Wahl hat, ob er ein Produkt in Anspruch nimmt, etwa in Bereichen der kritischen Infrastrukturversorgung wie der Strom-, Wasser- und Energieversorgung, in denen er existenziell auf die Leistung angewiesen ist, vgl. Simitis u. a., BDSG/*Simitis*, § 4a Rd. 64, 3. Im Bereich des E-Governments wird zur interaktiven Erledigung der Verwaltung der traditionelle Gang zur Verwaltung als alternativer Weg erhalten bleiben, jedoch ist abzusehen, dass aufgrund der Vergünstigungen (etwa schnellere Erledigung einer Steuererklärung mittels ELSTER) ein faktischer Zwang der staatlichen Autorität besteht.

cherheitslücken sein können,[401] eine die Schaffung einer Gefahrenquelle bei einer informativen Webpräsenz möglich.

Nach ständiger Rechtsprechung muss derjenige,

> *„der in seinem Verantwortungsbereich eine Gefahrenlage schafft oder andauern lässt, alle ihm zumutbaren Maßnahmen und Vorkehrungen treffen, um eine Schädigung anderer zu verhindern."*[402]

Nach der Rechtsprechung sind „*faktische und tatsächliche Handlungsmöglichkeiten*"[403] zumutbar und begrenzt auf solche Maßnamen, *„die ein verständiger und umsichtiger, in vernünftigen Grenzen vorsichtiger Mensch für notwendig und ausreichend hält, um andere vor Schaden zu bewahren."*[404] Diese Formel bringt die Wechselseitigkeit der Sicherungsmaßnahmen, respektive der Informationspflichten, zum Ausdruck.

Ein solches Zusammenwirken setzt voraus, dass sich jede Seite bestimmte Erwartungen hinsichtlich der Sorgfalt des anderen macht.[405] Soweit unterstellt werden kann, dass der Nutzer im tatsächlichen Umgang mit dem Internet nicht sehr sicherheitsbewusst agiert,[406] erhöht dies zunächst die Informationsanforderungen an den Anbieter. Ob sich in dem fehlenden Sicherheitsbewusstsein ein Mitverschulden realisiert, ist bei der Obliegenheit des Nutzers zu diskutieren.[407]

Kriterien der Zumutbarkeit sind weiterhin das *„Ausmaß der drohenden Schäden"* und der *„Grad der Realisierbarkeit"*[408]. Insofern erfolgt eine Abwägung im Einzelfall. Anhand dieser Kriterien soll die Pflicht der Anbieter sich und die Nutzer zu informieren als Verkehrssicherungspflicht diskutiert werden.

Von den allgemeinen Voraussetzungen des § 823 Abs. 1 BGB interessieren hier als grundsätzlich zu beurteilende Fragen die Rechtsgutverletzung, das „Ob" einer Ver-

---

401 Vgl. Kapitel 2 B II. 2. a) und Kapitel 2 B III. 1. a).

402 MünchKommBGB/*Wagner,* § 823 Rd. 230 mit Hinweisen auf die Rechtsprechung.

403 MünchKommBGB/*Wagner,* § 823 Rd. 248.

404 BGH, Urteil v. 04.12.2001 - VI ZR 447/00, NJW-RR 2002, 525 (526); ebenso BGH, Urteil v. 20.09.1994 - VI ZR 162/93, NJW 1994, 3348 (3348); BGH, Urteil v. 19.12.1989 - VI ZR 182/89, NJW 1990, 1236 (1237); vgl. MünchKommBGB/*Wagner,* § 823 Rd. 248 mit Hinweisen auf weitere Rechtsprechung.

405 MünchKommBGB/*Wagner,* § 823 Rd. 251; Raab, Die Bedeutung der Verkehrssicherungspflichten, in: JuS 2002, 1041 (1045)

406 Vgl. Kapitel 3 C I. und II.

407 Vgl. Kapitel 5 C IV.

408 MünchKommBGB/*Wagner,* § 823 Rd. 249; v. Westphalen nennt zusätzlich zur „Zumutbarkeit" das Kriterium der „Erforderlichkeit", v. Westphalen, Produzentenhaftung, in: v. Westphalen/Langheid/Streitz (Hrsg.), Der Jahr 2000 Fehler, 1999, S. 267, Rd. 796. Auf dieses Kriterium kann allerdings verzichtet werden, wenn die „Zumutbarkeit" wie dargelegt verstanden wird.

kehrssicherungspflicht und die haftungsbegründenden Kausalität. Ob und in welcher Höhe ein Schaden eingetreten ist, bleibt einer Bewertung im Einzelfall überlassen.

a) Rechtsgutverletzung

Die Sicherheitslücke müsste eines der in § 823 Abs. 1 BGB genannten Rechtsgüter verletzen.

Ausgangspunkt der folgenden Überlegungen ist eine Gleichbehandlung der Netzsicherheit mit den Fällen der Stromunterbrechungen. Bei Stromunterbrechungen ist die Anwendung des Deliktsrechts dann fraglich, wenn diese reine Vermögensschäden darstellen, mithin keine anerkannte Rechtsgutverletzung im Sinn des § 823 Abs. 1 BGB vorliegt. Fraglich ist hier, wann die Störung der Netzsicherheit als Nutzungsbeeinträchtigung oder -ausfall nur einen Vermögensschaden (etwa durch den entgangenen Gewinn mangels Nutzung des IT-Systems) zeitigt und wann sie als Eigentumsverletzung zu qualifizieren ist.

Soweit eine Stromunterbrechung keinerlei Substanzschäden verursacht, sondern bloß einen zeitweiligen Betriebsstillstand zur Folge hat, soll mit der Rechtsprechung eine Eigentumsverletzung ausscheiden.[409] Gleiches muss gelten, wenn durch die Ausnutzung einer Sicherheitslücke, die Anbindung zum Internet unterbrochen bzw. das System oder der Rechner nur „lahm gelegt" wurde.

Soweit eine Störung der Netzsicherheit möglich ist, stellt diese grundsätzlich keine Rechtsgutverletzung dar. Damit ist – selbst bei Annahme einer Verkehrssicherungspflicht nach § 823 Abs. 1 BGB – ein Haftungstatbestand nach § 823 Abs. 1 BGB nicht erfüllt. Mithin kann § 823 Abs. 1 BGB diesbezüglich keine steuernde Wirkung entfalten.

Soweit wie in Szenario 3 die Daten der Kunden kompromittiert sind, kommt eine Verletzung des informationellen Selbstbestimmungsrechts als sonstiges Recht in § 823 Abs. 1 BGB in Betracht. Soweit in Szenario 2 der Inhalt von E-Mail einsehbar ist, kommt eine Verletzung des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG re-

[409] MünchKommBGB/*Wagner,* § 823 Rd. 114; mit Hinweis auf BGH, Entscheidung v. 25.01.1977 – VI ZR 29/75, NJW 1977, 1147; BGH, Entscheidung v. 09.12.1959 – VI ZR 199/57, NJW 1959, 479 (481). Mit der Literatur ist auch eine Nutzungsbeeinträchtigung eine Eigentumsverletzung, wenn die Nutzung nicht etwa unerheblich beeinträchtigt ist. Allerdings gehen die Kriterien der Literatur am eigentlichen Grund für die Ausklammerung der Vermögensschäden, die Ausuferung der Haftung zu verhindern, vorbei, vgl. MünchKommBGB/*Wagner,* § 823 Rd. 117.

spektive § 88 Abs. 1 TKG in Betracht.[410] Soweit in Szenario 4 infolge der Manipulation der Webseite die Rückkehr und Planung des Berufes mithin bloße Erwerbsaussichten betroffen sind, ist kein Rechtsgut i.S.d. § 823 Abs. 1 BGB betroffen.[411]

Fraglich ist, ob das Recht auf informationelle Selbstbestimmung ein absolutes Recht i.S.d. § 823 Abs. 1 BGB ist. Das allgemeine Persönlichkeitsrecht ist als sonstiges Recht i.S.d. § 823 Abs. 1 BGB grundsätzlich anerkannt.[412] Soweit dieses als Recht beschrieben wird, selbst bestimmen zu können, inwieweit Informationen über die eigene Persönlichkeit Dritten zugänglich gemacht werden,[413] umfasst § 823 Abs. 1 BGB auch das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis.[414]

Festzuhalten ist, eine Rechtsgutverletzung ist im Rahmen der Verkehrssicherungspflicht primär als Offenlegung von personenbezogen Daten mithin als Verletzung des informationellen Selbstbestimmungsrechts oder des Fernmeldegeheimnisses mithin eines sonstigen Rechts im Sinn des § 823 Abs. 1 BGB denkbar. Bei Verletzung der Netzsicherheit liegt regelmäßig keine Rechtsgutverletzung vor.

---

410 Soweit die Daten vom Empfänger zur Kenntnis genommen wurden, endet grundsätzlich der Schutz durch das Fernmeldegeheimnis, vgl. Umbach/Clemens/*Schmidt* Grundgesetz Kommentar, Art. 10 Rd. 67. Soweit der Inhalt der E-Mail allerdings auf dem Server des Providers gespeichert bleibt, und jederzeit erneut abrufbar ist, kann sich der Schutz nicht bis zur ersten Kenntnisnahme erstrecken, sondern muss sich auf jede Kenntnisnahme Dritter erstrecken, da es für den Schutz der Vertraulichkeit des Kommunikationsvorgangs nicht erheblich sein kann, ob der Empfänger den Inhalt kennt.

411 MünchKommBGB/*Wagner,* § 823 Rd. 169. Soweit durch die Fehlinformation nicht rechtzeitig ein Kindergartenplatz erlangt werden kann, kämen die Kosten der alternativen Kinderbetreuung (abzüglich der ersparten Kindergartengebühren) oder die entfallenen Einnahmen wegen eines (verspäteten) Berufswiedereintritt als Schaden in Betracht.

412 Bamberger/Roth-*Bamberger* § 832 Rd. 2.

413 Bamberger/Roth-*Bamberger* § 832 Rd. 47.

414 Vgl. OLG Düsseldorf, Entscheidung v. 11.05.2005 - 15 U 196/04, NJW 2005, 2401 (2402); OLG Karlsruhe, Entscheidung v. 10.01.2005 - 1 Ws 152/04; Bamberger/Roth-*Bamberger* § 832 Rd. 49; a. A. BGH, Urteil v. 19.05.1981 – VI ZR 273/79, NJW 1981, 1738 (1740), der über das BDSG hinaus Ansprüche nach § 823 Abs. 1 BGB infolge unzulässiger Datenverarbeitung verneint; AG Freiburg, Beschluss v. 29.10.1996 – 5 C 1200/96, NJW-CoR 1996, 386, durch die Möglichkeit des Missbrauchs der Daten wird das allgemeine Persönlichkeitsrecht noch nicht i.S.d. § 823 BGB verletzt.

b) Verkehrssicherungspflicht

aa) Verkehrssicherungspflicht sich zu informieren

In der Literatur wurde eine Verkehrssicherungspflicht andere vor Viren zu schützen diskutiert. Fraglich ist, ob dieses Ergebnis für die Bestimmung der Informationspflichten herangezogen werden kann. Grundsätzlich sind Viren und Sicherheitslücken vergleichbar, da die Gefahr für Rechtsgüter Dritter sich bei beiden mit der Übermittlung realisiert und der Schaden identisch sein kann. Teilweise wird nur von *„rudimentären Sicherungspflichten"* für den *„Marktort"* Internet gesprochen.[415] Teilweise wird unter dem Aspekt der Zumutbarkeit eine Verkehrssicherungspflicht des Anbieters beim Versenden von E-Mails nur in der b2c Konstellation angenommen.[416] Eine rechtlich relevante Eigenverantwortung privater Nutzer wird demnach in der Kommunikation mit Unternehmen nicht gesehen.[417] Soweit der Anbieter sich an private Kunden richtet, ist er diesen gegenüber zur Informationssammlung (und Weitergabe) verpflichtet. Soweit er sich an gewerbliche Nutzer richtet, könnte er zusätzlich mit der eigenen Informationssammlung – und gegebenenfalls Weitergabe der Information – rechnen. Eine Übertragung dieses Gedankens ist allerdings nur bedingt möglich. Bei Viren sind grundsätzlich auf beiden Seiten die gleichen Schutzvorkehrungen möglich, während die Ausforschung einer Sicherheitslücke grundsätzlich in der Sphäre des Anbieters liegt. Demnach muss sowohl in der b2c- als auch b2b- und g2c- und g2g-Konstellationen die Pflicht des Anbieters sich über Sicherheitslücken zu informieren angenommen werden.

Der Umfang der Pflicht sich über Sicherheitslücken zu informieren hängt von der *„faktischen und tatsächlichen Handlungsmöglichkeit"* und dem *„Grad der Realisierbarkeit",* mithin von der technischen, personellen und organisatorischen Ausstattung des Unter-

---

415 Podehl, Internetportale, in: MMR 2001, 17 (21).

416 So für den Verkehrschutz beim Versenden von E-Mails: Koch, Haftung für die Weiterverbreitung von Viren, in: NJW 2004, 801 (806); ebenso Soergel/*Krause*, § 823 Anh II Rd. 120; ablehnend für eine b2b Konstellation etwa das LG Köln, das einem Lektorat bei nachträglichem Virenbefall einer Diskette keine Pflicht gegenüber einem Autor zur Warnung auferlegt, LG Köln, Urteil v. 21.07.1999 - 20 S 5/99, NJW 1999, 3206.

417 Hingegen soll in der b2b-Konstellation mit dem Gedanken der Vorteilsziehung ein Selbstschutz des Empfängers zugunsten des Versenders zu berücksichtigen sein, siehe Koch, Haftung für die Weiterverbreitung von Viren, in: NJW 2004, 801 (805); a. A. im Ergebnis wohl Libertus, Zivilrechtliche Haftung bei Computerviren, in: MMR 2005, 507 (509 und 512), der auch in der b2b-Konstellation die Erwartung des Empfängers hinsichtlich Vorkehrungen des Versenders unterstellt. Zur Pflicht des Nutzers sich zu informieren vgl. im Übrigen den nächsten Gliederungspunkt.

nehmens oder der Behörde ab. Soweit die Verkehrssicherungspflicht so geprägt ist, kann diese sich nicht an der tatsächlichen vorhandenen technischen, personellen und organisatorischen Ausstattung im Einzelfall orientieren. Vielmehr ist es faktisch und tatsächlich möglich, die Administration und IT-Sicherheit der Webseite bei fehlenden technischen, organisatorischen und personellen Kapazitäten auszulagern. Hier besteht eine Verantwortlichkeit, den Provider sorgfältig auszusuchen und zu überwachen,[418] mithin kann der Anbieter sich über die Zwischenschaltung eines Providers nicht seiner Informationspflichten entledigen; diese wohl aber reduzieren.

Soweit eine gesetzliche oder vertragliche Pflicht besteht, Daten weiterzugeben – etwa an den Staat nach § 112 TKG oder nach § 9 WpHG – ist darüber hinaus denkbar, dass zusätzlich die Pflicht zur Weitergabe der Daten bei Vorliegen einer Sicherheitslücke suspendiert werden muss, bis der Schutz der Daten wieder gewährleistet werden kann.

Als Ergebnis kann festgehalten werden, dass zumindest gewerbliche und staatliche Anbieter in die Pflicht genommen werden können, Schutzvorkehrungen vorzuhalten und sich über Sicherheitslücken zu informieren.

bb) Verkehrssicherungspflicht zu informieren

Fraglich ist, inwieweit eine Verkehrssicherungspflicht besteht, den Nutzer über Sicherheitslücken zu informieren. Soweit es um personenbezogene Daten geht, ist eine solche Pflicht grundsätzlich dem Schutzauftrag des BDSG zu entnehmen. Dies bestätigt auch die Anerkennung des § 4 BDSG als ein Recht i.S.d. § 823 Abs. 2 BGB.[419] Da § 823 Abs. 2 BGB in Bezug auf die Rechtsgüter eine Präzisierungsfunktion besitzt, können die in den Schutzgesetzen niedergelegten Verhaltensstandards darüber hinaus bei der Konturierung der Verkehrssicherungspflicht berücksichtigt werden.[420] Soweit mit dem BGH ein Auskunftsrecht nach § 34 BDSG als Schutzgesetz abgelehnt wird,[421] ist dies nicht auf das Szenario 3 übertragbar; zumal ein Auskunftsrecht – wie bereits dargelegt[422] – nicht ausreichend ist, einen Schutz durch Information bei Vorliegen von Sicherheitslücken zu erreichen. Die bereits

---

418 Libertus, a.a.O., (Fn. 417), 507 (510); Koch, Haftung für die Weiterverbreitung von Viren, in: NJW 2004, 801 (807). Auch hier soll bei dem Umfang der Überwachung die technische, personelle und organisatorische Ausstattung betrachtet werden.

419 OLG Hamm, Entscheidung v. 04.04.1995 - 9 U 42/95, NJW 1996, 131 (131).

420 MünchKommBGB/*Wagner,* § 823 Rd. 319.

421 Zweifelnd BGH, Urteil v. 19.05.1981 – VI ZR 273/79, NJW 1981, 1738 (1740).

422 Vgl. Kapitel 4 A II. 2. b) am Ende.

dargelegten[423] Wertungen des BDSG indizieren vielmehr eine Pflicht zu informieren, mithin eine diesbezügliche Verkehrssicherungspflicht nach § 823 Abs. 1 BGB.

Fraglich ist, inwieweit die Interessen des Anbieters zu berücksichtigen sind. Soweit festgestellt wurde, dass IT-Sicherheitslücken als Betriebs- und Geschäftsgeheimnis der Geheimhaltung unterliegen und sogar verfassungsrechtlich geschützt sein können,[424] ist dieses im Einzelfall wohl mit dem *„Ausmaß des drohenden Schadens"*, mithin den Interessen der von den Auswirkungen der Sicherheitslücke Betroffenen abzuwägen.

Soweit sich eine Sicherheitslücke in der Verwendung unsicherer Software – etwa dem Betriebssystem des Servers – realisiert, ist fraglich, ob der Anbieter interaktiver Webseiten auf diese hinweisen muss. Kriterium ist im Einzelfall, ob diese Information – etwa bei Entwicklung eines Patches – primär sicherheitserhöhend ist, oder überwiegend als Einladung verstanden werden kann die Sicherheitslücken auszunutzen.[425] Letzteres ist eine Wirkung, die mit dem Kriterium des „*Ausmaßes des drohenden Schadens"* greifbar wird.

Soweit das Ausmaß des drohenden Schadens im Rahmen der Zumutbarkeit ein Kriterium für Annahme einer Verkehrspflicht ist, muss allerdings die Reputation des Verpflichteten bei der Bestimmung der Informationspflicht grundsätzlich unbeachtlich bleiben. Soweit diese sich in Gewinnrückgang realisiert, kann sie als ökonomisches Kriterium mit dem Ausmaß des Schadens abgewogen werden.[426]

cc) Verkehrssicherungspflicht zu informieren bei Ermöglichung eines Exploits

Soweit die Veröffentlichung einer Sicherheitslücke eine Anleitung zur Ausnutzung der Lücken bietet, mithin ein schädliches Exploit ermöglicht, könnte dies eine Verkehrssicherungspflicht die Nutzer zu informieren ausschließen, respektive ein Recht zu informieren beschränken.

---

423 Vgl. Kapitel 5 C I 1.a). Soweit die Verkehrssicherungspflicht im Ergebnis der entsprechenden Anwendung des § 33 Abs. 1 S. 1 BDSG gleichsteht, steht Art. 103 Abs. 2 GG dem nicht entgegen, da das Analogieverbot nur vor willkürlichen staatlichen Sanktionen schützt, nicht aber vor einer im Deliktsrecht begründeten Haftung.

424 Vgl. Kapitel 5 B V. 2. a).

425 Insoweit kann auf die Studie des BSI verwiesen werden: BSI, Lage der IT-Sicherheit in Deutschland 2005, S. 15 f., http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf (30.05.2006).

426 Zur Berücksichtigung finanzieller Erwägungen: MünchKommBGB/*Wagner,* § 823 Rd. 250.

Zieht man in Betracht, dass selbst ein Patch Grundlage eines Exploits sein kann,[427] so könnte dies dazu führen, dass keine Information an Dritte weitergegeben werden dürfte. Faktisch wird allerdings dem Anbieter zugemutet, einschätzen zu können, ob und inwieweit die Veröffentlichung der Sicherheitslücke durch Dritte schädlich ausgenutzt werden kann.

Diesem Handlungskonflikt des Anbieters kann mit folgenden vier Überlegungen begegnet werden. Diese Überlegungen können, kumulativ eingesetzt, die Risiken einer Veröffentlichung minimieren und können die Verkehrssicherungspflicht inhaltlich ausgestalten.

Erstens kann unter der Prämisse der technischen Bewertung eine „unpredictable Full-Disclosure“[428] die Verkehrssicherungspflicht ausgestalten. Allerdings ist dies abhängig vom technischen Sachverstand des Anbieters und verschiebt im Zweifel lediglich den Aspekt der Bewertung vom „Ob“ zum „Wie“ der Veröffentlichung. Kriterien könnten hierbei die Verbreitung und die grundsätzliche Fehlerneigung, sowie das Alter der Software – respektive die Fortentwicklung neuer Versionen – sein.

Zweitens kann der Anbieter im Zweifel verpflichtet sein, stets zu veröffentlichen, da nur so die Eigenverantwortung des Nutzers ermöglicht wird. Diese Lösung entlastet den Anbieter von seinen Sorgfaltspflichten, die Gefahrenquelle tatsächlich zu beherrschen und verschiebt die Verantwortung allein auf den Nutzer. Allerdings wird die Verkehrssicherungspflicht durch die Möglichkeit des Selbstschutzes Dritter bestimmt.[429] Insofern ist es zu rechtfertigen, dass der Beitrag des Anbieters zur Verhinderung der Ausnutzung der Sicherheitslücke – die unter dem Aspekt der „sicheren Unsicherheit“[430] stets möglich ist – mit der Information über diese endet. Entsprechend kann absolute Sicherheit nicht vom Anbieter verlangt werden.[431] Vielmehr soll die Offenbarung der Sicherheitslücke gerade Basis des Nutzers sein, sich selbst schützen zu können. Soweit der Nutzer sich durch Maßnahmen selbst schützen kann – etwa wie im Fall des Sasser mit der Installation des Updates[432] – hat er das Risiko einer missbräuchlichen Ausnutzung der Information zu übernehmen.

---

427 So etwa im Fall Sasser, vgl. Tatbestand bei LG Verden, Urteil v. 08.07.2005 – 3-5/05.

428 Vgl. Kapitel 3 B.

429 Soergel/*Krause*, § 823 Anh II Rd. 30.

430 Vgl. Kapitel 3 B.

431 Soergel/*Krause*, § 823 Anh II Rd. 30.

432 Vgl. Darlegung des Sachverhaltes und der Fundstellen in der Einleitung, a.a.O., (Fn. 3).

Drittens kann der Konflikt dogmatisch auf der Ebene der Zumutbarkeit gelöst werden.[433] Folgender Überlegung liegt die Prämisse zu Grunde, dass Nutzungsbeeinträchtigungen als Vermögensschäden im Rahmen des § 823 Abs. 1 BGB wie folgt abzulehnen sind: Die Ablehnung von Vermögensschäden im Deliktsrecht ist begründet mit *„diffusen Schadensbildern, die im Streitfall schwer zu verifizieren sind und gegen die sich das Opfer leicht selbst schützen kann"*[434] und die zu einer Ausuferung der Haftung führen. Zwar ist anerkannt, dass Nutzungsbeeinträchtigungen Eigentumsverletzungen i.S.d. § 823 Abs. 1 BGB darstellen können.[435] Jedoch könnten gerade Ausfälle von Computern entsprechend den reinen Vermögensschäden zu behandeln sein.

Das Ausnutzen einer offenbarten Sicherheitslücke durch ein Exploit kann in quantitativer Hinsicht jenen diffusen Schadensbildern, die im Streitfall schwer zu verifizieren und vor allem zu quantifizieren sind, entsprechen; etwa wenn das Ausnutzen eines Buffer Overflows zu einem beständigen Hoch- und Runterfahren des Betriebssystems und damit zu einer Nutzungsbeeinträchtigung führt.

Hier drohen (Vermögens)Schäden der unterschiedlichsten Art und Höhe und damit ebenfalls eine Überflutung mit Haftungsklagen, während etwa besonders abhängige gewerbliche Nutzer sich durch entsprechende Maßnahmen selbst schützen können.[436] Kern der Argumentation ist, dass eine Steuerung durch eine Haftung keine Folge zeitige, wenn der Gesamtumfang der Haftung quantitativ und qualitativ nicht vorhersehbar sei.[437] Zudem würden solche Ansprüche Kosten verursachen, denen kein entsprechender gesellschaftlicher Nutzen gegenüberstünde.[438]

Überträgt man diese Gedanken auf die quantitativ und qualitativ unübersehbaren Folgen der Offenbarung durch ein mögliches Exploit, so bleibt die Möglichkeit der Anleitung zum Exploit aufgrund der unübersehbaren Haftung unbeachtlich. Damit ist der Anbieter davon befreit, die Folgen eines Exploits abschätzen zu müssen.

---

433 Vgl. Kapitel 5 a.a.O., (Fn. 402 und 403).

434 MünchKommBGB/*Wagner,* § 823 Rd. 117. Ausnahmen bilden die Haftung nach § 826 BGB bei Vorsatz oder nach § 823 Abs. 2 BGB bei Vorliegen eines Schutzgesetzes.

435 Auf die Darstellung der unterschiedlichen Kriterien in der Literatur kann verzichtet werden, da sie hier nicht weiterführend sind. Vgl. MünchKommBGB/*Wagner,* § 823 Rd. 115 ff. mit einem Überblick über die unterschiedlichen Kriterien in der Literatur.

436 MünchKommBGB/*Wagner,* § 823 Rd. 118. Zu denken ist hier an eine redundante Stromversorgung, bzw. durch redundante Client und Server. Auf den privaten Nutzer lassen sich diese Selbstschutzaspekte in dieser Reichweite allerdings nicht übertragen.

437 Koziol, Generalnorm und Einzeltatbestände als Systeme einer Verschuldenshaftung, in: ZEuP, 1995 359 (363); MünchKommBGB/*Wagner,* § 826 Rd. 16.

438 MünchKommBGB/*Wagner,* § 823 Rd. 117.

Soweit keine anderen Rechtsgüter betroffen sind, hat der Anbieter damit bei Nutzungsbeeinträchtigungen im Ergebnis keine Verkehrssicherungspflicht.

Viertens erscheint regelmäßig eine Lösung über die Zwischenschaltung eines professionellen Sachverstandes indiziert. Soweit es nicht möglich ist, die Folgen der Offenbarung abzuschätzen, gilt: Erst durch die Einschaltung von Fachleuten ist eine Steuerung der Gefahr möglich.[439] In den Fällen des Zweifels könnte der Anbieter seiner Verkehrssicherungspflicht durch die Zwischenschaltung eines CERT genügen. In Betracht kommt etwa das CERT des BSI. Dieses kann professionelle Hilfestellung und weitere Handlungsvorgaben bei der Veröffentlichung einer Sicherheitslücke geben, vgl. § 3 Abs. 1 Nr. 7 BSIG. Von einer derivativen Übertragung der Verkehrssicherungspflicht auf das CERT soll allerdings nicht ausgegangen werden. Soweit das CERT nur beratend tätig ist und die Entscheidung zu veröffentlichen und die Veröffentlichung dem Anbieter obliegt, soll die Frage der Verantwortlichkeit des CERT hier unberührt belieben.[440]

Festzuhalten ist, die Verkehrssicherungspflicht des Anbieters bleibt bei der Möglichkeit der Ausnutzung der Offenbarung der Sicherheitslücke durch ein Exploit grundsätzlich bestehen, soweit die Information eigenverantwortliche Reaktionen des Nutzers auf die Sicherheitslücke ermöglicht. Im Einzelfall kann und muss jedoch eine partielle Information genügen, um eigenverantwortlich Maßnahmen ergreifen zu können. Insoweit begrenzt die Möglichkeit des Exploits auch nicht ein Recht zu informieren. Das „Wie" der Offenbarung kann allerdings inhaltlich eingeschränkt oder die Zwischenschaltung eines professionellen Sachverstandes verfahrensmäßig indiziert sein. Bei bestimmten Fällen der Gefahr der Nutzungsbeeinträchtigung kann die Verkehrsicherungspflicht zu informieren auch abzulehnen sein.

c) Haftungsbegründende Kausalität

Schwierig ist im Rahmen der haftungsbegründenden Kausalität zu beweisen, dass das Unterlassen der Information für den Schaden kausal war. Dieser Beweis ob-

439 Soergel/*Krause*, § 823 Anh II Rd. 52.

440 Ob und inwieweit das CERT und der Anbieter nebeneinander verantwortlich sind, ist hier nicht auszuführen. Hier soll nur ein möglicher Lösungsansatz vorgestellt werden. Zum Träger der Verkehrssicherungspflicht bei Delegation, etwa Soergel/*Krause*, § 823 Anh II Rd. 52 ff.

liegt dem Verletzten.[441] Die Beweisführung könnte hier mit dem BGH jedoch unterbleiben: Dieser führt hinsichtlich einer möglichen Beweiserleichterung aus: Es

> *„(…) kann eine tatsächliche Vermutung dafür bestehen, dass dann, wenn auf bestimmte Gefahren deutlich und für den Adressaten plausibel hingewiesen worden ist, dies auch beachtet worden wäre."*[442]

Angesichts der Darlegungen zum Sicherheitsbewusstsein[443] ist hier allerdings wohl zu konstatieren, dass diese Beweisregelung nicht auf die Sicherheitslücken im Internet übertragen werden, bzw. der Anbieter – mit dem Verweis auf entsprechende Studien – diese Vermutung entkräften kann.[444] Nach einschlägigen Studien hat etwa die Hälfte der Nutzer bei der Nutzung des Internet kein Sicherheitsbewusstsein.[445] Der obigen Ausführung des BGH lag der Fall zu Grunde, dass es unterlassen wurde darauf hinzuweisen, dass das Dauernuckeln an einer Babyflasche bei Kindern Karies verursachen könne. Eine Übertragung der Lebenserfahrung, nichts anderes ist eine Vermutung, dass Eltern in Fürsorge für ihr Kind Herstellerhinweise penibel beachten, kann für Sicherheitshinweise bei der normalen Nutzung des Internet nicht indiziert sein. Man beachte nur den meist erfolglosen Hinweis, keine unbekannten E-Mail Anhänge zu öffnen. Demnach müsste der verletzte Nutzer im Einzelfall beweisen, dass er entsprechende Informationen beachtet hätte, ohne dass ihm eine Beweiserleichterung zu Hilfe stünde.

d) Ergebnis

Festzuhalten ist, dass staatlichen und gewerblichen Anbietern eine Verkehrssicherungspflicht trifft, sich über Sicherheitslücken zu informieren und den Nutzer zu informieren. Der Umfang der Informationspflichten hängt u.a. von der Qualität des Nutzers und dem drohenden Schaden ab.

---

441 Palandt, 65. Aufl. 2006, § 823 Rd. 183; MünchKommBGB/*Wagner,* § 823 Rd. 614.

442 So die Rechtsprechung für Warnungen im Rahmen der Produzentenhaftung: BGH, Urteil v. 12.11.1991 – VI. ZR 7/91, BGHZ 116, 60 (73), DB 1999, 891 (892); BGH, Urteil v. 18.10.1988 – VI ZR 94/88, VersR 1989, 155 (157), mit dem Argument, dass auf eine dahin gehende Wirkung allgemein solche Warnhinweise gründen. Diese Vermutung kann der Warnpflichtige entkräften.

443 Vgl. Kapitel 3 C I. und II.

444 Ebenso kann die Annahme einer solchen Vermutung abgelehnt werden, wenn der Geschädigte bereits über die Gefahren informiert war, OLG Karlsruhe, Urteil v. 28.04.1993 – 7 U 77/89, NJW-RR 1994, 798 (799). Gleiches gilt, wenn er sich derart unvernünftig verhält, dass er eine Warnung aller Voraussicht nach nicht beachtet hätte, OLG Köln, Urteil v. 24.10.1985 – 18 U 46/85, VersR 1987, 573 (574).

445 Vgl. Hinweis auf entsprechende Studien, Kapitel 3 C I. und II.

3. Informationspflicht als Amtspflicht

Hier sollen spezifische Aspekte der staatlichen Informationspflicht als Ausprägung einer Amtspflicht erörtert werden. Eine Amtspflicht umfasst jede persönliche Verhaltenspflicht Amtsträgers in Bezug auf seine Amtsführung.[446]

Als Anspruchsgrundlage für eine Haftung des Staates kommen § 839 BGB i.V.m. Art. 34 GG bzw. §§ 823 i.V.m. 31, 89 BGB in Betracht.[447] Beide Haftungstatbestände setzen eine zurechenbare Pflichtverletzung voraus. Da der Amtsträger die Pflicht zu gesetzmäßigem Verhalten hat, umfasst § 839 BGB auch die Beachtung der allgemeinen Verkehrssicherungspflichten aus der unerlaubten Handlung nach § 823 Abs. 1 BGB.[448] Demnach stellt ein tatbestandsmäßiger und rechtswidriger Eingriff nach § 823 BGB im Regelfall zugleich eine Amtspflichtverletzung dar.[449]

Grundsätzlich ist fraglich, ob bei dem Versagen technischer Einrichtungen überhaupt ein Handeln eines Amtsträgers vorliegt.[450] Hier steht allerdings nicht das Versagen einer technischen Einrichtung in Frage, sondern der Umgang mit dem Versagen bei Sicherheitslücken.

Im Folgenden liegt der Fokus auf der Frage, welche Amtspflichten über die Verkehrssicherungspflichten hinaus Informationspflichten des Staates begründen können, insbesondere welche Amtspflicht im Szenario 4 angenommen werden kann. Da im Rahmen der Arbeit nur diese Aspekte von Interesse sind, soll eine vollständige Prüfung eines Amtshaftungsanspruchs nicht unternommen werden. Amtspflichten können nach Gesetz begründet sein, oder auch direkt auch allgemeinen Rechtsgrundsätzen abgeleitet werden.[451] Hierunter fällt auch eine Pflicht die Amtsführung inhaltlich korrekt zu erledigen.

---

446 Soergel/*Vinke*, § 839 Rd. 108.

447 Soweit ein hoheitliches Handeln des Amtsträgers zu Grunde liegt, ist § 839 BGB i.V.m. Art. 34 GG gegenüber §§ 823 ff. BGB abschließend, Palandt, 65. Aufl. 2006, § 839 Rd. 3. Des Weiteren ist das Verhältnis der Haftung des Staates zur persönlichen Haftung des Beamten zu klären. Auf Ausführungen hierzu wird allerdings verzichtet, da der Fokus auf das Bestehen einer Pflicht gerichtet ist.

448 MünchKommBGB/*Papier* § 839 Rd. 199 für den tatbestandsmäßigen und rechtswidrigen Eingriff in § 839; Palandt, 65. Aufl. 2006, § 839 Rd. 37 f.

449 MünchKommBGB/*Papier* § 839 Rd. 199.

450 Grundsätzlich wird dies mit dem Verweis auf die Ausweitung einer öffentlich-rechtlichen Gefährdungshaftung abgelehnt, MünchKommBGB/*Papier* § 839 Rd. 139.

451 Soergel/*Vinke*, § 839 Rd. 110.

a) Amtspflicht nach § 25 VwVfG

Soweit die Stadt interaktive Angebote im Online-Verfahren zur Verfügung stellt, könnte sie aufgrund der Fürsorge- und Betreuungspflicht aus § 25 VwVfG zur Weitergabe von Information verpflichtet sein. Soweit er hierbei Verfahren wählt, die den Einsatz zusätzlicher technischer Maßnahmen, wie etwa ein Signaturverfahren, erforderlich machen, soll er über deren Anwendungsvoraussetzungen soweit informieren, dass ein *„durchschnittlich verständiger Kunde"*[452] das Angebot wahrnehmen kann. Dies ergebe sich aus seiner Fürsorge- und Betreuungspflicht nach § 25 VwVfG.[453] § 25 VwVfG setzt allerdings tatbestandsmäßig einen Antrag des Bürgers voraus. Wie bereits diskutiert, kann eine Auskunftspflicht, die aktiv-initiativ einen Antrag des Betroffenen voraussetzt, keinen effektiven Beitrag zur Vermeidung von Gefahren leisten.[454]

b) Amtspflicht als Verkehrssicherungspflicht im engeren Sinne[455]

So wie die allgemeine Straßenverkehrsicherungspflicht dem Staat für dem öffentlichen Verkehr gewidmete Straßen obliegt, kann die Fürsorge für den Datenverkehr über das Internet dem Staat aufgrund der Fürsorge für das Angebot der Nutzung des Internets und seiner zu Grunde liegende Infrastruktur übertragen werden.[456] Allerdings sind der Straßenverkehr und der Datenverkehr nur bedingt vergleichbar. Dies zeigt sich bei folgender Entscheidung.

Mit der Rechtsprechung besteht keine Verpflichtung Wildschutzzäune aufzustellen, das Aufstellen von Warnhinweisen sei ausreichend,[457] da die Straße sich grundsätzlich *„in einem dem regelmäßigen Verkehrsbedürfnis entsprechenden Zustand"*[458] befand.

---

452 E-Government-Handbuch, Rechtliche Rahmenbedingungen für E-Government, S. 32, http://www.bsi.bund.de/fachthem/egov/download/2_Recht.pdf (30.05.2006).

453 E-Government-Handbuch, a.a.O., (Fn. 452), S. 32 f.

454 Vgl. Kapitel 4 A II. 2. a) cc) und C I.

455 Verkehrssicherungspflicht kann im engeren Sinne verstanden werden als Pflicht, die durch die Teilnahme am Straßenverkehr entsteht, vgl. Erman-*Schiemann* § 823 Rd. 88. Ein Bezug an die Straßenverkehrsicherungspflichten ist eine Erinnerung an das Verständnis des Internets als Datenautobahn.

456 Ob die Verkehrssicherungspflicht als entsprechende Anwendung der Straßenverkehrssicherungspflicht oder als alternative Bezeichnung für die allgemeine Verkehrspflicht zu verstehen ist, kann dahingestellt bleiben, da diese terminologische Differenzierung keine Auswirkungen hat.

457 BGH, Urteil v. 13.07.1989 – III ZR 122/88, NJW 1989, 2808 (2809).

Unmittelbar übertragen auf den Datenverkehr ergibt sich das praxisferne Ergebnis, dass keine Schutzvorkehrungen erforderlich sind, sondern Warnhinweise ausreichen. Im Datenverkehr muss demnach schon im Rahmen der Subsumtion bei dem Kriterium differenziert werden, ob die Infrastruktur sich *„in einem dem regelmäßigen Verkehrsbedürfnis entsprechenden Zustand"*[459] befindet. Hierbei können entsprechend „*Art und Häufigkeit der Benutzung des Verkehrsweges und seine Bedeutung"* berücksichtigt werden.[460] Neben diesen Kriterien gilt für den Inhalt und den Umfang der Straßensicherungspflicht grundsätzlich folgendes:

> *„Maßgebliche Kriterien sind (…) die Grundsätze der Zumutbarkeit der Pflichterfüllung sowie der Einsichtsfähigkeit der Verkehrsteilnehmer."*[461]

Die Einsichtsfähigkeit der Verkehrsteilnehmer korreliert mit dem oben bereits berücksichtigten Sicherheitsbewusstsein der Nutzer. Dieses kann als Kriterium für den Inhalt einer Amtspflicht herangezogen werden, jedoch kann die Straßenverkehrspflicht im Wege der Analogie hier im Ergebnis keine Amtspflicht begründen.

c) Amtspflicht im Szenario 4

Fraglich ist, ob im Szenario 4 eine Amtspflicht der Stadt besteht, die Nutzer über die Sicherheitslücke zu informieren. Dem könnte entgegenstehen, dass behördliche Warnungen und Empfehlungen in den letzten Jahren gesetzlich fixiert worden sind. Hierin kann allerdings keine abschließende Konkretisierung der Amtspflichten bei Verbraucherwarnungen gesehen werden.[462]

Die Sicherheitslücke, die eine Information erforderlich macht, müsste sich in Ausübung des Amtes manifestieren.[463] Soweit die Stadt F im Szenario 4 Informationen

---

458 BGH, Urteil v. 13.07.1989 – III ZR 122/88, NJW 1989, 2808 (2808).

459 BGH, Urteil v.13.07.1989 – III ZR 122/88, NJW 1989, 2808 (2808).

460 BGH, Urteil v. 13.07.1989 – III ZR 122/88, NJW 1989, 2808 (2809).

461 MünchKommBGB/*Papier* § 839 Rd. 200. Es müssten nur „*objektiv erforderliche*" und nach „*objektiven Maßstäben zumutbare*" Maßnahmen ergriffen werden, a.a.O.,

462 Soergel/*Vinke*, § 839 Rd. 124.

463 Für die dem Internet vergleichbaren Kommunikationsmedien Post und Telekommunikation wird festgehalten, dass mit der Privatisierung der Staat durch die Nutzung dieser Medien nicht zwangsläufig in Ausübung seiner öffentlichen Gewalt handelt, MünchKommBGB/*Papier* § 839 Rd. 163 f.

über die städtischen Kindergärten bereithält, erfüllt dies die Funktion eines virtuellen Rathauses und ist damit zumindest schlicht-hoheitliche Verwaltungshandeln.[464]

Fraglich ist, welche Amtspflicht im Szenario 4 verletzt wurde. In Betracht kommen eine Amtspflicht bei Auskünften und Erklärungen und eine Amtspflicht zur Gleichbehandlung.

aa) Amtspflicht zur Erteilung richtiger Auskünfte und Erklärungen

Den Staat können, anders als bei einer Webpräsenz eines Unternehmens, bei Ausfall oder Manipulation des Inhaltes[465] andere – inhaltsbezogene – Informationspflichten treffen. Mehr als Private ist der Staat an die Richtigkeit und Sachlichkeit seiner Informationen gebunden. Eine Auskunft, die einem Bürger gegeben wird, muss *„richtig, klar, unmissverständlich und vollständig"*[466] erteilt werden. Dieser Maßstab konkretisiert die Verhaltenspflicht über das Maß der Unternehmen und Bürger auferlegten Pflichten hinaus, da das Vertrauen in die Richtigkeit staatlicher Information besonders schutzwürdig ist und Grundlage von Vermögensdispositionen sein kann.[467] Dies gilt auch, wenn keine Pflicht zur Erteilung einer Auskunft bestand.[468] Allerdings ist eine Auskunft von einem aktiv-initiativen Handeln der Bürger geprägt. Fraglich ist, ob dieser den gleichen Schutz genießt, wenn der Amtsträger sich aktiv-initiativ an den Bürger richtet. In diesem Fall muss ist der Bürger erst recht schützenswert, da die Information eine Verhaltenssteuerung des Bürgers bezwecken.

Für das Szenario 4 ist evident, dass die Informationen nicht dem inhaltlichen Maßstab genügen. Ist der Server durch das Ausnutzen einer Sicherheitslücke gehackt und die Webseite manipuliert, so ist darüber zu informieren. Durch die Einschaltung der virtuellen Verwaltung kann die Stadt F nicht davon enthoben sein, den inhaltlichen Anforderungen an eine Information an ihre Bürger zu genügen, zumal die Zuteilung der Plätze von der rechtzeitigen Anmeldung abhängt. Durch die Bestätigung der Online-Anmeldung wurde ein Vertrauenstatbestand geschaffen, den sich die Stadt F als Verantwortliche für die Webseite zurechnen lassen muss. Den

---

464 Inwieweit das Angebot der Online-Anmeldung eine verbindliche Zuteilung und damit ein Verwaltungsakt darstellt, kann hier unbeachtlich bleiben, zumal der Sachverhalt die näheren Umstände des Vertragschlusses (öffentlich-rechtlich oder privatrechtlich) nicht darlegt.

465 Vgl. „Hack" des Bundeswehrservers in Straußberg, heise news vom 20.01.2003, http://-www.heise.de/newsticker/meldung/33818 (30.05.2006).

466 MünchKommBGB/*Papier,* § 839 Rd. 218; Palandt, 65. Aufl. 2006, § 839 Rd. 41.

467 Sachs-*Bonk* Art. 34 GG Rd. 68; MünchKommBGB/*Papier,* § 839 Rd. 219.

468 Palandt, 65. Aufl. 2006, § 839 Rd. 41.

drohenden finanziellen Folgen der Haftung für diesen Vertrauenstatbestand – die Kosten einer alternativen Betreuung oder den Einkommensausfall wegen eines späteren Berufeintritts – kann die Stadt F nur durch eine Richtigstellung und einen entsprechenden Hinweis entgehen.

bb) Amtspflicht zur Gleichbehandlung

Im Szenario 4 kommt darüber hinaus eine Amtspflicht zu Gleichbehandlung der Bürger in Betracht. Soweit die Stadt durch die Veröffentlichung einen Tatbestand geschaffen hat, auf dessen Grundlage Interessenten disponieren, gebietet es das Vertrauensschutzprinzip und das verfassungsrechtliche Gleichbehandlungsgebot, dass sich dieser Tatbestand für alle realisiert.[469] Demnach gebietet es die Gleichbehandlung aller Bürger, dass wichtige Informationen gleichermaßen für alle Bürger zur Verfügung stehen, weshalb an den Schutz vor Ausfall der gesamten Infrastruktur (Netzsicherheit) im Einzelfall auch erhöhte Anforderungen zu stellen sind. Dem könnte entgegenstehen, dass durch die Manipulation der Webseite das Vertrauen in die Zusicherung eines Kindergartenplatzes mangels Kenntnis sich gerade nicht realisieren kann. Soweit allerdings alternative Betreuungskosten anfallen oder ein Einkommensausfall entsteht, sind diese Informationen und die dadurch veranlassten Dispositionen der Stadt F zuzurechnen.

d) Drittbezogenheit der Amtspflicht

Schlussendlich muss die Amtspflicht einem Dritten gegenüber bestehen. Inwieweit dies grundsätzlich bei der sicheren Organisation des IT-Systems der Fall ist, ist fraglich. Die Drittbezogenheit ist allerdings weit auszulegen. Dritter im Sinn der Vorschrift ist jeder, dessen Interessen die Amtspflicht dient.[470] Zumindest kann wohl die sichere Organisation der Daten der Bürger als drittbezogene Amtspflicht bezeichnet werden. Dies ergibt sich aus dem Zweck des BDSG, § 1 Abs. 1 BDSG. D. h. die Informationspflicht erstreckt sich zumindest auf die Betroffenen im Sinne des BDSG.

469 Soergel/*Vinke*, § 839 Rd. 125.

470 Palandt, 65. Aufl. 2006, § 839 Rd. 45.

Soweit Informationen aufgrund mangelnder Aktualisierung nachträglich unrichtig werden, wird teilweise eine Haftung ausgeschlossen, da keine Amtspflicht zur laufenden Aktualisierung der Information bestehe, da diese nicht drittschützend sei.[471]

Allerdings besteht die Amtspflicht gegenüber jedem, in dessen Interesse die Auskunft erteilt wird.[472] Gleiches muss für die Adressaten einer intendierten Verhaltenssteuerung gelten. Durch das Angebot eines interaktiven Dienstes (im Szenario 4 die Anmeldung zum Kindergarten), ergibt sich aufgrund der interaktiven Kommunikation eine Individualisierung des Handelns der Verwaltung. D. h. die Informationspflicht erstreckt sich zumindest auf die Nutzer der Online-Anmeldung. Da diese nicht konkret angeschrieben werden können, muss die Information öffentlich verbreitet werden.

Die Informationen können zudem direkt an den betroffenen Nutzer adressiert werden. Soweit eine individuelle Kommunikation über die Manipulation der Seite jedoch nicht möglich ist, kann der drohende Betreuungsengpass nur durch eine öffentliche Information etwa eine „Gegendarstellung" auf der eigenen Webseite oder anderen Medien verhindert werden indiziert sein.

e) Ergebnis

Festzuhalten ist, dass im Szenario 4 die Stadt eine Pflicht trifft, den Bürger über die Manipulation der Webseite zu informieren. Soweit durch die Fehlinformation nicht rechtzeitig ein Kindergartenplatz erlangt werden kann, kämen als Schaden die Kosten der alternativen Kinderbetreuung (abzüglich der ersparten Kindergartengebühren) oder die entfallenen Einnahmen wegen eines (verspäteten) Berufswiedereintritt in Betracht.

IV. Informationsobliegenheit der Nutzer (sich) zu informieren

Die folgenden Ausführungen beschäftigen sich mit der Schadensminimierungspflicht des Nutzers und können somit im Rahmen der Verkehrssicherungspflicht als Mitverschulden behandelt werden. Letztendlich sind diese ein Spiegelbild der

---

471 Vgl. E-Government-Handbuch, Rechtliche Rahmenbedingungen für E-Government, S. 40 und 51, http://www.bsi.bund.de/fachthem/egov/download/2_Recht.pdf (30.05.2006).

472 BGH, Urteil v. 13.06.1991 - III ZR 76/90 (KG), NJW 1991, 3027 (3027); Palandt, 65. Aufl. 2006, § 839 Rd. 41.

Verkehrssicherungspflichten der Anbieter und die rechtliche Bewertung der Selbstgefährdung des Nutzers.[473]

1. Pflicht sich zu informieren

Eine spezialgesetzliche Pflicht, Informationen aktiv zu sammeln, besteht für private Nutzer grundsätzlich nicht. Eine Verkehrssicherungspflicht des Nutzers sich zu informieren scheidet aus, da diese grundsätzlich den Schädiger treffen. Der Nutzer soll hier jedoch primär als Geschädigter betrachtet werden und als solches betreffen ihn allenfalls, wie im eingangs angerissen Punkt erörtert, Informations"pflichten" zum Selbstschutz (Obliegenheiten). Diese Einleitung erfolgt im Bewusstsein, dass Schädiger- und Opferrolle nicht immer trennscharf auf Anbieter und Nutzer zu verteilen sind. Soweit es zur Interaktion kommt, hat der Nutzer eine ambivalente Rolle, da er etwa mit virenverseuchten E-Mails (unbewusst) auch zum Schädiger werden kann.

Der Nutzer könnte zur Abwendung eines drohenden oder zur Minimierung eines eingetretenen Schadens eine Obliegenheit sich zu informieren nach § 254 Abs. 2 BGB haben; bzw. könnte ihn an dem Eintritt des Schadens ein Mitverschulden nach § 254 Abs. 1 BGB treffen. An einer Informationsobliegenheit kann gleichzeitig der Grad der zu erwartenden Eigenverantwortung gemessen werden. Insoweit können Informationsobliegenheit und Eigenverantwortung gleichgesetzt werden.

Ein Mitverschulden liegt vor, wenn der Geschädigte die Sorgfalt außer Acht lässt, *„die ein verständiger Mensch im eigenen Interesse aufwendet, um sich vor Schaden zu bewahren."*[474] Maßgeblich ist hierbei die vernünftige und allgemein übliche Verkehrsanschauung.[475] Für Schutzmaßnahmen im Rahmen des Straßenverkehrs wird etwa differenziert, ob eine entsprechende gesetzliche Pflicht besteht, etwa Sicherheitsgurte oder Schutzhelme zu tragen.[476] Ein Mitverschulden liegt nicht bereits dann vor, wenn eine Gefahrenquelle – Straße – unvermeidbar genutzt wird. Ein Mitverschulden kann allerdings in dem Umgang mit der Gefahrenquelle – etwa in der Nicht-Beachtung von Gefahrhinweisen – liegen.[477]

---

473 MünchKommBGB/*Wagner,* § 823 Rd. 310.

474 MünchKommBGB/*Oetker*, § 254 Rd. 30 mit Hinweis auf die Rechtsprechung.

475 MünchKommBGB/*Oetker*, § 254 Rd. 30.

476 MünchKommBGB/*Oetker,* § 254 Rd. 38, so werde das Nicht-Tragen eines Sturzhelms bei Fußgängern (vgl. § 21a Abs. 2 StVO) nicht nach § 254 Abs. 1 BGB berücksichtigt.

477 MünchKommBGB/*Oetker*, § 254 Rd. 63.

Übertragen auf die Pflicht sich zu informieren bzw. zu schützen, könnte man mit diesem Ansatz eine diesbezügliche Sorgfaltspflicht sich aktiv zu informieren verneinen. Soweit allerdings auf die übliche Verkehrsanschauung und damit eine allgemeine Überzeugung abgestellt wird, wäre eine Obliegenheit sich zu informieren und zu schützen in einem gewissen Rahmen zu bejahen, soweit etwa „populäre Gefahren" wie Viren berührt sind.[478] Mit steigendem Sicherheitsbewusstsein wachsen die Anforderungen, die an die Obliegenheit des Nutzers sich zu schützen gestellt werden können. Für den derzeitigen Stand, scheint es vertretbar, außer dem Virenschutz keine weiteren proaktiven Vorkehrungen als Obliegenheiten anzunehmen.

Anhaltspunkte, inwieweit dem Nutzer eine Schadensminderungspflicht sich zu informieren obliegt,[479] soll die Diskussion der Sorgfaltspflichten des Nutzers im Umgang mit dem Jahr 2000-Fehler geben. Die Diskussion um diesen Fehler kann als gelöstes technisches und rechtliches Problem der Vergangenheit Optionen für die Gegenwart und Zukunft bieten. Der Jahr 2000-Fehler resultierte aus der ungenügenden Verwendung von vierstelligen Jahreszahlen bei der Programmierung von Anwendungen. Man befürchtete, dass die Jahresumstellung zum Jahr 2000 deshalb fehlerhaft ablaufen würde und in IT-Systemen nicht kalkulierbare Schwachstellen und IT-Sicherheitsrisiken entstehen würden. Die Folgen dieses Millenium-Bugs wurden für alle Kategorien der IT-Sicherheit befürchtet und kontrovers diskutiert.[480]

Im Zuge der rechtlichen Diskussion des Jahr-2000-Fehlers wurde konstatiert, dass die Erfassung der Risiken und Einleitung der Maßnahmen zur Problembewältigung einer allgemeinen Pflicht des Softwarenutzers zum Selbstschutz entspräche.[481] Für den Jahr 2000-Fehler wurde festgestellt, dass gewerbliche Nutzer etwa Schwachstellenanalysen durchzuführen und Reserveeinrichtungen vorzuhalten ha-

---

478 Vgl. die bereits erwähnte Studie des BSI, nach der 76% in Eigenverantwortung einen Virenscanner benutzen (Tabelle 4), BSI, IT-Awareness-Monitoring – Bevölkerung, Repräsentativumfrage in der bundesdeutschen Bevölkerung zu Themen der IT-Sicherheit, September 2004; Hinweise zur Fundstelle zur Studie in den Pressemitteilungen des BSI, http://-www.bsi.de/presse/pressinf/270105ohn_Virensch.htm (30.05.2006).

479 Schadensminderungspflichten ex ante lassen sich der Kommentarliteratur nicht entnehmen. Die dort aufgelisteten Fallgruppen stellen alle schadensmindernde Maßnahmen ex post nach Eintritt des Schadens dar. Vgl. Bamberger/Roth-*Grüneberg* § 254 Rd. 31 ff.; Erman-*Kuckuk* § 254 Rd. 60 ff.; MünchKommBGB/*Oetker* § 254 Rd. 76 ff. Ex ante wird vielmehr von einer Schadensabwendungspflicht gesprochen.

480 Einen Überblick bietet Gerhard, ein Mitarbeiter des BSI, http://www.vdw-online.de/htm/public/doku/dok-14-jahr-2000-problem.htm (30.05.2006).

481 Spindler, Das Jahr 2000-Problem, in: NJW, 1999, 3737, (3744).

ben.[482] Zumindest den gewerblichen Nutzern sei es zumutbar, *„die einschlägigen, allgemein zugänglichen Informationsquellen zu nutzen und beim Hersteller Gewissheit darüber zu erlangen, ob bei ihrem genutzten Produkt ein Problem zu befürchten ist.“*[483] Diese Feststellung bezieht sich auf einen konkreten Softwarefehler, der seit geraumer Zeit bekannt war und dessen Schadensrealisierung erst zu einem konkreten Termin befürchtet wurde (Jahresumstellung 1999/2000), und ist damit nicht ohne Weiteres auf „laufende“ Informationspflichten des Alltags und auf jegliche potenzielle Sicherheitslücke und Schwachstelle im IT-System übertragbar. Übertragen werden kann diese Pflicht zudem nur bedingt auf den privaten Nutzer, dem weder die Erfahrung noch die personellen und technischen Ressourcen zur Verfügung stehen, die erlangte Information zu verwerten. Voraussetzung ist, dass der Nutzer in der Lage ist, das Sicherheitsrisiko und das Schadenspotenzial einschätzen zu können. Eine solche Erkenntnismöglichkeit wird bei einem Unternehmen[484] mit eigener IT-Abteilung regelmäßig anders einzuschätzen sein als bei einem privaten Nutzer.

Insoweit bestünde keine Obliegenheit des Nutzers, sich zu informieren. Die allgemeinen Voraussetzungen an eine Informationsobliegenheit in § 254 Abs. 2 S. 1 BGB bestätigen dieses Ergebnis. Eine Pflicht sich über Sicherheitslücken zu informieren ist als präventive Maßnahme vielmehr eine Frage der Schadensabwendungspflicht. Da eine bloße Information nicht den Schaden beeinflusst, sich somit nicht schadensmindernd auswirken kann, ist die Informationsobliegenheit im Rahmen der Schadensabwendungspflicht im weiteren Sinn zu verstehen als die „Pflicht“ sich zu schützen, § 254 Abs. 1 BGB.

Die an die Schadensabwendung anzulegenden Maßstäbe setzen voraus, dass das Opfer bessere Erkenntnismöglichkeiten als der Schädiger besitzt.[485] Da öffentliche Quellen über Sicherheitslücken beiden offen stehen und der Schädiger regelmäßig

---

482 Spindler, a.a.O., (Fn. 481), 3737, (3744); so stellte das OLG Hamm, Urteil v. 17.06.1996 - 13 U 30/96, NJW-RR 1998, 380 (381), etwa die Notwendigkeit eines Zweitdruckers fest.

483 Spindler, a.a.O., (Fn. 481),, 3737, (3744). Nicht auf den Jahr-2000-Fehler bezogen stellt das LG Kleve, Urteil v. 29.06.1995 – 7 O 17/95, CR 1996, 292 (293), fest, dass ein EDV-Fachverlag vor Auslieferung von Disketten als Beilage einer vom ihm vertriebenen Zeitschrift, die von einem externen Unternehmen dupliziert wurden, diese auf Fehler (Viren) hätte untersuchen müssen. Andernfalls sei eine Genehmigung nach § 377 Abs. 2 HGB erfolgt.

484 Bei einer Aktiengesellschaft wird auch § 91 Abs. 2 AktG in die Überlegungen zur Schadensabwehr und -minderungspflicht einzubeziehen sein.

485 MünchKommBGB/*Oetker,* § 254 Rd. 71 i.V.m. 75. Etwas anderes könnte für den Vergleich der Erkenntnismöglichkeiten der gewerblichen Nutzer gelten. Hier ist auch eine Informationsobliegenheit des Nutzers nicht unwahrscheinlich.

über bessere eigene Ressourcen zur Ausforschung verfügt, obliegt die Informationssammlung grundsätzlich dem Anbieter und nur bedingt dem privaten Nutzer.

Eine Pflicht zur vorbeugenden Datensicherung wurde im geschäftlichen Bereich vom OLG Hamm[486] vorausgesetzt. Dieses konstatierte eine Datensicherungspflicht im Unternehmen im eigenen Interesse. Bei (extern ausgeführten) Arbeiten im IT-System gingen die Daten des Unternehmens verloren. Aufgrund des Fehlens einer zuverlässigen Sicherheitsroutine nahm das Gericht ein Mitverschulden nach § 254 BGB an. Inwieweit die Entscheidung auf den privaten Nutzer übertragen werden kann, erscheint fraglich. Im Rahmen der „Dialer-Entscheidung" des BGH[487] wurde die Pflicht zur Vorbeugung abgelehnt, soweit die Vorsorge mit einem Dialerschutzprogramm zur Diskussion stand.

Diese Beispiele indizieren, dass – zumindest für den gewerblichen Kontext – „Sorgfaltspflichten" im Rahmen eines Mitverschuldens angenommen werden können. Für gewerbliche Nutzer kann sich eine Pflicht sich zu informieren zudem aus der Konkretisierung der Vorsorge- und Organisationspflicht aus § 91 Abs. 2 AktG ergeben.[488]

Weitergehend wird vertreten, dass eine Pflicht zur Erfassung der Risiken aus der *„allgemeinen Pflicht des Softwarenutzers zum Selbstschutz"*[489] bestehe. Soweit ein Schaden durch die Verletzung einer Verkehrssicherungspflicht droht, besteht eine Sorgfaltsobliegenheit, wenn Anhaltspunkte dafür erkennbar sind und man die Möglichkeit besitzt, sich auf diese Situation einzustellen.[490] Teilweise wird weitergehend sogar bei Programmen mit bekannten Sicherheitslücken angenommen, der Nutzer müsse *„dieses Programm sperren und darf es nicht mehr einsetzen, sofern er Ausweichmöglichkeiten hat, zum Beispiel bei Web-Browsern."*[491] In letzter Konsequenz könnte dies ein Entfallen

---

486 OLG Hamm, Urteil v. 01.12.2003 – 13 U 133/03, MMR 2004, 487. In diesem Urteil ging es um eine Schadensersatzforderung, wegen eines Datenverlustes infolge des Austauschs einer Festplatte an einer Datenverarbeitungsanlage. Ein solcher wurde verneint, da das Unternehmen es *„grob fahrlässig (blauäugig)"* vernachlässigte, eine eigene Datensicherung durchzuführen. Nach Ansicht des Gerichts hätte diese täglich, eine Vollsicherung mindestens einmal wöchentlich erfolgen müssen. Insoweit treffe dem Unternehmen ein Mitverschulden nach § 254 Abs. 1 BGB. Ebenfalls eine Obliegenheit zur Datensicherung annehmend, OLG Karlsruhe, Urteil v. 07.11.1995 - 3 U 15/95, NJW 1996, 200 (201). Ebenfalls zur Datensicherungspflicht u. v.: Meier/Wehlau, Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, in: NJW 1998, 1585.

487 BGH „Dialer", Entscheidung v. 04.03.2004 - III ZR 96/03, MMR 2004, 308.

488 Vgl. Kapitel 2 A II. 4. b) bb).

489 Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3149).

490 MünchKommBGB/*Oetker,* § 254 Rd. 46.

491 Spindler, IT-Sicherheit und Produkthaftung, in: NJW 2004, 3145 (3149).

des Schadensersatzes zur Folge haben. Zumindest für private Nutzer sind aber an die Ausweichmöglichkeiten hohe Anforderungen zu stellen, will man die grundsätzliche Wertung der „vorrangigen" Informationspflicht des Anbieters und Herstellers nicht ins Leere laufen lassen. Soweit etwa Sicherheitslücken alternativer Browser ebenfalls bekannt werden, besteht in einem Wechsel keine adäquate Ausweichmöglichkeit. Angesichts der Bedeutung der Browser und der generellen mangelnden Fehlerfreiheit ist ein vollkommener Verzicht ebenfalls keine adäquate und damit dem Nutzer obliegende Ausweichmöglichkeit.

Schlussendlich umfasst die Pflicht sich zu informieren als Schadensabwendungspflicht, die Pflicht die Informationen zu verwerten, mithin Patches zu installieren. Diese sind grundsätzlich zeitnah zu installieren. Das konkrete Zeitfenster ist abhängig von dem Grad der Komplexität des eigenen Systems. Der Nutzen für die Schadensabwendung muss dabei mit der Kompatibilität mit dem eigenen System abgewogen werden.

Eine Obliegenheit sich zu informieren und zu schützen besteht daher im Grundsatz. Der Umfang der Informationssammlung und der Schutzmaßnahmen ist an dem üblicherweise eingesetzten technischen und personellen Aufwand zu messen. Insoweit ist es privaten und gewerblichen Internetnutzern zumindest zumutbar, sich aus öffentlich zugänglichen Quellen über neueste für sie relevante Sicherheitslücken zu informieren und gegebenenfalls Patches zu installieren.

Festzuhalten ist, eine Obliegenheit des privaten Nutzers sich über den aktuellen Sicherheitsstandard und aktuelle Sicherheitslücken zu informieren besteht im geringen, zumutbaren Umfang und gesteigert für gewerbliche Nutzer als Verkehrssicherungspflicht bzw. Schadensminderungsobliegenheit nach § 254 BGB.

2. Pflicht zu informieren

Dem Nutzer der Software kann eine „Pflicht" zur Warnung aus der Obliegenheit zur Schadensabwehr oder –minderung nach § 254 Abs. 2 S. 1 BGB zukommen, den Hersteller oder Anbieter über Sicherheitslücken zu informieren.[492]

[492] Diese Ausführungen sind wohl eher theoretischer Natur. Ein Nutzer, der eine Sicherheitslücke in Erfahrung bringt, wird nach allgemeiner Lebenserfahrung so sicherheitsbewusst und technisch versiert sein, auch entsprechende Vorkehrungen zur Schadensvermeidung zu treffen.

Ein Vertragsverhältnis vorausgesetzt – etwa über Internetnutzung oder über Webspace mit dem Provider – obliegt es dem Nutzer als Gläubiger des Vertrages nach § 254 Abs. 2 S. 1 BGB den Schuldner *„auf die Gefahr eines ungewöhnlich hohen Schaden aufmerksam zu machen, die der Schuldner weder kannte noch kennen musste"*. Zusätzlich obliegen ihm sonstige Maßnahmen der Schadensabwendung oder –minderung. Konkretisiert als Pflicht zur Warnung, trifft den Nutzer eine Schadensabwendungspflicht allerdings nur, wenn er bessere Erkenntnismöglichkeiten als der Schädiger hat.[493] Dies ist im klassischen Verhältnis b2c und g2c regelmäßig abzulehnen, zumal dem Nutzer durch die Strafbarkeit des Hackens und das Verbot des Reverse Engineering einige Methoden des Erkenntnisgewinns versagt sind. Im b2b Verhältnis wird eine Interessenabwägung im Einzelfall stattzufinden haben, wer und im welchen Umfang als Schädiger eine Verkehrssicherungspflicht und wer als Opfer eine Obliegenheit verletzt hat.

Zudem trifft den Nutzer ein Vorwurf des Mitverschuldens nur, wenn die Verletzung der Pflicht zur Warnung ursächlich für die Entstehung des Schadens oder die Schadenshöhe war.[494] Dies ist etwa dann nicht der Fall, wenn der Hersteller die Information nicht beachtet hätte[495] oder keine Maßnahmen hätte ergreifen können.[496] Die Beweislast obliegt hierfür dem Nutzer.

Festzuhalten ist, eine „Pflicht" des privaten Nutzers den Hersteller oder Anbieter zu informieren besteht nach § 254 Abs. 2 S. 1 BGB nur im Ausnahmefall, grundsätzlich ist diese abzulehnen. Für den gewerblichen Nutzer ist im Einzelfall abzuwägen, ob ihn als Schädiger eine Verkehrssicherungspflicht oder als Opfer eine Obliegenheit trifft.

D IT-Informationsrecht am Beispiel des GPSG

Die Meldepflicht des Herstellers nach § 5 Abs. 2 GPSG und die Informationsrechte des Staates nach §§ 10 Abs. 2 und 8 Abs. 4 S. 3 GPSG wurden bewusst aus der bisherigen Systematik dieses Kapitels herausgenommen, um anhand von zusam-

493 MünchKommBGB/*Oetker* § 254 Rd. 72; Bamberger/Roth-*Grüneberg* § 254 Rd. 28; Spindler, Das Jahr 2000-Problem, in: NJW, 1999, 3737 (3743), der darauf hinweist, dass ohne die Kenntnis vom Quellcode eine bessere Erkenntnismöglichkeit fraglich ist.

494 Spindler, Das Jahr 2000-Problem, in: NJW, 1999, 3737 (3743).

495 BGH, Urteil v. 26.05.1988 - III ZR 42/87, NJW 1989, 290 (292), eine Warnpflicht soll dem Schädiger Gelegenheit geben, Gegenmaßnahmen zu ergreifen. Sind solche offensichtlich wirkungs- und aussichtslos, bedarf es keiner Warnung.

496 BGH, Urteil v. 19.09.1995 - VI ZR 226/94, VersR 1996, 380 (381).

menwirkender Informationspflichten- und rechten die Idee eines IT-Informationsrechts deutlich zu machen. Diese Darstellung impliziert die Prüfung, ob diese Normen überhaupt auf Sicherheitslücken bei der Nutzung des Internets anzuwenden sind.

In einem abschließenden Ausblick, wird angedacht, ob das GPSG eine Vorlage eines IT-Informationsrechts bieten kann. Hierbei sollen die Herausforderungen, die ein IT-Informationsrecht zu bewältigen hat, berücksichtigt werden. Diese bestehen in der rechtlichen Handhabung der Ambivalenz der Maßnahme und der Kollision mit bestehenden abgeschlossenen „Mikro-Rechtsordnungen" wie dem Urheberrecht.

I. Pflicht der Hersteller nach § 5 Abs. 2 GPSG zu informieren

§ 8 Abs. 4 S. 3 und § 5 Abs. 2 GPSG enthalten seltene gesetzliche und spezifische Regelungen zur Informationspflicht des Herstellers. Aus § 8 Abs. 4 S. 3 GPSG ergibt sich ein vorrangiges Recht und eine Pflicht der Hersteller, die Öffentlichkeit vor Gefahren zu warnen. Im Folgenden soll jedoch nur die Meldepflicht nach § 5 Abs. 2 GPSG betrachtet werden.

Im Rahmen des GPSG[497] vom 06.01.2004 besteht nach § 5 Abs. 2 GPSG[498] eine Meldepflicht der Hersteller und Erzeuger über die Produktsicherheit ihrer Verbraucherprodukte, wenn sie Anhaltspunkte dafür haben, dass von diesen eine Gefahr für Gesundheit und Sicherheit von Personen ausgeht. Diese Meldepflicht gibt den zuständigen Behörden die notwendigen Informationen, um gegebenenfalls Schutzmaßnahmen für die Nutzer ergreifen zu können.[499]

Die Meldepflicht – so sie auf IT-Sicherheitslücken Anwendung finden kann – ist im Rahmen der Arbeit aus zwei Gesichtspunkten interessant. Zum einen wäre sie eine der wenigen normierten Pflichten den Staat über IT-Sicherheitslücken zu in-

---

497 Geräte und Produktesicherheitsgesetz, BGBl. 2004 I Nr. 1, 09.01.2004, S. 2.

498 § 5 Abs. 2 GPSG: *„Der Hersteller, sein Bevollmächtigter und der Einführer haben jeweils unverzüglich die zuständigen Behörden (…) zu unterrichten, wenn sie wisse oder anhand der ihnen vorliegenden Informationen oder ihrer Erfahrung eindeutige Anhaltspunkte dafür haben, dass von einem von ihnen in Verkehr gebrachten Verbraucherprodukt eine Gefahr für die Gesundheit und Sicherheit von Personen ausgeht; insbesondere haben sie über die Maßnahmen zu unterrichten, die sie zur Abwendung dieser Gefahr getroffen haben. (…)."*

499 Hagena/Freeman/Volz, Die behördliche Meldung unsicherer Verbraucherprodukte, in: BB 2005, 2591 (2591).

formieren. Zum anderen träfe sie situativ-initiativ[500] denjenigen, der mit der Gefahr vertraut sein sollte. Nach § 5 Abs. 2 GPSG sind die zuständigen Behörden durch den Hersteller zu unterrichten, wenn Gefahren von Geräten oder Produkten für Gesundheit oder Sicherheit von Personen ausgehen. Die zuständige Behörde ist etwa in Hessen das Regierungspräsidium.[501]

Voraussetzung hierfür wäre, dass durch die IT-Sicherheitslücke ein Verbraucherprodukt unsicher wird und dadurch eine Gefahr für die Gesundheit und Sicherheit von Personen ausgeht. Soweit IT-Produkte ubiquitär eingesetzt werden, kann dieses Tatbestandsmerkmal nicht zwingend ausgeschlossen werden. Allerdings wird deutlich, dass § 5 Abs. 2 GPSG auf die gewöhnliche Sicherheitslücke im alltäglichen Kontext, die etwa lediglich ein Ausspähen von Daten erlaubt, keine Anwendung findet, da hier regelmäßig eine solche Gefahr nicht angenommen werden kann. Was aber, wenn über das bloße Ausspähen in infrastrukturkritischen Bereichen hinaus, etwa dem Stellwerk der Bahn,[502] Daten verändert werden können? Führt diese zu einem außerplanmäßigen Zusammentreffen zweier Züge, so sind Gefahren für die Gesundheit und Sicherheit von Personen nicht ausgeschlossen.

Zunächst ist fraglich, ob Soft- und Hardware Produkte im Sinne dieses Gesetzes sind. Produkte sind nach § 2 Abs. 1 GPSG technische Arbeitsmittel und Verbraucherprodukte. Technische Arbeitsmittel sind Produkte, die ausschließlich im Bereich der Arbeit und nicht beim Verbraucher verwendet werden. In der Regel dürften im Bereich der Informations- und Kommunikationstechnik die Produkte nicht ausschließlich als technische Arbeitsmittel, sondern auch als Verbraucherprodukte zu qualifizieren sein.[503]

---

500 Vgl. Kapitel 4 A II. 2. a) cc) und C I.

501 In Hessen etwa das Regierungspräsidium nach § 1 Abs. 1 Nr. 9 und 16 der Verordnung über Zuständigkeiten auf dem Gebiet des Arbeitsschutzes, der Sicherheitstechnik, der Produktsicherheit und des Medizinprodukterechts, vgl. GVBl. I Nr. 12, 2003, S. 206.

502 Seit Mitte November 2005 werden am Frankfurter Hauptbahnhof die Züge mittels digitaler Steuerungstechnik geleitet, vgl. hr-online.de vom 20.11.2005, http://www.hr-online.de/website/rubriken/nachrichten/index.jsp?rubrik=5710&key=standard_document_13380734 (30.05.2006).

503 Eine Einordnung als technisches Arbeitsmittel ist etwa denkbar für „Großrechneranlagen" und Server gewisser Speicherkapazitäten. Zweifelhaft ist allerdings das Vorliegen des Kriteriums technischer Arbeitsmittel. So wurden als Arbeitseinrichtungen im Gerätesicherheitsgesetz a. F. beispielhaft Gegenstände aufgelistet, deren Gefährlichkeit für die Sicherheit und Gesundheit von Personen aus ihrer mechanischen Beweglichkeit resultiert, ebenso Hoeren/Ernstschneider, Das neue Geräte- und Produktsicherheitsgesetz , in: MMR, 2004, 507 (507).

Verbraucherprodukte können zunächst unzweifelhaft die Hardware ab dem Netzanschluss (angefangen von Verteilerdosen über das Netzkabel bis zum Endgerät) sein[504].

Fraglich ist, ob die außerhalb der Eingriffmöglichkeit des Nutzers liegenden Netze und Server Verbraucherprodukte im Sinn des GPSG sind. Verbraucherprodukte sind nach § 2 Abs. 3 S. 2 GPSG auch sonstige Produkte, die dem Verbraucher im Rahmen von Dienstleistungen zur Verfügung gestellt werden. Damit könnten auch Netze und Server als Verbraucherprodukte zu qualifizieren sein. Allerdings setzt das zur Verfügung Stellen ein eigenes Bedienen des Gegenstandes voraus.[505] Soweit der Verbraucher nur in den Nutzen kommt, der gewerblich Dienstleister das Produkt aber benutzt, liegt demnach kein zur Verfügung stellen vor. Demnach sind Netze und Server des gewerblichen Dienstleisters grundsätzlich keine Verbraucherprodukte. Somit fällt ein wichtiger und sicherheitsrelevanter Bereich der physikalischen Infrastruktur nicht unter das GPSG.

Fraglich ist, ob Software ein Produkt im Sinne des GPSG ist.[506] *„Software dürfte vom Anwendungsbereich des Gesetzes nicht gänzlich ausgenommen sein."*[507] Diese vorsichtige Formu-

---

504 Beispielhaft werden Gegenstände „wie Laptops, Rechner, Tastaturen, Mäuse, Monitore und Drucker sowie die meisten Zubehörteile" aufgezählt, Hoeren/Ernstschneider, a.a.O., (Fn. 503), 507 (507).

505 Vgl. Begründung im Gesetzesentwurf zur Neuordnung der Sicherheit von technischen Arbeitsmitteln und Verbraucherprodukten vom 05.09.2003, BR-Drs. 631/03, S. 38; vgl auch Erwägungsgrund 9 der Produktsicherheitsrichtlinie (Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember2001 über die allgemeine Produktsicherheit, ABl. Nr. L 11, vom 15.01.2002, S. 4): die Sicherheit von Produkten, die der Dienstleister selbst zur Erbringung seiner Dienste für die Verbraucher benutzt, fällt nicht unter die Richtlinie.

506 Eine Übersicht aus der Anfangszeit der Diskussion der Frage ob „Software ein Produkt im Sinne des Produkthaftungsgesetzes" sei – vor der Beurteilung durch die Rechtsprechung, findet sich bei Reese, Produkthaftung und Produzentenhaftung für Hard- und Software, DStR 1994, 1121 (1124): E. A. Software sei ein geistiges Gut und damit keine Sache: Argumente: Software sei *„unkörperlicher Gegenstand"* (kein Gegenstand nach § 90 BGB); Software könne online übertragen werden; Software sei Immatrialgut; der wirtschaftliche Wert liegt in den gespeicherten Befehlsfolgen, nicht in der Verkörperung. A. A. Software sei ein Produkt im Sinne des Produkthaftungsgesetzes: Argumente: EG-Richtlinienkonforme Auslegung; Software sei Ware im Sinn des UN-Kaufrechts; Software sei ein industriell hergestelltes Gut; Standardsoftware habe Warencharakter; Rechtsprechung wende Sachmängelansprüche auf Software an; meistens Verkörperung auf Datenträger; Software sei vergleichbar mit Elektrizität.

507 Hoeren/Ernstschneider, a.a.O., (Fn. 503), 507 (508). Dies bleibt mehr eine These, die argumentativ kaum belegt wird: *„Das GPSG zielt nach seinem Sinn und Zweck wesentlich auf den Schutz der Sicherheit und Gesundheit von Personen vor gefährlichen körperlichen Gegenständen ab, sodass es sich bei einem Computerprogramm, zumindest sofern es sich auf einem Datenträger verkörpert, nach dem Wort-*

lierung ist wohl der fehlenden Unterstützung einer Subsumtion durch eine Auslegung der Produktsicherheitsrichtlinie[508] und der gesetzesvorbereitenden Materialen[509] sowie der Heranziehung des Gerätesicherheitsgesetzes alter Fassung und des Produktsicherheitsgesetzes alter Fassung geschuldet. Der Begründung der Regierungsvorlage zur Umsetzung der Produktsicherheitsrichtlinie in Österreich ist allerdings explizit die Anwendbarkeit bei Software zu entnehmen.[510]

Die folgenden Ausführungen konzentrieren sich auf „selbstständige Software". Soweit Software in anderen Produkten integriert ist (embedded-Software), ist sie Verbraucherprodukt im Sinne des GPSG.[511] Für die Einordnung von selbstständiger Software als Verbraucherprodukt i.S.d. § 2 Abs. 3 S. 2 GPSG spricht, dass Artikel 2 lit. b) der Produktsicherheitsrichtlinie eine begriffliche Berücksichtigung auch von Software entnommen werden kann, da danach die Verwendung eines „sicheren Produkts" auch die *„Installation"*[512] einschließt.

Der Begründung zu dem Gesetzesentwurf ist ein sehr weites Verständnis von Verbraucherprodukten zu entnehmen, *„Verbraucherprodukt kann alles sein, was aus einem Herstellungsprozess hervorgehen kann (…)."*[513]

---

laut und Zweck des Gesetzes um einen Gebrauchsgegenstand oder ein Produkt i.S.d. § 2 Abs. 3 GPSG bzw. um eine Arbeitseinrichtung i.S.d. § 2 Abs. 2 GPSG handeln dürfte."

508 Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 03. Dezember 2001 über die allgemeine Produktsicherheit, ABl. Nr. L 11, vom 15.01.2002, S. 4. Diese Richtlinie wurde mit dem GPSG umgesetzt.

509 Gesetzesentwurf zur Neuordnung der Sicherheit von technischen Arbeitsmitteln und Verbraucherprodukten vom 05.09.2003, BR-Drs. 631/03.

510 512 der Beilagen zu den stenographischen Protokollen des Nationalrates XXII. GP, S. 17 http://www.sbg.ac.at/ver/links/bgbl/xxii_mat/I00512.pdf (30.05.2006): *„Abweichend vom PSG 1994 wird die Einschränkung auf „körperliche" Sachen fallengelassen, da etwa Software durchaus sicherheitsrelevante Eigenschaften besitzen kann und mittlerweile nicht mehr nur auf „körperlichen" Datenträgern, sondern auch als Download in Verkehr gebracht wird.*"

511 Runte/Potinecke, Software und GPSG, in: CR 2004, 725 (726).

512 Mit Installation kann auch ausschließlich der traditionelle Einbau und der Anschluss von technischen Anlagen bezeichnet worden sein. In der Informationstechnik wird mit der Installation die Einrichtung und Vorbereitung der Nutzung eines Programms bezeichnet.

513 Gesetzesentwurf zur Neuordnung der Sicherheit von technischen Arbeitsmitteln und Verbraucherprodukten vom 05.09.2003, BR-Drs. 631/03, S. 41.

Der Software wird regelmäßig bescheinigt grundsätzlich fehlerhaft zu sein.[514] Soweit dies mit niedrigen Sicherheitserwartungen der Nutzer korreliert, könnte etwa das ProdHaftG für Software keine Anwendung finden, § 3 Abs. 1 ProdHaftG.[515] In der Regel äußert sich die erwartete Fehlerneigung in Programmabstürzen, d. h. in der Gebrauchstauglichkeit. Fraglich ist, ob sich das GPSG ebenfalls an den Sicherheiterwartungen der Verbraucher orientiert. Eine entsprechende explizite Regelung existiert nicht. Das GPSG orientiert sich allerdings an den tatsächlichen Auswirkungen. Soweit die fehlende Gebrauchstauglichkeit eine Gefahr für Sicherheit und Gesundheit der Verwender oder Dritter darstellt, kommt es auf die Sicherheitserwartungen nicht an. Unter dem Aspekt der Verbrauchererwartungen ist die Software demnach nicht vom GPSG ausgeschlossen.

Letztendlich wird, soweit die Literatur sich mit der Anwendung des GPSG auf Software beschäftig, eine Anwendung des GPSG bejaht.[516]

Festzuhalten ist, Hard- und Software können Verbraucherprodukte sein. Somit besteht grundsätzlich eine Pflicht der Hersteller – bei Vorliegen einer entsprechenden Gefahrenlage – die zuständige Behörde nach § 5 Abs. 2 GPSG über IT-Sicherheitslücken zu informieren. Allerdings erstreckt sich diese nicht auf wichtige Bereiche wie Server oder die Infrastruktur.

II. Recht des Staates nach §§ 10 Abs. 2 S. 1 und 8 Abs. 4 S. 3 GPSG zu informieren

Staatliche Stellen können nach §§ 8 Abs. 4 S. 3 und 10 Abs. 2 S. 1 GPSG[517] Informationen weitergeben. Solche Stellen sind nach § 8 Abs. 1 GPSG nach Landes-

---

514 Software ist regelmäßig fehlerbehaftet auch wenn sie dem Stand der Technik entspricht und einem Qualitätsmanagement unterlaufen hat. So statt vieler: Heussen, Unvermeidbare Softwarefehler, in: CR 2004, 1 (3). Nicht damit zufrieden geben will sich Bartsch, Computerviren und Produkthaftung, in: CR 2000, 721 (721 f.) der ausführt, dass bei Sicherheitsmängel regelmäßig der Stand der Technik unterschritten wäre. Die komplexer Software grundsätzlich bescheinigte Fehlerhaftigkeit könne nur für *„durch sorgfältiges Testen kaum auffindbare Sicherheitslücken diskutiert werden"* (nicht aber für die in dem Aufsatz diskutierten Defizite von Softwareprodukten eines führenden Herstellers).

515 Lutterbeck zieht den Ausschluss der Haftung für Software aus diesem Grund in Erwägung, Lutterbeck/Horns/Gehring, Sicherheit in der Informationstechnologie und Patentschutz für Software-Produkte, 2000, S. 125, Fn. 247, http://www.ipjur.com/data/LuGeHo.pdf (30.05.2006).
§ 3 Abs. 1 ProdHaftG: *„(1) Ein Produkt hat einen Fehler, wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände, insbesondere (…) berechtigterweise erwartet werden kann."*

516 Hoeren/Ernstschneider, a.a.O., (Fn. 503), 507 (508); Spindler, IT-Sicherheit, in: NJW 2004, 3145 (3148); Runte/Potinecke, Software und GPSG, in: CR 2004, 725 (727).

recht zu bestimmende „zuständigen Behörden“[518] bzw. die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin als nach §§ 10 Abs. 2 S. 1 i.V.m. 2 Abs. 14 GPSG beauftragte Stelle.

Während § 8 Abs. 4 S. 3 GPSG als Warnung im oben dargelegten Sinne normiert ist, soll § 10 Abs. 2 GPSG exemplarisch für einen Paradigmenwechsel in der staatlichen Informationstransparenz stehen.[519] Nicht nur, dass die Informationsverbreitung über das Internet angeregt wird (§ 10 Abs. 2 S. 2GPSG), es wird auch eine Pflicht des Staates erfasst,

> *„der Öffentlichkeit allgemein und anlassunabhängig die den Behörden zur Verfügung stehenden Informationen über von Verbraucherprodukten ausgehende Gefahren zugänglich zu machen (…) an die Stelle einer zur Amtsverschwiegenheit verpflichteten Behörde tritt eine Verwaltung, die forums-ähnlich das bei ihr gesammelte Wissen der breiten Allgemeinheit grundsätzlich nicht vorenthält.“*[520]

Bisher nur als eine spezielle Regelung für Verbraucherprodukte normiert, könnte die Idee der Informationstransparenz für jegliche Informationen über Sicherheitslücken und Schwachstellen im IT-System gelten. § 10 Abs. 2 S. 1 GPSG setzt ebenfalls voraus, dass die Komponenten des IT-Systems Verbraucherprodukte i.S.d. § 2 Abs. 1 GPSG sind. Wie oben bereits dargelegt, ist § 10 Abs. 2 S. 1 GPSG – fokussiert auf ihre Anwendbarkeit für Informationen über Sicherheitslücken und Schwachstellen in IT-Systemen – nur im engen Bereich anwendbar, mithin nicht für alle Teile der Infrastruktur eines IT-Systems.

§ 8 Abs. 4 S. 3 GPSG erfasst darüber hinaus technische Arbeitsmittel mithin – wie oben dargelegt – Server und Netze als Teile der Infrastruktur.

Speziell auf Produkte und Geräte zugeschnitten finden §§ 8 Abs. 4 S. 3 und 10 Abs. 2 S. 1 GS grundsätzlich keine Anwendung auf Sicherheitslücken verursacht durch Verfahren oder Akteure. Die Anwendung der §§ 8 Abs. 4 S. 3 und 10 Abs. 2

---

517 § 8 Abs. 4 S. 3 GPSG: *„Die Behörde selbst kann die Öffentlichkeit warnen, wenn andere ebenso wirksame Maßnahmen, insbesondere Warnungen durch den Hersteller, nicht oder nicht rechtzeitig getroffen werden.“*
§ 10 Abs. 2 S. 1 GSPG: „D*ie zuständigen Behörden und die beauftragte Stelle machen der Öffentlichkeit sonstige ihnen zur Verfügung stehenden Informationen über von Verbraucherprodukten ausgehende Gefahren für die Sicherheit und Gesundheit der Verwender zugänglich; dies betrifft insbesondere Informationen zur Identifizierung der Verbraucherprodukte, die Art der Gefahren und die getroffenen Maßnahmen.“*

518 A.a.O., (Fn. 501).

519 Vgl. Klindt, Das neue Geräte- und Produktsicherheitsgesetz, in: NJW 2004, 465 (471), der den Begriff Informationstransparenz verwendet. Zur Warnung des Staates, vgl. Kapitel 4 C I. 2. a).

520 Klindt, Das neue Geräte- und Produktsicherheitsgesetz, in: NJW 2004, 465 (471).
Etwa unter http://www.icsms.org (30.05.2006) werden Verbraucherwarnungen zur Verfügung gestellt.

S. 1 GPSG ist demnach nur für Soft- und Hardwarefehler als Teil der physikalischen Infrastruktur denkbar.

Ob diese Informationspflicht tatsächlich ein Absatz- und Reputationsrisiko für die Hersteller darstellt, wie teilweise vermutet wird,[521] wird durch zukünftig auftretenden und bekannt werdenden Personenschäden durch Sicherheitslücken und Schwachstellen in IT-Systemen bestimmt werden.

III. GPSG als Vorlage eines IT-Informationsrechts?

Als Ausblick sollen – ohne den Anspruch einer abschließenden Konzeption eines IT-Informationsrechts – pointiert Regelungen aufgezeigt werden, die auf Herausforderungen rekurrieren, die im Laufe der Arbeit angesprochen wurden. Ausgehend von den Meldepflichten und Informationsrechten im § 5 Abs. 2 und § 10 Abs. 2 GPSG kann die Regelungstechnik des GPSG dafür ein Anhaltspunkt sein, ist aber – wie vorangehend erläutert – nicht mit einem IT-Informationsrecht gleichzusetzen.

Durch die Ausführungen zur Meldepflicht und zum staatlichen Reaktionsrecht in § 5 Abs. 2 und § 10 Abs. 2 GPSG wurde das notwendige Zusammenwirken dieser Komponenten für ein IT-Informationsrecht deutlich gemacht. Eine effiziente und effektive Steuerung der Sicherheit durch die Veröffentlichung von Sicherheitslücken durch ein IT-Informationsrecht erfordert die Verquickung von Rechten und Pflichten. Diese Verknüpfung konkretisiert sich auch in den Pflichten des Anbieters und Herstellers zu informieren, ergänzt durch eine spiegelbildliche Obliegenheit des Nutzers sich zu informieren.

Gerade die in § 10 Abs. 2 GPSG geregelte Idee des Staates als Informationsintermediär[522] könnte mit einem (staatlichen) CERT als zuständige Behörde realisiert werden. Soweit diese, wie bereits erwähnt, die Aufgabe hat

> *„der Öffentlichkeit allgemein und anlassunabhängig die den Behörden zur Verfügung stehenden Informationen über von Verbraucherprodukten ausgehende Gefahren zugänglich zu machen (…)“*[523],

scheint dieser Weg gerade für die alltäglichen Sicherheitslücken eher geeignet als eine Warnung, da letzterer stets Sachverhalte zu Grunde liegen, die – etwa mit Gefahren für Personen – erhebliche Folgen für Rechtsgüter zeitigen.

---

521 Hoeren/Ernstschneider, a.a.O., (Fn. 503),, 507 (513).

522 Eidenmüller, Der homo oeconomicus, in: JZ 2005, 216 (221).

523 Klindt, Das neue Geräte- und Produktsicherheitsgesetz, in: NJW 2004, 465 (471).

Anhand der §§ 10 Abs. 4 und 5 Abs. 2 S. 2 GPSG kann darüber hinaus die Ambivalenz der Wirkung der Information über Sicherheitslücken und die Auswirkungen urheber- und strafrechtliche Inkriminierung für ein IT-Informationsrecht diskutiert werden.

Soweit Regelungen fehlen, die eine solche Ambivalenz von Information berücksichtigen, könnte einerseits ein entsprechender § 10 Abs. 4 Nr. 5 GPSG folgendermaßen formuliert werden:

> *„Informationen nach Absatz 2 dürfen nicht zugänglich gemacht werden, (…)*
>
> *5. soweit sie geeignet sind, insbesondere aufgrund ihrer detaillierten Programmbeschreibung, die Sicherheitslücken unmittelbar auszunutzen. Bei der Bewertung ist unter anderen auch zu berücksichtigen, inwieweit Maßnahmen zum Schließen der Lücke vorhanden sind, das qualitative und quantitative Ausmaß der möglichen Gefahren und das Zeitfenster der Entwicklung von Maßnahmen zum Schließen der Lücke."*

Andererseits könnte ein in Anlehnung an das GPSG konzipiertes IT-Informationsrecht mit grundlegenden Wertungen anderer Rechtsgebiete kollidieren. Dies soll anhand des § 5 Abs. 2 S. 2 GPSG beispielhaft ausgeführt werden. Dieser führt aus:

> *„Eine Unterrichtung nach Satz 1 darf nicht zur strafrechtlichen Verfolgung des Unterrichtenden oder für ein Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Unterrichtenden verwendet werden."*

Wie oben dargelegt, sind Hacker und selbsternannte Sicherheitstester urheberrechtlich und strafrechtlich zu sanktionieren.[524] Ob ein neues IT-Informationsrecht innerhalb solcher überkommenden Ordnungen aufzubauen ist, oder nur innerhalb eines separaten IT-Informationsrechts möglich ist, ist fraglich.[525]

Für einen Ausblick mag aber an dieser Stelle genügen, dass der Gesetzgeber notwendige Mechanismen, die etwa das GPSG regelungstechnisch zur Verfügung stellt, an der Hand hat, um auf die Herausforderungen eines IT-Informationsrechts in Zukunft zu reagieren zu können.

E Ergebnis

Grundsätzlich kann ein unbegrenztes Recht zu informieren und sich zu informieren nicht angenommen werden. Dieses ist nicht die Regel, sondern eine Ausnahme im Bereich der Informationsrechte über Sicherheitslücken und Schwachstellen des IT-Systems.

---

524 Vgl. Kapitel 5 B I. 2.

525 Dreier, „Wem gehört die Information im 21. Jahrhundert?", in: Büllesbach/Dreier (Hrsg.), Wem gehört die Information, 2004, S. 107.

So wird das „Recht“, sich mittels Reverse Engineering oder Dekompilierung über Sicherheitslücken und Schwachstellen von proprietärer Software zu informieren, regelmäßig durch das Urheberrecht eingeschränkt. Ebenso werden unaufgeforderte Sicherheitstests durch die Strafbarkeit von Hacken unterbunden.

Die Beurteilung des Rechts über Sicherheitslücken zu informieren ist grundsätzlich von der Qualität des Inhalts abhängig. Soweit ihr wahre Tatsachen zu Grunde liegen, ist eine Beschränkung jenseits von Urheberrecht und Strafrecht nur in seltenen Ausnahmefällen anzunehmen, vgl. § 17 UWG. Grundsätzlich müssen – soweit das Urheber- und Strafrecht nicht betroffen sind – selbst ruf- und geschäftsschädigende Informationen über Sicherheitslücken hingenommen werden.

Am Urheberecht lässt sich ein zentrales Spannungsverhältnis aufzeigen, das sich auch im Bereich der Information über Sicherheitslücken auswirkt. Da das Urheberrecht den Waren- und statischen Charakter von Information als Zustand betont, kann dem – der Informationsasymmetrie im Sicherheitsbereich entspringenden – Bedürfnis nach einem Informationsvorgang nicht Rechnung getragen werden. Soweit die Information für sicherheitsrelevante Fragen genutzt werden kann und muss, kann hier die Verteilungsgerechtigkeit in Frage gestellt werden.

Soweit im Arbeitsverhältnis ein gesteigertes Informationsinteresse angenommen werden kann, trägt das Gesetz diesem, etwa bei dem Recht des Arbeitgebers sich zu informieren, Rechnung und beschränkt es nur, soweit es zum Schutz entgegenstehender Interessen und Rechte erforderlich ist. Auf der anderen Seite begrenzt das Arbeitsrecht das Informationsinteresse von Dritten und der Allgemeinheit, die von Sicherheitslücken und Schwachstellen im betrieblichen IT-System betroffen sind, nicht unverhältnismäßig. Das Recht des Arbeitnehmers über Sicherheitslücken zu informieren, ist mangels gesetzlicher Regelung aus dem Umfang und der Reichweite der Pflicht zur Rücksichtnahme des Arbeitnehmers zu entwickeln. Kriterien für die Veröffentlichung von Sicherheitslücken sind:

Die Information (1) ergeht an eine (externe) zuständige staatliche Stelle, (2) die Information ist im Interesse und zum Schutz der Öffentlichkeit oder Dritter, (3) die Information ergeht erst, nachdem interne Schadensbegrenzungsversuche fehlgeschlagen sind (Abhilfebemühen) und (4) die Motivation des Arbeitnehmers für die Veröffentlichung.

Soweit in diesem Abschnitt Informationspflichten aufgezeigt wurden, begründen sie regelmäßig keine Pflicht zur IT-Sicherheit an sich, sondern ergeben sich im Zusammenhang mit anderen Rechtsverhältnissen. Die IT-Sicherheit ist damit nicht

primäres Schutzziel, sondern nur erforderlich, soweit diese zum Schutz für andere Rechtsgüter tauglich ist bzw. eine Gefahr für diese besteht. Soweit keine expliziten Regelungen wie etwa mit dem US-amerikanischen „Security Breach Information Act" existieren, bestehen Informationspflichten nicht in jedem Fall der Kenntnis von Sicherheitslücken und Schwachstellen.

Gesetzliche Informationspflichten gibt es angesichts der Verbreitung und der Abhängigkeit vom Internet sowie der möglichen Schadenshöhen überraschend selten. Im Bereich der kritischen Infrastruktur bietet Art. 4 Abs. 2 der Elektronischen Datenschutzrichtlinie einen Schutz durch Information an. Dieser findet sich jedoch nicht konkret im deutschen Recht umgesetzt.

Zentrale Informationspflichten bestehen als Verkehrssicherungspflichten (sich) über das Bestehen von Sicherheitslücken und Schwachstellen zu informieren.

Die Differenzierung zwischen Pflichten der Hersteller und Anbieter bot die Gelegenheit, die Ausweitung bestehender Produzentenpflichten auf die Anbieter zu diskutieren. Soweit hier festgehalten werden kann, dass die Informationen der Anbieter nicht mit den Produkten gleichgesetzt werden können, entbindet dies die Anbieter im Ergebnis – Herstellern ähnlich – nicht von der Beachtung der Verkehrssicherungspflichten.

Den Anbieter und auch Hersteller treffen Verkehrssicherungspflichten, sich über Sicherheitslücken und Schwachstellen zu informieren und die Nutzer zu informieren. Letzterer steht eine spiegelbildliche Obliegenheit des Nutzers gegenüber, sich im zumutbaren Maße über Sicherheitslücken, d. h. über die Informationen der Hersteller und Anbieter, zu informieren. Dies ist nicht zuletzt erforderlich, um gewährleisten zu können, dass zeitkritische Informationen über Sicherheitslücken die Adressaten erreichen. Dies ist insbesondere dann der Fall, wenn der Nutzerkreis unbekannt ist, etwa wenn keine Kundendaten vorliegen.

CERTs können bei der Veröffentlichung einer Sicherheitslücke – mithin bei der Erfüllung der Verkehrssicherungspflichten – professionelle Hilfestellung geben.

Den Nutzer trifft nur in Ausnahmefällen eine Pflicht, sich über Sicherheitslücken zu informieren. Eine solche kann etwa mit der arbeitsrechtlichen Rücksichtnahmepflicht für den Arbeitnehmer als Nutzer begründet werden.

Den Pflichten über Sicherheitslücken zu informieren sind Herausforderungen bei der Begrenzung gestellt: Zum einen kann Aufklärung grundsätzlich grenzenlos betrieben werden, um ein wirklich aufgeklärtes Verhalten sicherzustellen. Zum ande-

ren dürfen Informationen über IT-Sicherheitslücken keine Anleitung zur Ausnutzung der Lücken sein.

Das Risiko der Anleitung zum Ausnutzen der Lücke wird wie folgt minimiert: Inhaltlich sind die Verkehrssicherungspflicht zu informieren bzw. das Recht zu informieren an einer „unpredictable Full-Disclosure" ausgestaltet. In der Konsequenz erhöht eine Veröffentlichung der Sicherheitslücke die (Eigen)Verantwortung des Rezipienten. Soweit eine bloße Nutzungsbeeinträchtigung droht ist diese unbeachtlich; im Ergebnis besteht dann keine Pflicht zu informieren. Regelmäßig ist die Einschaltung eines Informationsintermediärs indiziert. Grundsätzlich ändert ein mögliches Exploit nichts an dem „Ob" einer Verkehrssicherungspflicht, bzw. begrenzt das Recht zu informieren nicht. Da eine Anleitung zum Exploit durch die Veröffentlichung einer Sicherheitslücke regelmäßig nicht ausgeschlossen werden kann, sind diese Überlegungen stets bei der Konturierung von Informationsrechten und –pflichten zu berücksichtigen.

Das GPSG besitzt mit dem Zusammenwirkung von Meldepflicht an (staatlichen) Informationsintermediären und Recht bzw. Pflicht zu informieren Modellcharakter für ein IT-Informationsrecht.

Soweit der Großteil der Informationsrechte und –pflichten ex post über das Haftungsrecht begründet wird, ist letztendlich ein Beitrag durch das Recht im Sinne einer tatsächlichen Erhöhung der Sicherheit als gering zu werten. Der Beitrag des Rechts bemisst sich ungleich geringer als der Beitrag der Technik. Mithin *„bleibt der Jurist nur noch als Spezialist für die Anmeldung und Durchsetzung von Schadensersatzansprüchen gefragt."*[526]

[526] Wolf, Das Recht im Schatten der Technik, in: Kritische Justiz, 1983, 241 (242).

KAPITEL 6 ERGEBNIS IN THESEN

Was Informationsrechte und –pflichten begründet, beeinflusst und begrenzt soll auf der Grundlage der Ergebnisse der Arbeit zu folgenden allgemeinen Thesen verdichtet werden. Diese werden in thematischen Komplexen angeordnet.

Zusammengefasst werden die Antworten auf die Frage, „Ob" das Recht einen Beitrag zur Sicherheit im Internet zu leisten vermag. Im Anschluss daran werden personelle und inhaltliche Betrachtungen darüber referiert, „Wie" dieser Beitrag geleistet werden kann.

Demnach soll vorab zum „Ob" des Steuerungsvermögens von Informationsrechten und –pflichten Stellung bezogen werden (I.). In diesem Kontext waren die Fragen zu behandeln, ob das Recht überhaupt einen Beitrag zum Ausgleich von Informationsasymmetrien leisten kann.

„Wie" ein solcher Beitrag geleistet werden kann, soll mit der Analyse der Qualität der Akteure im nächsten Themenkomplex erfolgen, da diese entscheidend den Umgang mit Informationen beeinflusst (II.). Denn als personeller Aspekt der Informationsrechte und –pflichten bringen sie einen nicht unwesentlichen Beitrag zur Bestimmung des Umfangs dieser Rechte und Pflichten. Dabei können die inhaltliche Reichweite und Grenzen von Informationsrechten und –pflichten nur als generelle Linie aufgezeigt werden (III.); konkrete Informationsrechte und –pflichten lassen sich stets nur im Einzelfall bestimmen.

In einem Ausblick werden die kennzeichnenden Merkmale hervorgehoben, welche dazu dienen können, den Herausforderungen eines IT-Informationsrechts angemessen zu begegnen (IV.). Abschließend können aus den Ergebnissen für die einleitenden Szenarien praktische Konsequenzen gezogen werden (V.).

I. Zum Beitrag von Informationsrechten und –pflichten zur Reduzierung von Informationsasymmetrien:

1. Die klassische Einteilung der Steuerungsinstrumente ex ante und ex post ist durch die Informationsrechte und –pflichten als Steuerungsinstrumente „in operatione" zu ergänzen. Die Steuerung durch Informationsrechte und -pflichten erfolgt „in operatione", indem diese einen Beitrag im Umgang mit der „sicheren Unsicher-

heit“ leisten und auf diese Weise mittelbar zur Sicherheit des Internets beitragen, da sie Handlungsoptionen für Dritte eröffnen.

2. Dort, wo es an der Durchsetzbarkeit des Rechts fehlt – etwa im internationalen Kontext – kann auf den Anreiz und auf die freiwillige Akzeptanz von Recht und Information und damit auf Eigenverantwortung gesetzt werden.

3. Die Geheimhaltung von Sicherheitslücken durch Informationsrechte und –pflichten als Steuerungsinstrument ist solange in Frage zu stellen, als es nicht feststellbar ist, ob Dritte nicht auch ohne Veröffentlichung der Sicherheitslücke Kenntnis von dieser erhalten haben (Aspekt der „sicheren Unsicherheit“).

4. Informationsrechte und –pflichten können nur einen Beitrag zur Reduzierung der system- und nutzungsbedingten Sicherheitslücken leisten. Sie setzen insoweit voraus, dass der Rezipient der Information den Informationsinhalt wahrnimmt, entsprechend handelt und durch sein Verhalten keine (nutzerbedingte) Sicherheitslücken erzeugt.

5. Information ist Basis für die Wahrnehmung von Eigenverantwortung und ermöglicht mithin Reaktionen, wie die Konfiguration von Clients, der Firewall und der (techno)logischer Infrastruktur oder das Einspielen von Patches.

6. Informationsrechte und –pflichten gleichen Informationsasymmetrien nicht aus, soweit – durch das Urheber- und Strafrecht oder als Betriebs- und Geschäftsgeheimnis – geschützte Interessen an Geheimhaltung der Sicherheitslücke Vorrang genießen.

II. Zum Einfluss der Qualität der Akteure auf die Informationsrechte und –pflichten im Kontext von IT-Sicherheitslücken:

1. Informationsrechte und -pflichten werden als Beitrag zur Erhöhung der Sicherheit im Internet vom Faktor Mensch als nutzerbedingte Sicherheitslücke begrenzt; sie können die Sicherheit tatsächlich nur dann erhöhen, wenn die Nutzer sicherheitsbewusst sind und die nutzerbedingten Sicherheitslücken minimiert werden können.

2. Der Informations(zu)stand der Akteure besitzt – in seinen Ausprägungen als Sicherheitsbewusstsein und Sicherheitserwartung – Relevanz für die Haftung. Das Sicherheitsbewusstsein ist eine Voraussetzung für die Sicherheitserwartung. Eine niedrige Sicherheitserwartung der Nutzer hat Einfluss auf die Haftung für Sicherheitslücken. Je mehr durch Information Einfluss auf das Sicherheitsbewusstsein

genommen wird, desto mehr muss Sicherheit in Eigenverantwortung geleistet werden und desto höher sind aber auch die Sicherheitserwartungen, die an ein sicheres Internet gestellt werden können.

3. Ein Leitbild für einen Durchschnittsnutzer, das der Zuweisung von Verantwortung und der Schutzsphärenverteilung im Falle der Haftung dienen könnte, ist für das Internet nicht feststellbar.

4. Die Chancen des Beitrags des Staates bei Informationspflichten liegen mehr in der Bereitstellung von Informationszentren als Informationsintermediäre und weniger in der Ausübung von Informationsrechte und –pflichten.

5. Der Staat kann gewerblichen Anbietern nicht gleichgestellt werden, soweit Hoheitsträger für die Veröffentlichung von Sicherheitslücken Kompetenzen und Befugnisse bedürfen.

III. Zur Reichweite und Grenzen der Informationsrechte und –pflichten im Kontext von IT-Sicherheitslücken:

1. Inhaltlich sind die Verkehrssicherungspflicht zu informieren bzw. das Recht zu informieren an einer „unpredictable Full-Disclosure“ zu orientieren. Prozedural ist die Einschaltung eines Informationsintermediärs indiziert.

2. Bei Zweifeln hinsichtlich der Nützlichkeit der Information ist die Veröffentlichung grundsätzlich einer Geheimhaltung vorzuziehen, soweit zusätzliche Sicherheit durch die (Eigen)Verantwortung des Rezipienten erreicht werden kann.

3. Im Arbeitsverhältnis kann exemplarisch nach § 88 Abs. 3 S. 1 TKG ein Recht des Arbeitgebers sich über die nutzerbedingte Sicherheitslücke zu informieren angenommen werden.

4. Das Recht des Nutzers sich über Sicherheitslücken proprietärer Software mittels Reverse Engineering bzw. Dekompilierung zu informieren, wird durch das Urheberrecht und § 202a StGB eingeschränkt.

5. Das Recht des Nutzers zu informieren besteht auch bei Verbreitung ruf- und geschäftsschädigender wahrer Tatsachen. Grundsätzlich wird dieses Recht auch nicht durch die Gefahr eingeschränkt, dass diese Information zur Grundlage eines Exploits genutzt werden kann.

6. Die Hersteller von Soft- und Hardware trifft eine Produktbeobachtungspflicht nach § 823 Abs. 1 BGB, sich über Sicherheitslücken zu informieren. Dies kann

auch zu einer Pflicht führen, Kunden zu warnen und gegebenenfalls ein Patch zu veröffentlichen.

7. Staatliche und gewerbliche Anbieter haben ebenfalls eine Verkehrssicherungspflicht nach § 823 Abs. 1 BGB, sich über Sicherheitslücken zu informieren und den Nutzer zu informieren.

8. Soweit eine bloße Nutzungsbeeinträchtigung droht, besteht keine Pflicht nach § 823 Abs. 1 BGB den Nutzer zu informieren.

9. Dem privaten Nutzer und gesteigert dem gewerblichen Nutzer obliegt es nach § 254 BGB, sich über den aktuellen Sicherheitsstandard und aktuelle Sicherheitslücken zu informieren.

10. Eine Obliegenheit des privaten Nutzers den Hersteller oder Anbieter zu informieren besteht nach § 254 Abs. 2 S. 1 BGB grundsätzlich nicht.

IV. Kennzeichnende Merkmale eines IT-Informationsrechts:

1. Ein IT-Informationsrecht ist situativ-initiativ durch den Informationsvorgang desjenigen gekennzeichnet, der sich im „Erfahrensbereich" der Sicherheitslücke befindet. Damit scheidet eine Auskunftspflicht des Herstellers oder Anbieters gegenüber dem – zur Antragstellung verpflichteten – Nutzer aus. Kennzeichnend sind vielmehr Anzeige- oder Aufklärungspflichten. Die Ad-hoc-Mitteilung nach § 15 Abs. 1 WpHG hat in prozeduraler und zeitlicher Hinsicht Modellcharakter.

2. Das IT-Informationsrecht gewinnt durch das Zusammentreffen von Meldepflichten und (staatlichen) Informationsmediären sowie dem Recht bzw. der Pflicht zu informieren an Wirkung.

3. Wesentliche Voraussetzung der Steuerungskraft eines IT-Informationsrechts ist die Ergänzung der Pflicht der Anbieter und Hersteller zu informieren mit einer spiegelbildlichen Obliegenheit des Nutzers sich zu informieren.

4. Die Ambivalenz der Information als Chance und Risiko indiziert die Zwischenschaltung eines Informationsintermediärs. Hier bieten sich professionelle CERTs an.

V. Informationsrechte und –pflichten in den Szenarien:

1. Im Szenario 1 bestehen parallele staatliche und administrative Kompetenzen für die Warnung vor dem Browser und die Aufklärung über Java-Script. Hinsichtlich einer Ermächtigungsgrundlage gilt, dass bei der Bundesregierung von der Aufgabe auf die Befugnis geschlossen werden kann, der Landesdatenschutzbeauftragte mit § 39 Abs. 4 S. 2 DSG-SH eine solche besitzt, aber das BSI bei einer Warnung vor dem Browser seine Beratungsbefugnis aus § 3 Abs. 1 Nr. 7 BSIG überschreitet. Darüber hinaus kann festgehalten werden, dass die Information bezüglich Java-Script eine Aufklärung ohne Grundrechtsrelevanz ist. Die Warnung vor dem Browser greift zwar in Art. 2 Abs. 1 GG des Herstellers ein, ist allerdings gerechtfertigt.

2. Die arbeitsrechtliche Treupflicht nach § 242 i.V.m. § 241 Abs. 2 BGB bestimmt die Reichweite und Grenzen eines Rechts des Arbeitnehmers über Sicherheitslücken zu informieren. Im Szenario 2 steht dem Arbeitnehmer im Ergebnis kein Recht zu, die Nutzer zu informieren.

3. Im Szenario 3 ist der Betreiber des Online-Versandshops nicht verpflichtet, entsprechend § 33 Abs. 1 S. 1 und 3 BDSG die Kunden über die Ausnutzung der Sicherheitslücke zu informieren. Ihn trifft jedoch nach § 823 Abs. 1 BGB eine Verkehrssicherungspflicht, die Kunden zu informieren.

4. Im Szenario 4 trifft die Stadt eine Amtspflicht zur Erteilung richtiger Auskünfte und Erklärungen. Daraus folgt, dass die Bürger über die Manipulation der Webseite zu informieren sind.

LITERATURVERZEICHNIS

Ahrens, Peter, Zur Aufklärungspflicht der nicht beweisbelasteten Partei im Zivilprozess, in: ZZP 96 (1983), 1-24

Albitz, Paul/Liu, Cricket, DNS und BIND, 3.Aufl. 2002

Anderson, Ross, Why Information Security is hard – an Economic perspective, 2001, http://www.cl.cam.ac.uk/ftp/users/rja14/econ.pdf (30.05.2006)

——, Open and Closed Systems are Equivalent (that is, in an ideal world), 2003, http://www.cl.cam.ac.uk/ftp/users/rja14/toulousebook.pdf (30.05.2006)

Assmann, Heinz-Dieter/Schneider, Uwe (Hrsg.), Wertpapierhandelsgesetz – Kommentar, 4. Aufl. 2006

—— (Hrsg.), Wertpapierhandelsgesetz – Kommentar, 3. Aufl. 2003

Bamberger, Heinz Georg/Roth, Herbert (Hrsg.), Kommentar zum Bürgerlichen Gesetzbuch, Band 1 Gesamtsachverzeichnis §§ 1-610, 2003

—— (Hrsg.), Kommentar zum Bürgerlichen Gesetzbuch, Band 2 §§ 611–1296 ErbbauVO WEG, 2003

Barthe, Caroline, Zur Informationstätigkeit der Verwaltung unter besonderer Berücksichtigung des Umweltschutzgesetzes des Bundes, 1993

Bartl, Harald, „Jahr-2000-Problem" und Anwenderpflichten, in: NJW 1999, 2144-2147

Barton, Dirk-M., Risiko-Management und IT-Sicherheit: Der europäische Gesetzgeber will die Überwachung des Internetarbeitsplatzes weitgehend einschränken, in: K&R 2004, 305-312

Bartsch, Michael, Computerviren und Produkthaftung, in: CR 2000, 721-725

——, Software und das Jahr 2000: Haftung und Versicherungsschutz für ein technisches Großproblem, 1998

Beckmann, Kirsten/Müller, Ulf, Online übermittelte Informationen: Produkte i.S.d. Produkthaftungsgesetz, in: MMR 1999, 14-19

Beck'scher TKG-Kommentar hrsg. v. Büchner, Wolfgang/Ehmer, Jörg/Geppert, Martin/Kerkhoff, Bärbel/Piepenbrock, Hermann-Josef/Schütz, Raimund/Schuster, Fabian, 2. Aufl. 2000

Bergles, Siegfried, Baseler Committee: „Kundensorgfaltspflichten" - ein Knebel für die Banken?, in: BKR 2002, 379-384

Berliner Kommentar zum Telekommunikationsgesetz, hrsg. Säcker, Franz Jürgen, 2006

Bier, Sascha, Internet und E-Mail am Arbeitsplatz, in: DuD 2004, 277-281

Birkenbihl, Klaus, Selbstregulierung des Internets am Beispiel von IPv6 und die Rolle ICANNs, in: Hamm, Ingrid/Machill, Marcel (Hrsg.), Wer regiert das Internet? Who controls the Internet?, ICANN als Fallbeispiel für Internet Governance ICANN as a Case Study in Global Internet Governance, 2001, S.407-451

Bizer, Johann, Datenschutzrechtliche Informationspflichten, in: DuD 2005, 451-457

Bizer, Johann/Hammer, Volker/Pordesch, Ulrich/Roßnagel, Alexander, Ein Bundesamt für die Sicherheit in der Informationstechnik – Kritische Bemerkungen zum Gesetzesentwurf der Bundsregierung, in: DuD 1990, 178-186

Bleich, Holger/Schmidt, Jürgen, Auf Phishzug – Passwortdiebstahl im Netz wird immer raffinierter, in: c´t 2004, Heft 17, 178-179

Boehme-Neßler, Volker, Cyberlaw – Lehrbuch zum Internet-Recht, 2001

——, Electronic Government: Internet und Verwaltung – Visionen, Rechtsprobleme, Perspektiven, in: NVwZ 2001, 374-380

Borsook, Pauline, Schöne neue Cyberwelt, 2000

Breuer, Rüdiger, Zunehmende Vielgestaltigkeit der Instrumente im deutschen und europäischen Umweltrecht – Probleme der Stimmigkeit und des Zusammenwirkens, in: NVwZ, 1997, 833-845

——, Schutz von Betriebs- und Geschäftsgeheimnissen im Umweltrecht, in: NVwZ 1986, 171-178

Brüggemeier, Gert, Produkthaftung und Produktsicherheit, in: ZHR 152 (1988), 511-536

Bull, Hans Peter, Die Staatsaufgaben nach dem Grundgesetz, 1973

Burkert, Herbert, Internetrecht – Informationsrecht – Vom zwar Nützlichen aber eher Zufälligen zurück zum möglicherweise Wesentlichen?, in: Schweizer, Rainer J./Burkert, Herbert/Gasser, Urs (Hrsg.), Festschrift für Jean Nicolas Druey, 2002, S. 693-714

——, Internet und Recht, in: Drossou, Olga/v. Harren, Kurt/Hensche, Detlef/Kubicek, Herbert/Mönig-Raane, Margret/Rilling, Rainer/Schmiede, Rudi/Wöltzel, Uwe/Wolf, Frieder Otto (Hrsg.), Machtfragen der Informationsgesellschaft, 1999, 385-393

Burmann, Michael, Die Verkehrssicherungspflicht für den Straßenverkehr, in: NZV 2003, 20-24

Burr, Wolfgang, Richter, Ariane, Discussion Paper No.: 2003-011E Referenzkunden als komplexe Signale hoher Dienstleistungsqualität, http://www.-

innovationsoekonomie.de/discussion-paper/economics/2003-011E.pdf (30.05.2006)

Bydlinski, Franz, Die Suche nach der Mitte als Daueraufgabe der Privatrechtswissenschaft, in: AcP 204 (2004), 309-395

Chang, Jason V., Computer Hacking: Making the Case for a National Reporting Requirement, Berkman Center for Internet & Society Research Publication No. 2004-07 4/2004, http://cyber.law.harvard.edu/home/2004-06 (30.05.2006)

Dannecker, Gerhard, Neuere Entwicklungen im Bereich der Computerkriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, in: BB 1996, 1285-1294

Däubler, Wolfgang, Internet und Arbeitsrecht, 3. Aufl. 2004

Derlien, Hans-Ulrich, Staatliche Steuerung in Perspektive, in: König, Klaus/Dose, Nicolai (Hrsg.), Instrumente und Formen staatlichen Handelns, 1993, S. 503-518

Dickmann, Roman, Inhaltliche Ausgestaltung von Regelungen zur privaten Internetnutzung im Betrieb, in: NZA 2003, 1009-1013

Dörr, Dieter/Gersdorf, Hubertus, Der Zugang zum digitalen Kabel – Zwei Rechtsgutachten im Auftrag der gemeinsamen Stelle digitaler Zugang der Landesmedienanstalten, 2002

Dreier, Horst (Hrsg.), Grundgesetz-Kommentar, Bd. 1 Präambel, Artikel 1-19, 2. Aufl. 2004

Dreier, Thomas, „Wem gehört die Information im 21. Jahrhundert? – Proprietäre versus nicht-proprietäre Verwertung digitaler Inhalte" vom geistigen Eigentum zu einer Informationsordnung, in: Büllesbach, Alfred/Dreier Thomas (Hrsg.), Wem gehört die Information im 21. Jahrhundert Proprietäre versus nicht-proprietäre Verwertung digitaler Inhalte, 2004, S. 95-113

–––, Informationsrecht in der Informationsgesellschaft, in: Bizer, Johann/Lutterbeck, Bernd/Rieß, Joachim (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft, 2002, 65-76

––––/Schulze, Gernot, Urhebergesetz, Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz – Kommentar, 2004

Dreyer, Gunda/Kotthoff, Jost/Meckel Astrid (Hrsg.), Heidelberger Kommentar zum Urheberrecht 2004

Droste, Thomas, Konzept eines komponentenbasierten, verteilten Sicherheitsverbundes, 2002

Druey, Jean Nicolas, Schutz der Information, in: Weber, Rolf/Hilty, Reto M. (Hrsg.), Daten und Datenbanken – Rechtsfragen zu Schutz und Nutzung, 1999, S. 7-25

——, Information als Gegenstand des Rechts: Entwurf einer Grundlegung, 1995

Eberle, Carl-Eugen/Rudolf, Walter/Wasserburg, Klaus (Hrsg.), Mainzer Rechtshandbuch der neuen Medien, 2003

Eberspächer, Jörg, Intelligenz in Netzen, in: Tinnefeld, Marie-Theres/Phillipps, Lothar/Weis, Kurt (Hrsg.), Sicherheit in der Informationstechnik Institutionen und Einzelne im Zeitalter der Informationstechnik, 1994, S. 165-182

Eckert, Claudia, IT-Sicherheit – Konzept, Verfahren, Protokolle, Studienausgabe, 2005

Ehmann, Eugen, Anmerkungen zu VG Köln Beschluss v. 11.03.1999 – 20 L 3737/98, in: CR 1999, 560-561

Eidenmüller, Horst, Der homo oeconomicus und das Schuldrecht: Herausforderungen durch Behavioral Law and Economics, in: JZ 2005, 216-224

Erman Bürgerliches Gesetzbuch: Handkommentar mit AGBG, EGBGB, ErbbauVO, HausratsVO, HausTWG, ProdHaftG, SachenRBerG, SchuldRAnpG, VerbKrG, hrsg. v. Westermann, Peter, 10. Aufl. 2000

Ernst, Stefan, Der Arbeitgeber, die E-Mail und das Internet, in: NZA 2002, 585-591

Di Fabio, Udo, Technikrecht – Entwicklung und kritische Analyse, in: Vieweg, Klaus (Hrsg.), Techniksteuerung und Recht: Referate und Diskussionen eines Symposiums an der Universität Erlangen-Nürnberg, 2000, S. 9-22

——, Das Kooperationsprinzip – ein allgemeiner Rechtsgrundsatz des Umweltrechts, in NVwZ 1999, 1153-1158

——, Verlust der Steuerungskraft klassischer Rechtsquellen, in: NZS 1998, 449-455

——, Information als hoheitliches Gestaltungsmittel, in: Jus, 1997, 1-7

——, Risikosteuerung im öffentlichen Recht – zwischen hoheitlicher Überwachung und regulierter Freiwilligkeit, in: Hoffmann-Riehm, Wolfgang/Schmidt-Aßmann, Eberhard (Hrsg.), Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, 1996, S. 143-165

Fenchel, Jörg, Negative Informationsfreiheit, Zugleich ein Beitrag zur negativen Grundrechtsfreiheit, 1997

Fett, Torsten, Rechtsschutz gegen schlicht-hoheitliches Verwaltungshandeln am Beispiel der Bank- und Versicherungsaufsicht, WM 1999, 613-620

Fezer, Karl-Heinz, Lauterkeitsrecht – Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG), Band 2 §§ 5-22, 2005

——, Das wettbewerbsrechtliche Irreführungsverbot als ein normatives Modell des verständigen Verbrauchers im Europäischen Unionsrecht – Zugleich eine Besprechung der Entscheidung „Mars“ des EuGH vom 6. Juli 1995 – Rechtssache Cm470/93, in: WRP 1995, 671-676

Fiedler, Herbert, Der Staat im Cyberspace, in: Informatik Spektrum, Band 24 Nr. 5 2001, 309-314

–––, Rechtssicherheit im Internet – kein verantwortungsfreier Raum?, in: Reinemann, Heinrich (Hrsg.), Regieren und Verwalten im Informationszeitalter – Unterwegs zur virtuellen Verwaltung, 2000, S. 326-328

Finckh, Andreas, Regulierte Selbstregulierung im Dualen System, 1998

Fitting/Kaiser/Heither/Engels, Betriebsverfassungsgesetz, hrsg. v. Kaiser, Heinrich/Heither, Friedrich/Engels, Gerd/ Schmidt, Ingrid, 20. Aufl. 2000

Fischer, Gero, Tendenzen der Rechtsprechung des BGH zum Anwaltshaftungsrecht, in: NJW 1999, 2993-2998

Fox, Dirk, Security Awareness oder: Die Wiederentdeckung des Menschen in der IT-Sicherheit, in: DuD 2003, 676-680

–––, Computer Emergency Response Team (CERT), in: DuD 2002, 493

Freitag, Andreas, Wettbewerbsrechtliche Probleme im Internet, in: Kröger, Detlef/Gimmy, Marc A. (Hrsg.), Handbuch zum Internetrecht Electronic Commerce – Informations- Kommunikations- und Mediendienste, 2000, 369-409

Freytag, Stefan, Providerhaftung im Binnenmarkt – Verantwortlichkeit für rechtwidrige Inhalte nach der E-Commerce-Richtlinie, in: CR 2000, 600-609

Gaul, Dieter, Die nachvertragliche Geheimhaltungspflicht eines ausgeschiedenen Arbeitnehmers, in: NZA 1988, 225-233

Gasser, Urs, Framing Information Quality Governance Research, in: Gasser, Urs (Hrsg.) Information Quality Regulation: Foundations, Perspectives and Applications, 2004, S. 3-20

Géczy-Sparwassser, Vanessa, Die Gesetzgebungsgeschichte des Internet, 2003

Gerd tom Markotten, Daniela, Benutzbare Sicherheit in informationstechnischen Systemen, 2003

Gehring, Robert A./Lutterbeck, Bernd (Hrsg.), Open Source Jahrbuch 2004 - Zwischen Softwareentwicklung und Gesellschaftsmodell, 2004, http://ig.cs.tu-berlin.de/osjb/OpenSourceJahrbuch2004.pdf (30.05.2006)

Gehring, Robert A., Sicherheit mit Open Source – Die Debatte im Kontext, die Argumente auf dem Prüfstein, in: Gehring, Robert A./Lutterbeck, Bernd (Hrsg.), Open Source Jahrbuch 2004 - Zwischen Softwareentwicklung und Gesellschaftsmodell, 2004, S. 209-235

–––, Software Development, Intellectual Property, and IT Security, in: Journal of Information Law & Technology 2003, Issue 1, http://elj.warwick.ac.uk/jilt/-03-1/gehring.htm (30.05.2006)

Gola, Peter/Schomerus, Rudolf, BDSG – Bundesdatenschutzgesetz Kommentar, 8. Aufl. 2005

Graser, Daniela, Whistleblowing: Arbeitnehmeranzeigen im US-amerkanischen und deutschen Recht, 2000

Grimm, Dieter, Staatsaufgaben – eine Bilanz, in: Grimm, Dieter (Hrsg.), Staatsaufgaben, 1994, S. 771-785

—— (Hrsg.), Wachsende Staatsaufgaben – sinkende Steuerungsfähigkeit des Rechts, 1990

Gröschner, Rolf, Öffentlichkeitsaufklärung als Behördenaufgabe, in: DVBl. 1990, 619-629

Grothe, Thorsten, Restriktionen politischer Steuerung des Rundfunks: systemtheoretische und handlungstheoretische Analysen, 2000

Grundmann, Stefan, Ausbau des Informationsmodells im Europäischen Gesellschaftsrecht, in: DStR 2004, 232-236

Gundel, Jörg, Neue Grenzlinien für die Direktwirkung nicht umgesetzter EG-Richtlinien unter Privaten – Zur Unanwendbarkeit richtlinienwidriger nationaler Verbotsgesetze im Konflikt unter Privaten, in: EuZW 2001, 143-149

Gusy, Christoph, Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse, in: VVDStRL 63 (2004), S. 151-188

——, Verwaltung durch Information – Empfehlungen und Warnungen als Mittel des Verwaltungshandelns, in: NJW 2000, 977-986

Gutmair, Ulrich, Die Politik des Codes, 2000, http://www.telepolis.de/deutsch/special/wos/67471.html (30.05.2006)

Haaß, Wolf-Dieter, Handbuch der Kommunikationsnetze – Einführung in die Grundlagen und Methoden der Kommunikationsnetze, 1997

Hagena, Gerd/Freeman, Rod/Volz, Fabian, Die behördliche Meldung unsicherer Verbraucherprodukte nach dem neuen Geräte- und Produktsicherheitsgesetz und ihre europäische Dimension, in: BB 2005, 2591-2595

Hanau, Peter/Hoeren, Thomas, Private Internetnutzung durch den Arbeitnehmer – Die arbeits- und betriebsverfassungsrechtlichen Probleme, 2003

Haselier, Rainer G./Fahnenstich, Klaus (Hrsg.), Internet: MP3, Online-Shopping, Zugang, Chat, Telefonieren, Suchen, 2000

Hausberg, Dietlind, Der Schutz von Betriebs- und Geschäftsgeheimnissen und das Akteneinsichtsrecht der Beteiligten im Entgeltgenehmigungsverfahren nach dem Telekommunikationsgesetz und dem Postgesetz, 2004

Heckmann, Dirk, Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen – Maßstäbe für ein IT-Sicherheitsrecht, in: MMR 2006, 280-285

Heintzen, Markus, Behördliches Informationshandeln bei ungewissem Sachverhalt – Zugleich zur Frage der Übertragbarkeit zivilrechtlicher Grundsätze auf behördliches Informationshandeln, in: NuR 1991, 301-306

——, Hoheitliche Warnungen und Empfehlungen im Bundesstaat, in: NJW 1990, 1448-1451

Helm, Horst, Das Verbraucherleitbild im Vergleich, in: Keller, Erhard/Plassmann, Clemens/v. Falck, Andreas (Hrsg.), Festschrift für Winfried Tilmann zum 65. Geburtstag, 2003, S. 142-147

Henning-Bodewig, Frauke, Das Europäische Lauterkeitsrecht: B2C, B2B oder doch besser beide?, in Keller, Erhard/Plassmann, Clemens/v. Falck, Andreas (Hrsg.), Festschrift für Winfried Tilmann zum 65. Geburtstag, 2003, S. 149-160

Henssler, Martin/Willemsen, Heinz Josef/Kalb, Heinz-Jürgen (Hrsg.), Arbeitsrechtskommentar, 2004

Herbert, Manfred/Oberrath, Jörg-Dieter, Schweigen ist Gold? – Rechtliche Vorgaben für den Umgang des Arbeitnehmers mit seiner Kenntnis über Rechtsverstöße im Betrieb, in: NZA 2005, 193-199

Hermes, Georg, Infrastrukturverantwortung: Rechtliche Grundstrukturen netzgebundener Transport- und Übertragungssysteme zwischen Daseinsvorsorge und Wettbewerbsregulierung am Beispiel der leitungsgebundenen Energieversorgung in Europa, 1998

Hess, Hans-Joachim/Werk, Hasso, Qualitätsmanagement, Risk Management, Produkthaftung, 1995

Heussen, Benno, Unvermeidbare Softwarefehler – Neue Entlastungsmöglichkeiten für den Hersteller, in: CR 2004, 1-10

Hilber, Marc/Frik, Roman, Rechtliche Aspekte der Nutzung von Netzwerken durch Arbeitnehmer und den Betriebsrat, in: RdA 2002, 89-97

Hilgendorf, Eric, Grundfälle zum Computerstrafrecht, in: JuS 1996, 509-512 und 702-706

Hilty, Reto M., Der Softwarevertrag – ein Blick in die Zukunft – Konsequenzen der trägerlosen Nutzung und des patentrechtlichen Schutzes von Software, in: MMR 2003, 3-15

Hirschmann, Stefan/Romeike, Frank, IT-Sicherheit als Rating-Faktor, http://-www.basel-ii.info/artikel76.html (30.05.2006)

Hoffmann-Riehm, Wolfgang, Verwaltungsrecht in der Informationsgesellschaft – Einleitende Problemskizze, in: Hoffmann-Riehm, Wolfgang/Schmidt-Aßmann, Eberhard (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 9-58

——, Innovationen durch Recht und im Recht, in: Schulte, Michael (Hrsg.), Technische Innovation und Recht, 1997, S. 3-32

——/Schulz, Wolfgang/Held, Thorsten, Konvergenz und Regulierung, 2000

Hoffmann-Riehm, Wolfgang/Schmidt-Aßmann, Eberhard (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000

—— (Hrsg.), Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, 1996

Hoeren, Thomas/Ernstschneider, Thomas, Das neue Geräte- und Produktsicherheitsgesetz und seine Anwendung auf die IT-Branche, in: MMR, 2004, 507-513

——, Internetrecht, Stand 2004, http://www.uni-muenster.de/Jura.itm/hoeren/material/Skript/skript_juli2004.pdf (30.05.2006)

——/Schuhmacher, Dirk, Verwendungsbeschränkungen im Softwarevertrag – Überlegungen zum Umfang des Benutzungsrechts für Standardsoftware, in: CR 2000, 137-146

——/Sieber, Ulrich (Hrsg.), Handbuch Multimedia-Recht – Rechtsfragen des elektronischen Geschäftsverkehrs, 1999, Loseblatt-Ausgabe

Holznagel, Bernd, Recht der IT-Sicherheit, 2003

——, Regulierte Selbstregulierung im Medienrecht, in: Berg, Wilfried/Fisch, Stefan/Schmitt Glaeser, Walter/Schoch, Friedrich/Schulze-Fielitz, Helmut (Hrsg.), Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem, Die Verwaltung Zeitschrift für Verwaltungsrecht und Verwaltungswissenschaften, Beiheft 4, 2001, S. 81-100

——/Temme, Ulrich, Kommunen im Internet, in: Hoeren, Thomas/Sieber, Ulrich, Handbuch Multimediarecht – Rechtsfragen des elektronischen Geschäftsverkehrs. Teil 26, 1999, Loseblatt-Ausgabe

Huber, Peter M., Die Informationstätigkeit der öffentlichen Hand – ein grundrechtliches Sonderregime aus Karlsruhe?, in: JZ 2003, 290-297

Hutter, Reinhard/Neubecker, Adolf, Kritische IT-Infrastrukturen, in: DuD 2003, 211-217

Issensee, Josef, Das Grundrecht auf Sicherheit – Zu den Schutzpflichten des freiheitlichen Verfassungsstaates, Heft 79 der Schriftenreihe der juristischen Gesellschaft e.V., 1983

——/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. II Demokratische Willensbildung – Die Staatsorgane des Bundes, 1987

Jessen, Ernst, Zugangsberechtigung und besondere Sicherung im Sinne von § 202a StGB: Datensicherung – Nicht nur ein juristisches Problem, 1994

Kalir, Erez/Maxwell, Elliot E., Rethinking Boundaries in Cyberspace – A report of the Aspen Insitut Internet Policy Project, 2002, http://inet2002.org/CD-ROM/lu65rw2n/papers/g02-a.pdf (30.05.2006)

Kallnik, Stefan, Pape, Daniel, Schröter, Daniel, Strobel, Stefan, Das Sicherheitsloch, 2001, in: http://www.heise.de/ct/01/23/216/ (30.05.2006)

Käß, Robert, Die Warnung als verwaltungsrechtliche Handlungsform, in: WiVerw 2002, 197-211

Katzenmeier, Christian, Entwicklungen des Produkthaftungsrechts, in: JuS 2003, 943-951

Kaufmann, Franz-Xaver, Steuerung wohlfahrtsstaatlicher Abläufe durch Recht, in: Grimm, Dieter/Maihofer, Werner (Hrsg.), Gesetzgebungstheorie und Rechtspolitik, 1988, S. 65-108

Kaufmann, Peter, ISO-OSI und TCP/IP, in DFN Mitteilungen 1990, Nr. 19/20, S. 21-23

Kersten, Heinrich, Sicherheit in der Informationstechnik – Einführung in Probleme, Konzepte und Lösungen, 2.Aufl. 1995

Kharitoniouk, Svetlana/Stewin, Patrick, Einleitung zu Kapitel 1 Grundlagen und Erfahrungen, in: Gehring, Robert A./Lutterbeck, Bernd (Hrsg.), Open Source Jahrbuch 2004, 2004, S. 1-15

Kilian, Wolfgang, Datensicherheit in Computernetzen, in: CR 1990, 73-81

Kind, Sandra, Die Grenzen des Verbraucherschutz durch Information – aufgezeigt am Teilzeitwohnraumrechtegesetz, 1997

Klindt, Thomas, Das neue Geräte- und Produktsicherheitsgesetz, in: NJW 2004, 465-471

Kloepfer, Michael, Informationsrecht, 2002

–––, Staatliche Informationen als Lenkungsmittel, 1998

Klußmann, Niels, Lexikon der Kommunikations- und Informationstechnik, 3. Aufl. 2002

Knitsch, Peter, Die Rolle des Staates im Rahmen der Produktinformation – zugleich ein Plädoyer für eine Verbraucherinformationsgesetz, in: ZRP 2003, 113-119

Koch, Frank, Handbuch Software- und Datenbankrecht, 2003

–––, Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen, in: CR 1997, 193-203

Koch, Robert, Haftung für die Weiterverbreitung von Viren durch E-Mails, in: NJW 2004, 801-807

Köhler, Helmut/Bornkamm, Joachim (Hrsg.), Baumbach/Hefermehl Wettbewerbsrecht, 23.Aufl. 2004

——, Zum Anwendungsbereich der §§ 1 und 3 UWG nach Aufhebung von RabattG und ZugabeVO, in: GRUR 2001, 1067-1079

Köhntopp, Kristian, Köhntopp, Marit, Pfitzmann, Andreas, Sicherheit durch Open Source? Chancen und Grenzen., in: DuD 2000, 508-513

König, Klaus/Dose, Nicolai, Klassifikationsansätze zum staatlichen Handeln, in: dies. (Hrsg.), Instrumente und Formen staatlichen Handelns, 1993, S. 3-150

——, Referenzen staatlicher Steuerung, in: dies. (Hrsg.), Instrumente und Formen staatlichen Handelns, 1993, S. 519-582

Koziol, Helmut, Generalnorm und Einzeltatbestände als Systeme einer Verschuldenshaftung: Unterschiede und Angleichungsmöglichkeiten, in: ZEuP, 1995 359-367

Krempl Stefan, Good Bye Internet, welcome Disney.net. Der Cyberlaw-Professor Lawrence Lessig stimmt den Abgesang auf das originäre Netz an, telepolis v. 13.02.2005, http://www.heise.de/bin/tp/issue/r4/download.cgi?artikelnr=-5784&pfad=/tp/r4/artikel/5/5784 (30.05.2006)

Krutisch, Dorothee, Strafbarkeit des unberechtigten Zugangs zu Computerdaten und –systemen, 2003

Kugelmann, Dieter, Die Informatorische Rechtsstellung des Bürgers – Grundlagen und verwaltungsrechtliche Grundstrukturen individueller Rechte auf Zugang zu Informationen in der Verwaltung, 2001

Kunig, Philip/Paetow, Stefan/Vestyl, Ludger-Anselm, Kreislaufwirtschafts- und Abfallgesetz - Kommentar, 1998

Kyas, Othmar/a Campo, Markus, Internet professionell: Infrastruktur, Protokolle & Dienste; Fast Internet-Technologien; die Referenz für den IT-Profi, 2. Aufl. 2001

Leiden, Candace/Wilensky, Marshall, TCP/IP für Dummies, 2. Aufl. 2001

Leidinger, Tobias, Hoheitliche Warnungen, Empfehlungen und Hinweise im Spektrum staatlichen Informationshandelns – zum aktuellen Stand der Diskussion in Rechtsprechung und Literatur, in: DÖV 1993, 925-935

Leitner, Frank, Architektur eines sicheren Mobile-Agenten-Systems für das Netzmanagement, 2003

Lell, Otmar, Umweltbezogene Produktkennzeichnung im deutschen, europäischen und internationalem Recht: unter besonderer Berücksichtigung von gentech-

nisch hergestellten Lebensmitteln und von Lebensmitteln aus ökologischer Landwirtschaft, 2003

Lessig, Lawrence, Code and other Laws of Cyberspace, 1999

Lettl, Tobias, Der Schutz des Verbrauchers nach der UWG-Reform, in: GRUR 2004, 449-461

Leube, Sabine C., Die Rolle des Staates im Internet: Eine Untersuchung der Möglichkeit, Zulässigkeit und Notwendigkeit staatlicher Regulierung, 2004

Libertus, Michael, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, in: MMR 2005, 507-512

Lochter, Manfred/Schindler, Werner, Missbrauch von PIN-gestützten Transaktionen mit ec- und Kreditkarten aus Gutachtersicht, in: MMR 2006, 292-297

Loewenheim, Ulrich, Handbuch des Urheberrechts, 2003

Loritz, Karl-Georg, Aufklärungs- und Informationsbeschaffungspflichten über Presseberichte beim Vertrieb von Kapitalanlagen, in: NZG 2002, 889-898

Lübbe-Wolff, Gertrude, Rechtsprobleme der behördlichen Umweltberatung, in: NJW 1987, 2705-2712

Lüdemann, Jörn, Edukatorisches Staatshandeln – Steuerungstheorie und Verfassungsrecht am Beispiel der staatlichen Förderung von Abfallmoral, 2002

Lutterbeck, Bernd, Globalisierung des Rechts – am Beginn einer neuen Rechtskultur?, in: CR 2000, 52-60

——/Horns, Axel H. /Gehring, Robert, Sicherheit in der Informationstechnologie und Patentschutz für Software-Produkte – ein Widerspruch?, Kurzgutachten, 2000, http://www.ipjur.com/data/LuGeHo.pdf (30.05.2006)

——/Ishii, Kei, Open Code and Open Societies, Paper zum Wizards of OS: Offene Quellen und Offene Software, 16.-17.07.1999, Berlin http://ig.cs.tu-berlin.de/oldstatic/bl/042/index_html#fn0 (30.05.2006)

Mandelartz, Herbert/Grotelüschen, Henning, Das Internet und die Rechtsprechung des BVerfG zur Öffentlichkeitsarbeit der Regierung, in: NVwZ 2004, 647-650

Manssen, Gerrit (Hrsg.), Telekommunikations- und Multimediarecht: ergänzbarer Kommentar zum Telekommunikationsgesetz, Mediendienstestaatsvertrag, Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz einschließlich Gesetzes- und Verordnungstexten und europäischen Schriften, Loseblattsammlung, Grundwerk 1999

Marly, Jochen, Softwareüberlassungsverträge – Erscheinungsformen, Pflichtverletzung, Vertragsgestaltung, Allgemeine Geschäftsbedingungen, Musterverträge, 4. Aufl. 2004

——, Urheberrechtsschutz für Computersoftware in der Europäischen Union – Abschied vom überkommenden Urheberrechtsverständnis, 1995

Masing, Johannes, Transparente Verwaltung: Konturen eines Informationsverwaltungsrechts, in: VVDStRL 63 (2004), S. 377-436

——, Grundstrukturen eines Regulierungsverwaltungsrechts: Regulierung netzbezogener Märkte am Beispiel Bahn, Post, Telekommunikation und Strom, in: Die Verwaltung, 36. Band 2003, S. 1-32

——, Politische Verantwortlichkeit und rechtliche Verantwortung, in: ZRP 2001, 36-42

Mayer-Schönberger, Viktor, Recht offen – Plädoyer für ein Informationsrecht im neuen Jahrtausend, S. 10 ff., Vortrag auf dem Europäischen Kongress des österreichischen Notariats, 09.07.2000, Wien

Mayntz, Renate, Politische Steuerung und gesellschaftliche Steuerungsprobleme – Anmerkungen zu einem theoretischen Paradigma, in: Ellwein, Thomas/Hesse, Joachim Jens/Mayntz, Renate/Scharpf, Fritz W. (Hrsg.), Jahrbuch zur Staats- und Verwaltungswissenschaft, 1987, S. 89-110

Meier, Klaus/Wehlau, Andreas, Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, in: NJW 1998, 1585-1591

Menke, Burkhart, Die moderne, informationsökonomische Theorie der Werbung und ihre Bedeutung für das Wettbewerbsrecht, dargestellt am Beispiel der vergleichenden Werbung, in: GRUR 1993, 718-728

Meyer, Alfred Hagen, Bemerkungen zur „Mars"-Entscheidung des EuGH, in: GRUR Int 1996, 98-101

Michalski, Lutz, Produktbeobachtung und Rückrufpflicht des Produzenten, in: BB 1998, 961-965

Micklitz, Hans-W., Zur Notwendigkeit eines neuen Konzepts für die Fortentwicklung des Verbraucherrechts in der EU, in: VuR 2003, 2-12

Mielke, Kai, Beruf: Komplize – Illegales Handeln im Auftrag des Arbeitgebers, c´t 2006, Heft 8, S. 170-171

Minkwitz, Oliver/Schöfbänker, Georg, „Information Warfare: Die neue Herausforderung für die Rüstungskontrolle", telepolis v. 31.05.2000, http://www.heise.de/tp/r4/html/result.xhtml?url=/tp/r4/artikel/6/6817/1.html&words=Information%20warfare (30.05.2006)

Möller, Erik, Sicherheit in Peer-to-Peer-Netzen, Beim Tauschen und Suchen sollte man die Risiken kennen, telepolis v. 29.06.2001, http://www.heise.de/tp/r4/artikel/7/7972/1.html (30.05.2006)

Mrozynski, Peter, Sozialgesetzbuch – Allgemeiner Teil (SGB I) Kommentar, 2. Aufl. 1995,

Müller, Günter, Enthält die Informatik Sprengkraft für Regulierungssysteme?, in: Bizer, Johann/Lutterbeck, Bernd/Rieß, Joachim (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft - Freundesgabe für Alfred Büllesbach, 2002, 93-103

Müller, Michael, Whistleblowing – ein Kündigungsgrund, in: NZA 2002, 424-437

v. Münch, Ingo/Kunig, Philip (Hrsg.) Grundgesetz-Kommentar, Bd. 1 Präambel Artikel 1-19, 5. Aufl. 2000

Münchener Kommentar zum Bürgerlichen Gesetzbuch, hrsg. v. Rebmann, Kurt/Säcker, Franz Jürgen/Rixecker, Roland, Band 2a Schuldrecht Allgemeiner Teil §§ 241-432, 4. Aufl. 2003

——, hrsg. v. Rebmann, Kurt/Säcker, Franz Jürgen/Rixecker, Roland, Band 5 Schuldrecht Besonderer Teil III, 4. Aufl. 2004

——, hrsg. v. Rebmann, Kurt/Säcker, Franz Jürgen/Rixecker, Roland, Band 10 Einführungsgesetz zum Bürgerlichen Gesetzbuche (Art. 1-38) Internationales Privatrecht, 3. Aufl. 1998

Münchner Kommentar zum Strafgesetzbuch, hrsg. v. Joecks, Wolfgang/Miebach, Klaus, Band 3 §§ 185-262, 2003

Murswiek, Dietrich, Das Bundesverfassungsgericht und die Dogmatik mittelbarer Grundrechtseingriffe – Zu der Glykol- und der Osho- Entscheidung vom 26.6.2002, in: NVwZ 2003, 1-8

——, Die staatliche Verantwortung für die Risiken der Technik – Verfassungsrechtliche Grundlagen und immissionsschutzrechtliche Ausformung, 1985

Naujock, Anke, Internet-Richtlinien: Nutzung am Arbeitsplatz: Ein Plädoyer für klare Regelungen, in: DuD 2002, 592-596

Neumann, Heinzgeorg, Die Verfassung der Freien Hansestadt Bremen, Kommentar, 1996

Nicolini, Käte/Ahlberg, Hartwig (Hrsg.), Möhring/Nicolini Urheberrechtsgesetz Kommentar, 2. Aufl. 2000

Niemöller, Stefan, Das Verbraucherleitbild in der deutschen und europäischen Rechtsprechung – Verhandlungs- und Vertragsparität als Regelungsgehalt des § 3 UWG, 1999

Oebbecke, Janbernd, Beratung durch Behören, in: DVBl. 1994, 147-154

Oppliger, Rolf, Sicherheit von Open Source Software – Mythos oder Wirklichkeit?, in: DuD 2003, 669-675

Ott, Stephan, Urheber- und wettbewerbsrechtliche Probleme von Linking und Framing, 2004

Pagenberg, Jochen, Betrieblicher Know-How-Schutz in gerichtlichen Auseinandersetzungen, in: CR 1991, 65-72

Palandt Bürgerliches Gesetzbuch mit Einführungsgesetz (Auszug), BGB-Informationspflichten-Verordnung, Unterlassungsklagengesetz, Produkthaftungsgesetz, etc., hrsg. v. Bassenge, Peter/Brudermüller, Gerd/Diederichsen, Uwe/Edenhofer, Wolfgang/Grüneberg, Christian/Heldrich, Andreas/Heinrichts, Helmut/Sprau, Hartwig/Putzo, Hans/Weidenkaff, Walter, 65. Aufl. 2006

Paschke, Marian, Medienrecht, 2. Aufl. 2001

Pfeiffer, Thomas, Welches Recht gilt für elektronische Rechtsgeschäfte?, in: Jus 2004, 282-285

Philipp, Renate, Staatliche Verbraucherinformationen im Umwelt- und Gesundheitsrecht, 1989

Pipkin, Donald L., Information Security. Protecting the Global Enterprise, 2000

Pitschas, Rainer, Staatliches Management für Risikoinformation zwischen Recht auf informationeller Selbstbestimmung und gesetzlichen Kommunikationsvorbehalt, in: Hart, Dieter (Hrsg.), Privatrecht im Risikostaat, 1997, S. 215-263

——, Verwaltungsverantwortung und Verwaltungsverfahren – Strukturprobleme, Funktionsbedingungen und Entwicklungsperspektiven eines konsensualen Verwaltungsrechts, 1990

Podehl, Jörg, Internetportale mit journalistisch-redaktionellen Inhalten – Anbieterpflichten und Haftungsrisiken, in: MMR 2001, 17-23

Pohl, Hartmut, Weck, Gerhard (Hrsg.): Beiträge zur Informationssicherheit: Strategische Aspekte der Informationssicherheit und staatliche Reglementierung, 1995

Pohl, Joachim, Informationsbeschaffung beim Mitbürger, 2002

Poledna, Tomas, Staatliche Informationspflichten (Grundversorgung mit elektronischen Daten), in: Koller, Heinrich/Koller, Thomas (Hrsg.), Recht und Rechtsdaten/Droit et données juridiques - Anspruch und Wirklichkeit/entre ambition et réalité - Tagung 2003 für Informatik und Recht/Journées 2003 d'informatique juridique, 2004, S. 69-104, http://www.informatique-juridique.ch/de/tagungsband_2003_de.html (30.05.2006)

Proksch, Wolfram, Internet Governance – Die Verwaltung des Internet, 2001, http://www.it-law.at/papers/proksch-internet-governance.pdf (30.05.2006)

Raab, Thomas, Die Bedeutung der Verkehrssicherungspflichten und ihre systematische Stellung im Deliktsrecht, in: JuS 2002, 1041-1048

Raepple, Martin, Sicherheitskonzepte für das Internet – Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, 2. Aufl. 2001

Rechenberg, Peter, Zum Informationsbegriff, der Informationstheorie, in: Informatik Spektrum, Band 26 Nr. 5 2003, S. 317-326

Reese, Jürgen, Produkthaftung und Produzentenhaftung für Hard- und Software, DStR 1994, 1121-1127

Rehbinder, Manfred, Urheberrecht, 12. Aufl. 2002

Reich, Norbert/Micklitz, Hans-W. (Hrsg.), Europäisches Verbraucherrecht, 4. Aufl. 2004

Reidenberg, Joel, Lex Informatica: The Formulation of Information Policy Rules through Technology , 76 TEXAS L. REV. 553 (1998), S. 553-584

Reinermann, Heinrich (Hrsg.), Regieren und Verwalten im Informationszeitalter – Unterwegs zur virtuellen Verwaltung, 2000

Richters, Swantje/Wodtke, Carolina, Schutz von Betriebsgeheimnisse aus Unternehmersicht – Verhinderung von Know-how Abfluss durch eigene Mitarbeiter, in: NZA-RR 2003, 281-288

Röhl, Hans Christian, Verwaltungsverantwortung als dogmatischer Begriff, in: Berg, Wilfried/Fisch, Stefan/Schmitt Glaeser, Walter/Schoch, Friedrich/Schulze-Fielitz, Helmuth, Die Verwaltung Zeitschrift für Verwaltungsrecht und Verwaltungswissenschaften, Beiheft 2, 1999, S. 33-55

Romeike, Frank, IT-Riskmanagement vor dem Hintergrund von Basel II und Solvency II, in: DuD 2004, 335-339

Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003

——, Notwendige und mögliche Regulierungen der IT-Sicherheit, in: Pohl, Hartmut/Weck, Gerhard (Hrsg.), Beiträge zur Informationssicherheit, 1995, S. 51-63

——, Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin, 1993

Rothe, Lothar, Produkthaftung. Rechtliche Grundlagen und ihre Auswirkungen auf die Industrie, in: CR 1993, 310-313

Röthel, Anne, Europarechtliche Vorgaben für das Technikrecht, in: Schulte, Martin, Handbuch des Technikrechts: Referate und Diskussionen eines Symposiums an der Universität Erlangen-Nürnberg, 2003, S. 155-184

Ruge, Reinhard, Die Gewährleistungsverantwortung des Staates und der Regulatory State – Zur Veränderten Rolle des Staates nach der Deregulierung der Stromwirtschaft in Deutschland, Großbritannien und der EU, 2004

Runte, Christian/ Potinecke, Harald W., Software und GPSG - Anwendbarkeit und Auswirkungen des Geräte- und Produktsicherheitsgesetzes auf Hersteller und Händler von Computerprogrammen, in: CR 2004, 725-729

Rüthers, Bernd, Rechtstheorie: Begriff, Geltung und Anwendung des Rechts, 1999

Rützel, Stefan, Illegale Unternehmensgeheimnisse?, in: GRUR 1995, 557-561

Sachs, Michael (Hrsg.), Grundgesetz Kommentar, 3. Aufl. 2003

Salje, Peter, Ökonomische Analyse des Technikrechts, in: Vieweg, Klaus (Hrsg.), Techniksteuerung und Recht: Referate und Diskussionen eines Symposiums an der Universität Erlangen-Nürnberg, 2000, S. 151-176

Saltzer, J. H./Reed, D. P./Clark, D. D., End-to-end arguments in system design, ACM Transactions in Computer Systems 2, 4, November, 1984, S. 277-288, http://web.mit.edu/saltzer/www/publications/endtoend/endtoend.pdf (30.05.2006)

Schaffland, Hans-Jürgen/Wiltfang, Noeme, Bundesdatenschutzgesetz – Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, 2005

Schatzschneider, Wolfgang, Informationshandeln im Bundesstaat, in: NJW 1991, 3202-3203

Schaub, Günter, Arbeitsrechts-Handbuch – systematische Darstellung und Nachschlagewerk für die Praxis, 10. Aufl. 2002

Scherzberg, Arno, Risikosteuerung durch Verwaltungsrecht: Ermöglichung oder Begrenzung von Innovationen?, in: VVDStRL 63 (2004), S. 214-258

Scheuerle, Klaus-Dieter/Mayen, Thomas (Hrsg.), Telekommunikationsgesetz – Kommentar, 2002

Schmid, Pirmin, Computerhacken und materielles Strafrecht – unter Besonderer Berücksichtigung von § 202a StGB, 2001, digitale Ressource, http://www.-ub.uni-konstanz.de/kops/volltexte/2001/680/ (30.05.2006)

Schmid, Viola, IT-Sicherheit durch Cyberlaw?, in: thema Forschung 1/2004

——, Cyberlaw – eine neue Disziplin im Recht?, in: Hendler, Reinhard/Marburger, Peter/Reinhardt, Michael/Schröder, Meinhard (Hrsg.), Jahrbuch des Umwelt- und Technikrechts 2003, S. 449-480

——, Strom- und Energiesparmarketing in ihrer Bedeutung für das Umweltrecht, 1997, S. 104

Schneider, Jochen, Neues zu Vorlage und Herausgabe des Quellcodes? – Kritische Überlegungen zur Dissonanz zwischen vertraglicher und prozessualer Beurteilung des Quellcodes durch den BGH, in: CR, 2003, 1-9

——/Günther, Andreas, Haftung für Computerviren, in: CR 1997, 389-396

Schneier, Bruce, Secrets & Lies: digital security in a networked world, 2000

Schoch, Friedrich, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, in: VVDStRL 57 (1998), S. 158-212

Scholz, Rupert/Pitschas, Rainer, Informationelle Selbstbestimmung und staatliche Informationsvorsorge, 1984

Schönke, Adolf/Schröder, Horst, Strafgesetzbuch Kommentar, 26. Aufl. 2001

Schrader, Leif U., Die wettbewerbsrechtliche Beurteilung von neuen Vertriebsformen im Internet, 2004

Schricker, Gerhard (Hrsg.), Urheberrecht Kommentar, 3. Aufl. 2006

Schulte, Martin, Techniksteuerung durch Technikrecht – rechtsrealistisch betrachtet, in: Vieweg, Klaus (Hrsg.), Techniksteuerung und Recht: Referate und Diskussionen eines Symposiums an der Universität Erlangen-Nürnberg, 2000, S. 23-34

—— (Hrsg.), Technische Innovation und Recht. Antrieb oder Hemmnis?, 1997

Schumacher, Markus, Security Patterns, in: Informatik Spektrum, Band 25 Nr. 3 2002, S. 220-223

Schuppert, Gunnar Folke, Verwaltungswissenschaft als Steuerungswissenschaft. Zur Steuerung des Verwaltungshandelns durch Verwaltungsrecht, in: Hoffmann-Riehm, Wolfgang (Hrsg.), Reform des allgemeinen Verwaltungshandeln: Grundfragen, Baden-Baden 1993, S. 65-114

——, Grenzen und Alternativen von Steuerung durch Recht, in: Grimm, Dieter (Hrsg.), Wachsende Staatsaufgaben – sinkende Steuerungsfähigkeit des Rechts, Baden-Baden 1990, S. 217-250

Schulz, Wolfgang, Regulierte Selbstregulierung im Telekommunikationsrecht. Die informationale Beteiligung Dritter bei der Regelsetzung des Regulierers in Deutschland und den Vereinigten Staaten, in: Berg, Wilfried/Fisch, Stefan/Schmitt Glaeser, Walter/Schoch, Friedrich/Schulze-Fielitz, Helmut (Hrsg.), Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem, Die Verwaltung Zeitschrift für Verwaltungsrecht und Verwaltungswissenschaften, Beiheft 4, 2001, S. 101-122

Schwarcz, Steven L., Private Ordering, Northwestern University Law Review Vol. 97, No. 1 S. 319-349

Schweizer, Robert, Die „normative Verkehrsauffassung" – ein doppeltes Missverständnis – Konsequenzen für das Leitbild des "durchschnittlich informierten, verständigen und aufmerksamen Durchschnittsverbrauchers", in: GRUR 2000 923-933

Sendler, Horst, Techniksteuerung und verwaltungsgerichtliche Rechtsprechung, in: Vieweg, Klaus (Hrsg.), Techniksteuerung und Recht: Referate und Diskussionen eines Symposiums an der Universität Erlangen-Nürnberg, 2000, S. 307-324

Shephard, Stephen. A., Vulnerability Disclosure – How do we define Responsible Disclosure, 2003, http://www.giac.org/certified_professionals/practicals/gsec/2541.php (30.05.2006)

Sieber, Ulrich, Computerkriminalität und Informationsstrafrecht – Entwicklungen in der internationalen Informations- und Risikogesellschaft, in: CR 1995, 100-112

Simitis, Spiros (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 5. Aufl. 2003

SK-STGB - Systematischer Kommentar zum StGB hrsg. v. Rudolphi, Hans-Joachim/Horn, Eckhard/Günther, Hans-Ludwig/Samson, Erich, Band 2 Besonderer Teil §§ 201-266b, 2003

Smedinghoff, Thomas J., Trends in the law of information security, in: 829 PLI/Pat (Practising Law Institute Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series PLI Order Number 6080, May-June 2005), 285-296

Soergel, Bürgerliches Gesetzbuch mit Einführungsgesetz und Nebengesetzen, hrsg. v. Spickhoff, Andreas, Band 12 Schuldrecht 10 §§ 823-853 ProdHG UmweltHG, 2005

Sonntag, Matthias, IT-Sicherheit kritische Infrastruktur – von der Staatsaufgabe zur rechtlichen Ausgestaltung, 2005

Spindler, Gerald, Haftung und Verantwortlichkeit im IT-Recht, in: CR 2005, 741-747

Spindler, IT-Sicherheit, und Produkthaftung – Sicherheitslücken, Pflichten der Hersteller und Softwarenutzer, in: NJW 2004, S. 3145-3150

——, Verantwortlichkeit und Haftung für Hyperlinks im neuen Recht, in: MMR 2002, 495-503

——, Das Jahr 2000-Problem in der Produkthaftung: Pflichten des Herstellers und der Softwarenutzer, in: NJW, 1999, 3737-3745

——, Verschuldensabhängige Produkthaftung im Internet, in: MMR 1998, 23-29

——/Schmitz, Peter/Geis, Ivo (Hrsg.), TDG – Teledienstegesetz Teledienstedatenschutzgesetz Signaturgesetz Kommentar, 2004

——/Klöhn, Lars, Neue Qualifikationsprobleme im E-Commerce – Verträge über die Verschaffung digitalisierter Information als Kaufvertrag, Werkvertrag, Verbrauchsgüterkauf, in: CR 2003, 81-86

Spinner, Helmut F., Ist Wissen analogiefähig? – Über Sach-, Geld-, Wasser- und andere Vergleiche, in: Schweizer, Rainer J./Burkert, Herbert/Gasser, Urs (Hrsg.), Festschrift für Jean Nicolas Druey, 2002, S. 947-969

Stadler, Astrid, Der Schutz des Unternehmensgeheimnisses im Zivilprozess, in: NJW 1989, 1202-1206

Stevens, Richard/Pohl, Hartmut, Honeypots und Honeynets, in: Informatik Spektrum Band 27 Nr. 3 2004, 260-264

Stoll, Peter-Tobias, Sicherheit als Aufgabe von Staat und Gesellschaft: Verfassungsordnung, Umwelt- und Technikrecht im Umgang mit Unsicherheit und Risiko, 2003

Stolpmann, Jens, Konzeption eines Software-Lifecycle-Managementsystems (SLM) zur Unterstützung und Beschleunigung von Softwareentwicklungsprozessen, 2003, http://miless.uni-essen.de/servlets/DerivateServlet/Derivate-11865/-dissertation.pdf (30.05.2006)

Taeger, Jürgen, Die Offenbarung von Betriebs- und Geschäftsgeheimnissen, 1988

——, Produkt- und Produzentenhaftung bei Schäden durch fehlerhafte Computerprogramme, in: CR 1996, 257-271

Tanenbaum, Andrew S., Computernetzwerke, 4.Aufl. 2003

Tierling, Eric, Internet - Das kompakte Wissen, 2001

Traumüller, Roland/Wimmer, Maria, Daten – Informationen – Wissen – Handeln: Management des Wissens, in: Reinermann, Heinrich (Hrsg.), Regieren und Verwalten im Informationszeitalter, 2000, S.482-498

Tremmel, Bernd/Nolte, Steffan, Amtshaftung wegen behördlicher Warnungen, in: NJW 1997, 2256-2273

Tröndle, Herbert/Fischer, Thomas, Strafgesetzbuch und Nebengesetze, 52. Aufl. 2004

Trute, Hans-Heinrich/Spoerr, Wolfgang/Bosch, Wolfgang, Telekommunikationsgesetz mit FTEG – Kommentar, 1. Aufl. 2001

——, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, in: VVDStRL 57 (1998), S. 216-268

Tschon, Michaela S., Kommunikationsordnung im Aufbruch, in: Vieweg, Klaus (Hrsg.) Spektrum des Technikrechts: Referate eines Symposiums aus Anlaß des 10jährigen Bestehens des Instituts für Recht und Technik in Erlangen, 2002, 129-154

Umbach, Dieter/Clemens, Thomas (Hrsg.), Grundgesetz – Mitarbeiterkommentar und Handbuch, Band I, 2002

Valerius, Brian, Der Weg zu einem sicheren Internet? – Zum In-Kraft-Treten der Convention on Cybercrime, in: K&R 2004, 513-518

Van den Bergh, Roger/Lehmann, Michael, Informationsökonomie und Verbraucherschutz im Wettbewerbs- und Warenzeichenrecht, in: GRUR Int 1992, 588-599

Vec, Miloš, Kurze Geschichte des Technikrechts. Von den Anfängen bis zum ersten Weltkrieg, in: Schulte, Martin, Handbuch des Technikrechts, 2003, S. 3-60.

Vieweg, Klaus, A Safety Code as an Instrument to Tighten Technical Law?, Dokument zum World Congress Safety of Modern Technical Systems, Saarbrücken, 13.09.2001, http://www.irut.de/saarbrueckene.html (30.05.2006)

——, Technik und Recht, in: Vieweg, Klaus/Haarmann, Wilhelm (Hrsg.), Beiträge zum Wirtschafts-, Europa- und Technikrecht. Festgabe für Rudolf Lukes zum 75.Geburtstag, 2000, S. 199-213

Volkmann, Christian, Der Störer im Internet – Zur Verantwortlichkeit der Internet-Provider im allgemeinen Zivil-, Wettbewerbs-, Marken- und öffentlichen Recht, 2005

Voigt, Rüdiger, Staatliche Steuerung aus interdisziplinärer Perspektive, in: König, Klaus/Dose, Nicolai (Hrsg.), Instrumente und Formen staatlichen Handels, Köln, 1993, S. 289-322

Voitl, Alexander, Behördliche Warnkompetenz im Bundesstaat, Zur Verteilung der Zuständigkeiten im Verhältnis zwischen Bund, Ländern und Gemeinden, 1993

Vossbein, Reinhard, Eigenverantwortung und Marktwirtschaft als Steuerungsimpulse der IT-Sicherheit. Sicherheit – ein Trivialproblem?, in: Pohl, Hartmut/Weck, Gerhard (Hrsg.), Beiträge zur Informationssicherheit: Strategische Aspekte der Informationssicherheit und staatliche Reglementierung, 1995, S. 43-49

Wagner, Florian, Die "Open Access Debatte" in den USA – Zugangsansprüche von Internet Service Providern zum Breitbandkabel, in: MMR 2001, 659-665.

Wagner, Gerhard in: Rebmann, Kurt/Säcker, Franz Jürgen/Rixecker, Roland (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 5 Schuldrecht Besonderer Teil III, 4. Aufl., 2004

Wagner, Gerhard, Haftung und Versicherung als Instrument der Techniksteuerung, in: Vieweg, Klaus (Hrsg.), Techniksteuerung und Recht: Referate und Diskussionen eines Symposiums an der Universität Erlangen-Nürnberg, 2000, S. 87-120

Wandtke, Artur-Axel/Bullinger, Winfried (Hrsg.), Praxiskommentar zum Urheberrecht, 2002

Weber, Rolf H., Ali Baba oder das Risiko exklusiver Informationsinhaltsrechte, in: Schweizer, Rainer J./Burkert, Herbert/Gasser, Urs (Hrsg.), Festschrift für Jean Nicolas Druey, 2002, S. 1009-1026

Weiss, Julian, Das Internet und die klassischen Medien Konvergenz – Konkurrenz oder Komplementierung? Eine medienpolitische Betrachtung, 2002

Weißnicht, Elmar, Die Nutzung des Internet am Arbeitsplatz, in: MMR 2003, 448-453

Wenger, Andreas/Metzger, Jan (Hrsg.), International CIIP Handbook 2004, An Inventory and Analysis of Protection Policies in Fourteen Countries, 2004

Wenning, Rigo, Das Internet - ein rechtsfreier Raum?, in: JurPC Web-Dok. 16/1997, http://www.jurpc.de/aufsatz/19970016.htm (30.05.2006)

Wertheimer, Frank, Bezahlte Karenz oder entschädigungslose Wettbewerbshandlung des ausgeschiednen Arbeitnehmers? – Zugleich Anmerkung zu BAG, 19.5,1998, BB 1999, 212 (Kantenbänder), in BB 1999, 1600-1603

v. Westphalen, Friedrich, Produzentenhaftung, in: v. Westphalen, Friedrich/Langheid, Theo/Streitz, Siegfried (Hrsg.), Der Jahr 2000 Fehler: Haftung und Versicherung, 1999, S. 249-332

——, Das neue Produkthaftungsgesetz, in: NJW 1990, 83–93

——, Jahr-2000-Fehler und deliktische Haftung, in: DStR 1998, 1722-1724

Wiebke, Andreas, „Deep Links" – Neue Kommunikationsformen im Wettbewerb aus lauterkeitsrechtlicher Sicht – Zugleich eine Besprechung der Entscheidung des OLG Celle vom 12.5.1999, Az. 13 U 38/99, in: WRP 1999, 734-740

Wolf, Thomas, Die Grundsätze der Rechtsprechung des EuGH im Bereich des Rechts gegen den unlauteren Wettbewerb, 2001, http://opus.bibliothek.uni-wuerzburg.de/opus/volltexte/2002/25/pdf/wolf.pdf (30.05.2006)

Wolf, Rainer, Das Recht im Schatten der Technik, in: Kritische Justiz, 1986, 241-262

Wolff, Heinrich, Der verfassungsrechtliche Schutz der Betriebs- und Geschäftsgeheimnisse, in: NJW 1997, 98-101

Zöllner, Dieter, Der Datenschutzbeauftragte im Verfassungssystem – Grundsatzfragen der Datenschutzkontrolle, 1995

ZUR PERSON DER VERFASSERIN

Die Verfasserin wurde am 23.12.1974 in Würzburg geboren. Ab 1981 besuchte sie die Grundschule Spardorf. Den schulischen Bildungsweg schloss sie 1994 mit dem Abitur am Emil-von-Behring-Gymnasium in Spardorf ab. Im Wintersemester 1994/1995 begann sie das Studium der Rechtswissenschaft an der Julius-Maximilians-Universität in Würzburg, das sie mit einem Sokrates-Erasmus Stipendium an der Universidad de Barcelona im Wintersemester 1997/1998 ergänzte und mit dem 1. juristischen Staatsexamen in Würzburg abschloss. Danach folgten das Referendariat im OLG-Bezirk Bamberg und das 2. juristische Staatsexamen im Jahr 2001.

Von 2002 bis 2005 war die Verfasserin aktive Wissenschaftliche Mitarbeiterin bei Frau Prof. Dr. Viola Schmid, LL.M. (Harvard) im Fachgebiet Öffentliches Recht am Fachbereich 1 der Technischen Universität Darmstadt. Seit Oktober 2005 bis heute ist sie in Elternzeit.