DEUTSCHER BUNDESTAG

ENQUETE-KOMMISSION
INTERNET UND DIGITALE GESELLSCHAFT

Deutscher Bundestag

Enquete-Kommission
Internet und digitale Gesellschaft

Ausschussdrucksache
17(24)064

TOP 1 am 14. Januar 2013

10.1.2013

Bericht

Projektgruppe Zugang, Struktur und Sicherheit im Netz

Vorsitzender: Sachverständiger Harald Lemke

Stand: 10. Januar 2013, 12 Uhr

Inhaltsverzeichnis

Grußwort des Vorsitzenden 10

I. Zugang zum Internet und Infrastruktur des Internets 11

I.1. Einleitung 11

I.2. Einführung und Auswirkungen neuer Protokolle 12

I.2.1 Förderung der Einführung neuer Protokolle 12

I.2.2 Absicherung gegenüber potenziellen negativen Effekten 14

I.2.2.1 Auswirkung auf den Wettbewerb 14

I.2.2.2 Exkurs: Sicherheitsaspekte bei der Einführung des neuen Internetprotokolls Version 6 (IPv6) 15

I.2.2.2.1 Einführung 15

I.2.2.2.1.1 Das Internetprotokoll Version 4 (IPv4) 15

I.2.2.2.1.2 Vergabe der IP-Adressen 16

I.2.2.2.1.3 IPv4-Adressknappheit 16

I.2.2.2.1.4 Das Internetprotokoll Version 6 (IPv6) 17

I.2.2.2.1.5 Aufbau von IPv6-Adressen 17

I.2.2.2.1.6 Technische Neuerungen von IPv6 gegenüber IPv4 18

I.2.2.2.1.7 Notwendigkeit der Umstellung auf IPv6 21

I.2.2.2.2 Chancen und Herausforderungen eines Umstiegs auf IPv6 22

I.2.2.2.2.1 Chancen 22

I.2.2.2.2.2 Herausforderungen 23

I.2.2.2.2.2.1 IPv6-fähige Hard- und Software 23

I.2.2.2.2.2.2 Neue Angriffsvektoren 25

I.2.2.2.2.2.3 Sicherheitsanforderung an Endgeräte 26

I.2.2.2.2.2.4 Statische und dynamische Adressvergabe 27

I.2.2.2.2.2.5 Privacy Extensions 30

I.2.2.2.2.2.6 Sensibilisierung der Nutzerinnen und Nutzer 32

I.3. Zugang zum Internet: Wettbewerb und Breitbandverfügbarkeit 33
I.3.1 Breitbandzugangstechnologien – Arten, Leistungsfähigkeit und Verbreitung. 35
I.3.1.1 Zugangstechnologien im Festnetz 35
I.3.1.1.1 DSL 35
I.3.1.1.2 TV-Kabel (Koaxialkabel) 37
I.3.1.1.3 Glasfaser (FTTx) 38
I.3.1.2 Kabellose Zugangstechnologien 39
I.3.1.2.1 Mobilfunklösungen 40
I.3.1.2.2 Satellit 44
I.3.1.2.3 Sonstige Funkzugangstechnologien 44
I.3.2 Wettbewerb im Internetzugangsmarkt 45
I.3.2.1 Wettbewerb verschiedener Infrastrukturen 46
I.3.2.2 Fortdauernde Bedeutung des Dienstewettbewerbs innerhalb einer Infrastruktur 48
I.3.2.3 Auswirkung zunehmender Verbreitung integrierter Geschäftsmodelle 50
I.3.3 Staatliche Handlungsoptionen zur Förderung von Breitbandverfügbarkeit 51
I.3.3.1 Berücksichtigung der Nachfrageentwicklung 51
I.3.3.2 Förderung von Kooperationen 52
I.3.3.3 Investitionszuschüsse 54
I.3.3.4 Universaldienstverpflichtung 55

II. Sicherheit im Internet 57
II.1. Schutz Kritischer Infrastrukturen im Internet 57
II.1.1 Einleitung 57
II.1.1.1 Kritische Informationsinfrastrukturen als Teil Kritischer Infrastrukuren 59
II.1.1.1.1 Definition – Kritische Infrastrukturen 60
II.1.1.1.2 Beispiele für die wachsende IT-Durchdringung der Kritischen Infrastrukturen 63

II.1.2 Bedrohungen Kritischer Infrastrukturen/Informationsinfrastrukturen 65
II.1.3 Vorhandene Regelungen und Maßnahmen zum Schutz kritischer Infrastrukturen beziehungsweise Informationsinfrastrukturen 73
II.1.3.1 Aktivitäten auf internationaler Ebene 73
II.1.3.2 Aktivitäten auf europäischer Ebene 76
II.1.3.2.1 Initiativen der Europäischen Union (EU) 76
II.1.3.2.2 Initiativen des Europarates 80
II.1.3.3 Aktiviäten auf Bundesebene 80
II.1.3.3.1 Akteure 80
II.1.3.3.2 Maßnahmen 85
II.2. Kriminalität im Internet 90
II.2.1 Grundlagen 91
II.2.1.1 Überblick und Eingrenzung des Themenfeldes „Kriminalität im Internet“ 91
II.2.1.2 Arbeitsdefinition 92
II.2.1.3 IT-Sicherheit 92
II.2.1.4 Motivation der Täter 93
II.2.1.5 Bedrohungen 94
II.2.1.5.1 Botnetze 94
II.2.1.5.2 Identitätsdiebstahl und -missbrauch 96
II.2.1.5.3 Spam 97
II.2.1.5.4 Professionalisierung/Organisierte Internetkriminalität 98
II.2.1.6 Angriffsmittel 101
II.2.1.6.1 Schadsoftware 101
II.2.1.6.1.1 Viren 101
II.2.1.6.1.2 Würmer 102
II.2.1.6.1.3 Trojaner 103
II.2.1.6.1.4 Backdoors 103
II.2.1.6.1.5 Rootkits 105

II.2.1.6.1.6 Spyware 105
II.2.1.6.2 Andere Angriffsmethoden 105
II.2.1.7 Infektions- und Angriffspunkte 106
II.2.1.7.1 Sicherheitslücken von Software 107
II.2.1.7.2 Social Engineering und Phishing 108
II.2.1.7.3 Ausnutzen des Anwenderverhaltens/Fehlendes Sicherheitsbewusstsein 110
II.2.1.7.4 Sonderproblem: Anbieter-/Produzentenverhalten 110
II.2.2 Schutzmöglichkeiten 111
II.2.2.1 Motivation der Angreifer verringern 111
II.2.2.2 Beseitigung oder Reduzierung von Infektions- und Angriffspunkten 112
II.2.2.2.1 Bereitstellung und Installation von Patches 112
II.2.2.2.2 Entwicklung sicherer Software 113
II.2.2.2.3 Schulung der Nutzer 113
II.2.2.2.4 Nutzung sicherer IT-Systeme 114
II.2.2.3 Reaktion auf akute Bedrohungen 114
II.2.3 Vorhandene Regelungen und Maßnahmen/Status Quo 115
II.2.3.1 Internationale Regelungen und Maßnahmen 115
II.2.3.1.1 Cybercrime Convention des Europarates von 2001 115
II.2.3.1.2 G8: Subgroup on High-Tech Crime 119
II.2.3.1.3 London Conference on Cyberspace 119
II.2.3.1.4 Bestrebungen auf Ebene der Vereinten Nationen (United Nations, UN) 120
II.2.3.2 Europäische Regelungen und Maßnahmen 121
II.2.3.2.1 Maßnahmen nach dem Stockholmer Programm 121
II.2.3.2.2 EU-Initiative: Safer Internet Action Plan (Nunmehr: Safer Internet plus Programme) 122
II.2.3.2.3 Entwurf EU-Richtlinie über Angriffe auf Informationssysteme 123
II.2.3.2.4 ENISA 123
II.2.3.2.5 Einrichtung eines europäischen IT-Notfallteams 124

II.2.3.2.6 Europol 125
II.2.3.3 Nationale Regelungen 126
II.2.3.3.1 Materiell-strafrechtliche Aspekte 126
II.2.3.3.2 Nebenstrafrechtliche Regelungen 129
II.2.3.3.3 Regelungen der Haftung und Verantwortlichkeit mit Steuerungswirkung für die IT-Sicherheit 130
II.2.3.3.3.1 Haftung des Angreifers 130
II.2.3.3.3.1.1 Deliktische Haftung gemäß § 823 Absatz 1 BGB 130
Verletzung des Eigentums 130
Leben, Körper, Gesundheit, Freiheit 131
Sonstige Rechte 132
II.2.3.3.3.1.2 Deliktische Haftung gemäß § 823 Absatz 2 BGB in Verbindung mit einem Schutzgesetz 133
II.2.3.3.3.1.3 Verantwortlichkeit nach Spezialgesetzen 133
II.2.3.3.3.2 Haftung des IT-Herstellers 133
II.2.3.3.3.2.1 Vertragliche Haftung 133
II.2.3.3.3.2.2 Außervertragliche Verschuldenshaftung nach § 823 Absatz 1 BGB 134
II.2.3.3.3.2.3 Außervertragliche Verschuldenshaftung nach § 823 Absatz 2 BGB 135
II.2.3.3.3.2.4 Außervertragliche, verschuldensunabhängige Haftung nach dem Produkthaftungsgesetz 135
II.2.3.3.3.2.5 Öffentlich-rechtliche Regelung der Produktsicherheit nach dem Produktsicherheitsgesetz 138
II.2.3.3.3.2.6 Zusammenfassung Haftung des IT-Herstellers 141
II.2.3.3.3.3 Haftung des IT-Nutzers 141
II.2.3.3.3.3.1 Vertragliche Haftung im Arbeitsverhältnis 142
II.2.3.3.3.3.2 Außervertragliche Verschuldenshaftung gemäß § 823 BGB 142
Verkehrssicherungspflichten privater IT-Nutzer 144
Verkehrssicherungspflichten professioneller IT-Nutzer 144

II.2.3.3.4 Infrastrukturbezogene Regelungen 145
II.2.3.3.5 Sonstige Regelungen mit Steuerungswirkung für die IT-Sicherheit 147
II.2.3.3.6 Rechtsdurchsetzung 147
II.2.3.3.6.1 Sicherung von Beweisen durch Strafverfolgungsbehörden 147
II.2.3.3.6.2 Erteilung von Bestandsdatenauskünften 148
II.2.3.3.6.3 Beauskunftung von Nutzungs- und Verkehrsdaten 149
II.2.3.3.6.4 Ermittlung von Inhaltsdaten 151
II.2.3.3.6.4.1 Beschlagnahme von Datenträgern 151
II.2.3.3.6.4.2 Öffentlich zugängliche Daten (virtuelle Streife) 151
II.2.3.3.6.4.3 Zugriff beim Telekommunikationsdienstleister 152
II.2.3.3.6.4.4 Online-Durchsuchung 153
II.2.3.3.6.4.5 Quellen-Telekommunikationsüberwachung 154
II.2.3.3.6.4.6 Einsatz von Ermittlungs-Software (so genannter Staatstrojaner) 155
II.2.3.3.6.5 Ausbildung und Training des Strafverfolgungspersonals 160
II.2.3.3.6.6 Technische und personelle Ausstattung der Strafverfolgungsbehörden 160
II.2.3.3.6.6.1 Computer-Forensik 160
II.2.3.3.6.6.2 Einsatz von Internettechnik für die Fahndung 161
II.2.3.3.6.6.3 Aus- und Weiterbildung des Personals 162
II.2.3.3.6.7 Einsatz von Anonymisierungstechnologien und Verschlüsselung 163
II.2.3.3.6.8 Internationale Zusammenarbeit 163
II.3. Spionage 165
II.3.1 Definition des Begriffs der Spionage 165
II.3.1.1 Vorhandene Definitionen 165
II.3.1.2 Abgrenzung vom Begriff Sabotage 166
II.3.2 Bedeutung des Internets für Spionage 167
II.3.3 Akteure 168
II.3.3.1 Hacker 168
II.3.3.2 Organisierte Kriminalität 170

II.3.3.3 Staaten ... 170
II.3.3.4 Wirtschaft ... 171
II.3.3.5 Weitere Akteure ... 172
II.3.4 Bedrohungen, Angriffsmittel und Schutzmöglichkeiten ... 172
II.3.5 Vorhandene Regelungen und Maßnahmen zum Schutz vor Spionage ... 172
II.3.5.1 Internationale Regelungen und Maßnahmen ... 172
II.3.5.2 Nationale Regelungen und Maßnahmen ... 172
II.3.5.2.1 Strafverfolgung ... 173
II.3.5.2.1.1 Landesverrat und Gefährdung der äußeren Sicherheit ... 173
II.3.5.2.1.2 Rechtsdurchsetzung ... 173
II.3.5.2.2 Sonstige Maßnahmen und Anreize ... 174
II.3.6 Risikoeinschätzung ... 175
II.4. Sabotage ... 177
II.4.1 Definition des Begriffs der Sabotage ... 177
II.4.2 Bedeutung des Internets für Sabotage ... 178
II.4.3 Akteure/Konstellationen ... 179
II.4.4 Bedrohungen, Angriffsmittel und Schutzmöglichkeiten ... 180
II.4.4.1 Angriff mit hochentwickelter Malware (zum Beispiel Stuxnet) ... 180
II.4.4.2 DDoS-Angriff auf Estland ... 181
II.4.5 Vorhandene Regelungen und Maßnahmen zum Schutz vor Sabotage ... 182
II.4.5.1 Internationale Regelungen und Maßnahmen ... 182
II.4.5.2 Nationale Regelungen und Maßnahmen ... 182
II.4.5.2.1 Strafverfolgung ... 182
II.4.5.2.1.1 Einschlägige Normen ... 182
II.4.5.2.1.2 Steuerungswirkung des Strafrechts ... 183
II.4.5.2.1.3 Rechtsdurchsetzung ... 184
II.4.5.2.2 Infrastrukturbezogene Regelungen ... 184
II.4.5.2.3 Initiativen ... 185

II.4.6 Defizitanalyse 185
II.4.7 Risikoeinschätzung 186

III. Handlungsempfehlungen 188

IV. Sondervoten 243

V. Dokumentation der Beteiligung der interessierten Öffentlichkeit an der Arbeit der Projektgruppe über die Online-Beteiligungsplattform enquetebeteiligung.de 244

VI. Anlagen 258

VI.1. Öffentliches Expertengespräch zum Thema „Sicherheit im Netz“ 258

VI.2. Öffentliches Expertengespräch zum Thema „IPv6 – Sicherheitsaspekte“ 259

VI.3. Nicht öffentliches Expertengespräch zum Thema „Internetkriminalität“ 260

Abkürzungsverzeichnis 261

Literatur- und Quellenverzeichnis 265

Mitglieder der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft 266

Grußwort des Vorsitzenden

I. Zugang zum Internet und Infrastruktur des Internets

I.1. Einleitung

Die Infrastruktur des Internets sowie die damit verbundenen technischen Standards und Kooperationsprozesse haben sich zunächst in einem nicht kommerziellen Rahmen entwickelt. Das Netz war zu Beginn ein reines Forschungsnetz. Die Internetstandards und RFCs (Request for Comments)[1] sind auf der Basis freier Entwicklung entstanden und wurden später im freien und wettbewerblichen Zusammenspiel der verschiedenen Beteiligten weiterentwickelt. Der Staat war eher als Teilnehmer beim Aufbau dieser Infrastruktur – zunächst im militärischen Bereich, später insbesondere im Forschungsbereich – beteiligt, weniger aber durch politisch-regulatorische Steuerung.

In der Bundesrepublik Deutschland kommt dem Staat gemäß Artikel 87 f Absatz 1 des Grundgesetzes (GG) ein Verfassungsauftrag zu, „angemessene und ausreichende Dienstleistungen“ bei der Telekommunikationsinfrastruktur zu gewährleisten. Zu erbringen sind diese Dienstleistungen jedoch gemäß Artikel 87 f Absatz 2 GG durch private Anbieter oder aber durch die aus dem Sondervermögen der Deutschen Bundespost hervorgegangenen Unternehmen.

Auf europäischer Ebene „trägt die Union zum Auf- und Ausbau transeuropäischer Netze in den Bereichen der Verkehrs-, Telekommunikations- und Energieinfrastruktur bei“.[2] Angesichts der heutigen Bedeutung des Internets für alle Lebensbereiche fällt auch die Infrastruktur des Internets in Deutschland und Europa unter diese grundsätzlichen Vorgaben. Ungeachtet dieser Gewährleistungsfunktion des Staates hat sich das Internet aber seit seinen Anfängen vorrangig aufgrund von freiwilligen, offenen technischen Standards und Kooperationsvereinbarungen der verschiedenen Beteiligten weiterentwickelt. Regulatorische Eingriffe für einen Ausbau waren weitestgehend nicht erforderlich. In der Folge konnte sich eine dezentrale technische Struktur des Netzes entwickeln, die durch internationale Governance-Formen verwaltet wird, welche auf Kooperation und breite Beteiligung sowie

---

[1] Unter Request for Comments (RFC) werden Dokumente verstanden, die technische und organisatorische Spezifikationen sowie Richtlinien über das Internet enthalten. Nur RFCs, die von der Internet Engineering Task Force (IETF) verabschiedet wurden, haben einen normativen Charakter und gelten als Internetstandard. Nähere Informationen zu RFCs sind online auf den Seiten der IETF abzurufen untern: http://www.ietf.org/ beziehungsweise http://www.rfc-editor.org/

[2] Artikel 170 Absatz 1 Vertrag über die Arbeitsweise der Europäischen Union (AEUV).

Standards und Normen setzen.[3] Es darf daher mit Recht bezweifelt werden, ob es eine vergleichbare dezentrale und dynamische Entwicklung des Internets bei einer durchgängigen staatlichen oder privatwirtschaftlichen Regulierung und Einflussnahme gegeben hätte.

Das Prinzip von nur geringen staatlich-regulatorischen Eingriffen in die Struktur und die technischen Standards des Internets hat sich beim Aufbau des Internets weitgehend bewährt und sollte hinsichtlich dieses Aspekts auch Grundlage für seine Weiterentwicklung bleiben.[4] Zugleich hat aber auch die zunehmende Diskussion über Netzneutralität gezeigt, dass Fragen des Zugangs und der Entgeltregulierung sowie von Missbrauchs- und Diskriminierungsverboten Themenbereiche sind, die Gegenstand staatlicher Regulierung sind beziehungsweise werden können, um die Diskriminierungsfreiheit im Internet in Deutschland auch weiterhin zu gewährleisten.[5]

Im Bereich der technischen Standardisierung und der Einführung neuer Protokolle, die exemplarisch an der Einführung des Internetprotokolls Version 6 (IPv6) betrachtet wird, kommt dem Staat nur eine begleitende Rolle zu (siehe hierzu Kapitel I. 2). Eine stärker ordnende Funktion hat der Staat jedoch im Bereich des Internetzugangs zu übernehmen, wenn es darum geht, einen funktionsfähigen Wettbewerb in diesem üblicherweise auch national begrenzten Markt zu gewährleisten, und gerade auch hierdurch die Verfügbarkeit einer leistungsfähigen Zugangsinfrastruktur zu sichern (siehe hierzu Kapitel I. 3).

I.2. Einführung und Auswirkungen neuer Protokolle

I.2.1 Förderung der Einführung neuer Protokolle

Die Einführung und Verbreitung neuer Protokolle vollzieht sich heute im Zusammenwirken von Wirtschaft, Wissenschaft und Politik unter Beteiligung der relevanten Standardisierungsgremien, wie zum Beispiel der Internet Engineering Task Force (IETF), der International Telecommunication Union (ITU) oder des Institute of Electrical and Electronics

---

[3] Das Thema Governance ist Gegenstand der Beratungen der Projektgruppe Internationales und Internet Governance. Hinsichtlich des Themas Standards und Normen sei auf den Bericht der Projektgruppe Interoperabilität, Standards, Freie Software verwiesen.

[4] Der Schutz des Internets als Kritische Infrastruktur für grundlegende Dienste der Daseinsvorsorge und der Aufrechterhaltung des Wirtschaftskreislaufes stellt hingegen eine gesamtgesellschaftliche Aufgabe dar und erfordert ein Zusammenwirken von Staat, Wirtschaft und Gesellschaft. Siehe hierzu ausführlich Kapitel II.1.

[5] Zum Thema Netzneutralität vgl. den vierten Zwischenbericht der Enquete-Kommission Internet und digitale Gesellschaft, Bundestagsdrucksache 17/8536. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zwischenberichte/Zwischenbericht_Netzneutralitaet_1708536.pdf

Engineers (IEEE) sowie dem World Wide Web Consortium (W3C). Die dort etablierten breiten Beteiligungsstrukturen für alle interessierten Gruppen, einschließlich der Nutzer, stellen weitestgehend sicher, dass die Interessen aller zu einem bestmöglichen Ausgleich gebracht werden. Die Schaffung offener Standards bietet dabei eine wichtige Grundlage für die Weiterentwicklung des Internets und ist grundsätzlich auch im Interesse der Nutzer.

Dem Staat kommt eine begleitende Rolle zu, um solche Standardisierungen zu fördern und nur bei Bedarf eventuellen problematischen Folgewirkungen entgegenzuwirken.

Verpflichtende staatliche Planungen oder Vorgaben zur Umstellung von Protokollen ohne Berücksichtigung der Marktsituation haben in der Vergangenheit nicht immer zum angestrebten Ergebnis geführt. Beispiele dafür sind das Open Systems Interconnection(OSI)-Referenzmodell sowie der Standard X.400 zur Übertragung elektronischer Nachrichten.

Die International Organization for Standardization (ISO) hat das ISO/OSI-Schichtenmodell als abstraktes Modell der Datenübertragung zwischen offenen, heterogenen Netzwerken entwickelt (festgeschrieben 1984 in der ISO-Norm 7489). Dieses bildet den Prozess des Datenaustausches in sieben einzelnen, aufeinander aufbauenden Schichten ab. Ziel war die Entwicklung von standardisierten Kommunikationsprotokollen, da zu dieser Zeit vorwiegend proprietäre und miteinander nicht kompatible Protokolle existierten.[6] Bereits vor der Entwicklung des ISO/OSI-Schichtenmodells entstand jedoch das Transmission Control Protocol/Internet Protocol(TCP/IP)-Referenzmodell (RFC 1122).[7] Dieses basierte im Gegensatz zum theoretisch entworfenen ISO/OSI-Schichtenmodell auf der dem Internet zugrunde liegenden TCP/IP-Protokollfamilie, welche sich bereits vor der Definition des Modells praktisch bewährt hatte.[8] Infolgedessen setzte sich das TCP/IP-Referenzmodell durch.[9]

Wie das ISO/OSI-Schichtenmodell konnte sich auch die X.400-Norm (Message Handling System) nicht als allgemeiner Standard zur Übermittlung von E-Mails etablieren. X.400 wurde 1984 von der ISO und dem CCITT (Comité Consultatif International Téléphonique et Télégraphique, heute International Telecommunication Union – Telecommunication Standardization Sector, ITU-T) als Protokoll der Anwendungsschicht des ISO/OSI-

---

[6] Vgl. Meinel, Christoph/ Sack, Harald: Internetworking – Technische Grundlagen und Anwendungen. 2012, S. 41f.

[7] Vgl. ebd., S. 53.

[8] Vgl. ebd., S. 51f.

[9] Vgl. ebd., S. 42.

Schichtenmodells herausgegeben. Heute findet X.400 vorwiegend Anwendung als sicherer Übertragungsstandard für Geschäftskommunikation.[10]

In der Regel erfolgt eine Einführung neuer Protokolle schrittweise. Die Vorgängerversionen neuer Protokolle sind noch für einen längeren Zeitraum im Parallelbetrieb nutzbar oder können alternativ über so genanntes Tunneling von den neuen Protokollen genutzt werden. Es hat sich gezeigt, dass daher eine Unterstützung öffentlicher Stellen oder gemeinnütziger Einrichtungen für die mit einer Umstellung notwendigen Investitionen nur in Ausnahmefällen erforderlich ist. Aufgrund eines fließenden Übergangs können die technologischen Neuerungen in die üblichen Investitionszyklen integriert werden.

Für die Umstellung auf IPv6 hat zum Beispiel die Bundesstelle für Informationstechnik (BIT) – der zentrale IT-Dienstleister der Bundesverwaltung – ein Beratungsprodukt zu IPv6 eingeführt. Über dieses wird Bundesbehörden gebündeltes Fachwissen beim Einsatz und der Optimierung von IPv6-relevanten IT-Prozessen aus verschiedenen Kompetenzfeldern (beispielsweise Technik oder Organisation) und umfassende Erfahrungen aus einer Vielzahl erfolgreicher Projekte zugänglich gemacht. Ähnliche Aktivitäten für den Bereich Sicherheit im Umfeld von IPv6 finden über das Bundesamt für Sicherheit in der Informationstechnik (BSI) durch die Veröffentlichung eines Leitfadens für eine sichere IPv6-Netzwerkarchitektur[11] statt.

I.2.2 Absicherung gegenüber potenziellen negativen Effekten

In einzelnen Bereichen kann es aber tatsächlich notwendig sein, dass der Staat auf drohende Negativfolgen neuer Standards hinweist und auf einen gebotenen Schutz der Interessen aller Beteiligter hinwirkt. Dies kann je nach Art und Gestaltung des technischen Standards unterschiedliche Bereiche betreffen.

I.2.2.1 Auswirkung auf den Wettbewerb

Negative Auswirkungen kann die Oktroyierung neuer Standards durch Einzelne, Gruppen, den Staat oder besonders marktmächtige Unternehmen haben. Kleinere Wettbewerber,

---

[10] Siehe das Angebot BusinessMail X.400 der Deutschen Telekom AG.

[11] Der Leitfaden für eine sichere IPv6-Netzwerkarchitektur des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_lana_leitfaden_IPv6_pdf.pdf?__blob=publicationFile

Anbieter von Diensten oder Produkten in Nischenmärkten, beziehungsweise auch nicht kommerzieller Beteiligte könnten hiervon besonders betroffen sein.

Sofern nicht schon die etablierten Strukturen oder der Markt dazu führen, dass neue Standards offen und diskriminierungsfrei allen Marktbeteiligten zur Verfügung stehen und ihre Anwendung keinen Beteiligten diskriminiert, ist deshalb im Einzelfall ein Einschreiten der Wettbewerbsbehörden oder auch ein legislatives Handeln des Staates zur Sicherung eines fairen Wettbewerbs denkbar.

Gleichzeitig darf aber der Schutz überholter Geschäftsmodelle und Technologien nicht der notwendigen technischen Fortentwicklung im Wege stehen. Schutzanordnungen müssen sich folglich auf möglichst geringe Eingriffe, wie etwa die Anordnung von Übergangszeiten, beschränken.

I.2.2.2 Exkurs: Sicherheitsaspekte bei der Einführung des neuen Internetprotokolls Version 6 (IPv6)[12]

Der vorliegende Exkurs zeigt nach einer kurzen technischen Einführung die mit IPv6 verbundenen Chancen und Herausforderungen auf, wobei der Aspekt der Sicherheit im Vordergrund steht.

I.2.2.2.1 Einführung

I.2.2.2.1.1 Das Internetprotokoll Version 4 (IPv4)

Das Internetprotokoll (IP) ist verantwortlich für den Transport von Datenpaketen zwischen den an das Internet angeschlossenen Endgeräten – beispielsweise einem Computer oder Smartphone. Damit die Datenpakete zum richtigen Ziel geleitet werden (englisch: routing), wird jeder Netzwerkschnittstelle (englisch: interface) eine eindeutige Adresse zugewiesen: die IP-Adresse.

Das aktuell verwendete Internetprotokoll Version 4, kurz IPv4, entstand bereits vor über 30 Jahren.[13] Die darauf basierenden IPv4-Adressen umfassen 32 Bit, wodurch rein rechnerisch

---

[12] Die Mitglieder der Projektgruppe danken den sachverständigen Anhörpersonen des Expertengesprächs zum Thema „IPv6 – Sicherheitsaspekte“ für ihre zahlreichen Hinweise und Anregungen. Es sei an dieser Stelle an auch auf die Stellungnahmen der Experten verwiesen. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/index.jsp

[13] IPv4 wurde 1981 definiert in RFC 791 – Internet Protocol. definiert. Online abrufbar unter: http://tools.ietf.org/html/rfc791

knapp 4,3 Milliarden Adressen (2^{32}) zur Anbindung von Endgeräten an das Internet zur Verfügung stehen – abgesehen von Adressbereichen, die für besondere Zwecke reserviert[14] oder in der Anfangszeit des Internets großzügig an Unternehmen oder Regierungsbehörden vergeben wurden.[15]

I.2.2.2.1.2 Vergabe der IP-Adressen

Die Internet Assigned Numbers Authority (IANA) – weltweit zuständig für die Verwaltung der IP-Adressen – vergibt IP-Adressen in großen, zusammenhängenden Blöcken an die fünf regionalen Registrierungsorganisationen (Regional Internet Registries, RIR)[16]. Diese unterteilen die Adressblöcke wiederum in kleinere Segmente, die sie ihren Mitgliedern, den Local Internet Registries (LIR), zuweisen. Die meisten LIR, welche letztendlich IP-Adressen an Endkunden vergeben, sind Internet Service Provider (ISP), Unternehmen und Behörden.[17]

I.2.2.2.1.3 IPv4-Adressknappheit

Im Februar 2011 hat die IANA die letzten fünf /8-Adressblöcke[18] an die RIR verteilt. Der IPv4-Adressvorrat ist damit erschöpft.[19] Die für Europa zuständige regionale Registrierungsorganisation RIPE hat im September 2012 begonnen, die letzten ihr zur Verfügung stehenden IPv4-Adressen zu vergeben. Laut RIPE ist es „now imperative that all stakeholders deploy IPv6 on their networks to ensure the continuity of their online operations and the future growth of the Internet“.[20] Schließlich steigt der Bedarf an IP-Adressen stetig an, da Entwicklungen wie die mobile Internetnutzung, das Internet der Dinge und das Internet der Energie für jedes Gerät, das mit dem Internet verbunden wird, eine eigene IP-Adresse beanspruchen.

---

[14] Einen Überblick liefert RFC 5735 – Special Use IPv4 Addresses. Online abrufbar unter: http://tools.ietf.org/html/rfc5735

[15] Vgl. IANA: IANA IPv4 Address Space Registry. Online abrufbar unter: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

[16] Die fünf RIR sind für die Region Afrika AfriNIC, für die Region Asien/ Pazifik APNIC, für die Region Europa, den Nahen Osten und Zentralasien RIPE NCC, für die Region Lateinamerika und die Karibik LACNIC und für die Region Nordamerika ARIN.

[17] Ein Überblick über alle LIR, die in Deutschland tätig sind, kann online abgerufen werden unter: https://www.ripe.net/membership/indices/DE.html

[18] Die CIDR-Notation oder auch Präfix-Notation basiert auf dem Verfahren des Classless Inter-Domain Routing (CIDR). Demnach wird eine IP-Adresse in ein Präfixteil und einen Hostteil aufgeteilt. Ein /8-Präfix umfasst einen zusammenhängenden IPv4-Adressblock von über 16 Millionen IP-Adressen. CIDR ist in RFC 4632 – Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan definiert. Online abrufbar unter: http://tools.ietf.org/html/rfc4632

[19] Vgl. RIPE NCC: RIPE NCC Receives Final /8 of IPv4 Address Space from IANA. 3. Februar 2012. Online abrufbar unter: http://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-receives-final-8-of-ipv4-address-space-from-iana

[20] Vgl. RIPE NCC: RIPE NCC Begins to Allocate IPv4 Address Space From the Last /8. 14 September 2012. Online abrufbar unter: http://www.ripe.net/internet-coordination/news/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8

I.2.2.2.1.4 Das Internetprotokoll Version 6 (IPv6)

Da bereits abzusehen war, dass der mit IPv4 zur Verfügung stehende Adressraum in wenigen Jahren erschöpft sein würde, hat die IETF in den 1990er-Jahren mit der Entwicklung eines neuen Protokolls begonnen: dem Internetprotokoll Version 6, kurz IPv6.[21]

Mit der Umstellung auf IPv6 vergrößert sich der Adressraum um ein Vielfaches. IPv6-Adressen bestehen aus 128 Bit, wodurch künftig 340 Sextillionen Adressen (2^{128}) zur Verfügung stehen.

I.2.2.2.1.5 Aufbau von IPv6-Adressen

IPv6-Adressen setzen sich aus drei Bereichen zusammen: dem Global-Routing-Präfix und dem Subnetz Identifier, welche zusammen ein 64 Bit umfassendes Netzwerk-Präfix bilden, sowie dem Interface Identifier.[22]

bilden zusammen das **Netzwerk Präfix** (64 Bit)		identifiziert die **Netzwerkschnittstelle** (64 Bit)
Global-Routing-Präfix	Subnetz ID	Interface ID
besteht aus n Bits	besteht aus m Bits	besteht aus 128 – n – m Bits

Global Routing Präfix: identifiziert den vom ISP zugewiesenen Bereich

Subnetz ID: durch den Endkunden zugewiesen

Interface ID: entweder automatisch aus der MAC-Adresse des Endgerätes abgeleitet oder per Zufall durch die Aktivierung der Privacy Extensions generiert

Abb. 1: Aufbau von IPv6-Adressen[23]

Die regionale Registrierungsorganisation RIPE hat eine Richtlinie[24] hinsichtlich der Verteilung und Zuweisung von IPv6-Adressen erlassen. Danach erhalten die LIR von der RIPE Global-Routing-Präfixe der Größe /32, das heißt die ersten 32 Bit des 64 Bit umfassenden Netzwerk-Präfix sind fest vorgegeben; die restlichen 32 Bit stehen zur Bildung

[21] IPv6 wird definiert in RFC 2460 – Internet Protocol, Version 6 (IPv6) – Specification. Online abrufbar unter : http://tools.ietf.org/html/rfc2460

[22] Unter IPv6 stehen je nach Verwendungszweck drei Arten von IPv6-Adresstypen zur Verfügung: Unicast, Anycast und Multicast. Unicast-Adressen gliedern sich wiederum in mehrere Untertypen auf. Wird innerhalb dieses Berichts von IPv6-Adressen gesprochen, so sind Global-Unicast-Adressen gemeint. Zum Aufbau von IPv6-Adressen vgl. RFC 4291 – IP Version 6 Addressing Architecture. Online abrufbar unter: http://tools.ietf.org/html/rfc4291

[23] Vgl. RFC 2460 – Internet Protocol, Version 6 (IPv6) – Specification. Online abrufbar unter : http://tools.ietf.org/html/rfc2460

[24] Vgl. RIPE: IPv6 Address Allocation and Assignment Policy. Online abrufbar unter: http://www.ripe.net/ripe/docs/ripe-552

von Teilnetzen zur Verfügung.[25] Ein LIR – beispielsweise ein Internet Service Provider – vergibt den ihm zugewiesenen IPv6-Adressraum wiederum nach eigenen Regeln[26] an seine Endkunden, wobei Global-Routing-Präfixe der Größe /56 sowie /48 bevorzugt zugeteilt werden.[27]

Der zweite Teil einer IPv6-Adresse, der Subnetz Identifier, kann vom Endkunden frei gewählt werden. Je nach Größe des Global-Routing-Präfix, welches der Endkunde von seinem ISP erhalten hat, können mehrere eigene Teilnetze gebildet werden. Dies kann beispielsweise für Unternehmen relevant sein, die für jeden Standort ein eigenes Netzwerk einrichten wollen. Ausgehend von einem /56-Präfix stehen 8 Bit zur Bildung eigener Subnetze zur Verfügung – dies entspricht 256 Subnetzen mit jeweils 2^{64} IPv6-Adressen.

Die letzten 64 Bit einer IPv6-Adresse bilden den Interface Identifier. Dieser dient dazu, ein Endgerät innerhalb eines Netzwerks eindeutig zu identifizieren. Die Vergabe des Interface Identifier erfolgt automatisch, wobei zu dessen Bildung zwei Optionen[28] zur Verfügung stehen: Bildung auf Basis der weltweit einmaligen Media-Access-Control(MAC)-Adresse des Endgerätes[29] oder Bildung auf Basis regelmäßig neu erzeugter Zufallszahlen mittels Privacy Extensions[30].

I.2.2.2.1.6 Technische Neuerungen von IPv6 gegenüber IPv4

Neben dem stark vergrößerten Adressraum gehen mit IPv6 diverse technische Neuerungen einher.[31] Dies sind u.a.:[32]

---

[25] In Einzelfällen können auch kürzere Präfixe vergeben werden. Vgl. RIPE: IPv6 Address Allocation and Assignment Policy, Absatz 4.3. Minimum allocation sowie 4.4. Consideration of IPv4 infrastructure. Online abrufbar unter: http://www.ripe.net/ripe/docs/ripe-552

[26] In RFC 3177 – IAB/IESG Recommendations on IPv6 Address Allocations to Sites wurde die Vergabe von /48-Präfixen empfohlen. Die IETF hat diese Empfehlung in RFC 6177 relativiert, da ein /48-Präfix möglicherweise nicht den Anforderungen jedes Endkunden entspricht. Vgl. RFC 6177 – IPv6 Address Assignment to End Sites. Online abrufbar unter: http://tools.ietf.org/html/rfc6177

[27] Vgl. RIPE: Understanding IP Adressing. Online abrufbar unter: http://www.ripe.net/internet-coordination/press-centre/understanding-ip-addressing

[28] Neben den im Text genannten Optionen gibt es unter bestimmten Voraussetzungen weitere Möglichkeite den Interface Identifier zu erzeugen. Siehe dazu Anhang 1 des RFC 4291 – IP Version 6 Addressing Architecture. Online abrufbar unter: http://tools.ietf.org/html/rfc4291

[29] Die Bildung des Interface Identifier erfolgt nach dem vom IEEE definierten Modified-EUI-64-Format. Siehe dazu RFC 4291 – IP Version 6 Addressing Architecture. Online abrufbar unter: http://tools.ietf.org/html/rfc4291, sowie die EUI-64 Guidelines der IEEE. Online abrufbar unter: http://standards.ieee.org/develop/regauth/tut/eui64.pdf

[30] Die Bildung des Interface Identifier auf Basis der Privacy Extensions wird in RFC 4941 definiert. Vgl. RFC 4941 – Privacy Extensions for Stateless Address Autoconfiguration in IPv6. Online abrufbar unter: http://tools.ietf.org/html/rfc4941

[31] Im öffentlichen Expertengespräch der Projektgruppe zum Thema „IPv6 – Sicherheitsaspekte“ wurde darauf hingewiesen, dass „viele der neuen Funktionen von IPv6 […] im Laufe der Zeit auch in IPv4 als Workaround eingebaut worden [sind].“ Beispielhaft wurde „die

– **Wiederherstellung des Ende-zu-Ende-Prinzips:** Da durch IPv6 jedem Gerät eine individuelle IP-Adresse zugewiesen werden kann, ist die Verwendung des Network Address Translation (NAT)-Verfahrens nicht mehr notwendig. Das NAT-Verfahren widerspricht dem ursprünglichen Gedanken der direkten Erreichbarkeit eines Rechners im Internet. Es wurde jedoch entwickelt, um der Adressknappheit unter IPv4 zu begegnen. Mittels NAT, welches üblicherweise auf einem Router implementiert ist, werden die privaten IP-Adressen eines Netzwerks, beispielsweise eines Unternehmens, durch eine öffentliche Adresse ersetzt.[33] Die einzelnen Geräte kommunizieren somit über dieselbe IP-Adresse ins Internet und werden durch NAT hinter dem Router quasi „versteckt". Dadurch sind sie über das Internet nicht direkt ansprechbar.
Dies ändert sich mit IPv6: Durch den mit der Einführung von IPv6 einhergehenden Wegfall von NAT ist eine direkte Kommunikation zwischen mehreren Rechnern wieder möglich. Da nun das Zwischenschalten eines fremden Servers zur Herstellung der Verbindung nicht mehr erforderlich ist, erhöht sich durch die Möglichkeit der Ende-zu-Ende-Verschlüsselung auch die Sicherheit bei der Kommunikation.[34] Die

---

Internet Protocol Security (IPsec), welche heutzutage zur Verschlüsselung von Kommunikation im Internet und zwischen Standorten von Unternehmen verwendet werde", genannt.
Protokoll des öffentlichen Expertengesprächs zum Thema „IPv6 – Sicherheitsaspekte" der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012, S. 10, 11 und 14. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Protokoll.pdf

[32] Zu den Vorteilen von IPv4 gegenüber IPv6 siehe: Bundesministerium für Wirtschaft und Technologie (Hrsg.): Strategiepapier zur Förderung der Einführung von IPv6 – AG2 Sonderthemengruppe „Einführung von IPv6". Nationaler IT-Gipfel München 2011, S. 9. Online abrufbar unter: http://www.it-gipfel.de/IT-Gipfel/Redaktion/PDF/strategiepapier-ag-2,property=pdf,bereich=itgipfel,sprache=de,rwb=true.pdf

[33] Sofern die Übersetzung einer privaten in eine öffentliche IP-Adresse bereits auf der Ebene des Provider-Netzwerks stattfindet, spricht man von Carrier Grade NAT. Siehe hierzu auch: Boeddinghaus, Wilhelm/Meinel, Christoph/Sack, Harald: Einführung von IPv6 in Unternehmensnetzen. Ein Leitfaden. Technische Berichte Nr. 52 des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam. 2011, S. 11f. Online abrufbar unter: http://www.hpi.uni-potsdam.de/fileadmin/hpi/source/Technische_Berichte/HPI_52_ipv6_leitfaden.pdf

[34] Vgl. Boeddinghaus, Wilhelm/Meinel, Christoph/Sack, Harald: Einführung von IPv6 in Unternehmensnetzen. Ein Leitfaden. Technische Berichte Nr. 52 des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam. 2011, S. 16f. Online abrufbar unter: http://www.hpi.uni-potsdam.de/fileadmin/hpi/source/Technische_Berichte/HPI_52_ipv6_leitfaden.pdf. sowie Bundesministerium für Wirtschaft und Technologie (Hrsg.): Das Internetprotokoll der Version 6 (IPv6) – Chancen und Herausforderungen für den Wirtschaftsstandort Deutschland – Abschlussbericht. Juni 2012. S. 11f. Online abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/bmwi-internetprotokoll-ipv6,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

direkte Adressierung eines Geräts ist zudem für Entwicklungen wie dem Internet der Dinge[35] von besonderer Bedeutung.

- **Autokonfiguration:** Durch die Autokonfiguration[36] von Endgeräten und Netzwerkkomponenten wird die Administration eines Netzwerks erleichtert, da sich ein Gerät, welches neu in ein Netzwerk eingebunden wird, selbst eine IP-Adresse zuweisen kann.[37] Eine Adresszuweisung mittels Dynamic Host Configuration Protocol(DHCP)-Server[38] oder eine manuelle Konfiguration sind somit nicht erforderlich. Die Funktion der Autokonfiguration ist beispielweise für Sensornetze[39], aber auch für die Integration verschiedener Geräte in ein Heimnetzwerk wichtig.
- **Mobile IPv6:** Durch Mobile IPv6[40] kann ein Anwender permanent über „ein mobiles Endgerät mit seinem Heimnetzwerk verbunden sein“ und „ohne Unterbrechung in ein anderes Netz […] wechseln (Roaming)“.[41]
- **Integration von IPsec:** Der Sicherheitsstandard Internet Protocol Security (IPsec)[42] dient dem „vertraulichen, integeren und authentifizierten Transport von IP-Paketen“[43].

---

[35] Siehe zum Begriff Internet der Dinge: Boeddinghaus, Wilhelm/Meinel, Christoph/Sack, Harald: Einführung von IPv6 in Unternehmensnetzen. Ein Leitfaden. Technische Berichte Nr. 52 des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam. 2011, S. 17f. Online abrufbar unter: http://www.hpi.uni-potsdam.de/fileadmin/hpi/source/Technische_Berichte/HPI_52_ipv6_leitfaden.pdf sowie Horvarth, Sabine: Aktueller Begriff – Internet der Dinge. Deutscher Bundestag – Wissenschaftlicher Dienst – Fachbereich WD 10 – Kultur, Medien, Sport. 17.07.2012. Online abrufbar unter: http://www.bundestag.de/dokumente/analysen/2012/Internet_der_Dinge.pdf

[36] Die zustandslose Adresskonfiguration unter IPv6 wird definiert in RFC 4862 – IPv6 Stateless Address Autoconfiguration. Online abrufbar unter: http://tools.ietf.org/html/rfc4862

[37] Vgl. Hagen, Silvia: IPv6 – Grundlagen, Funktionalität, Integration. 2009, S. 124.

[38] Zur IP-Adresszuweisung mittels DHCP-Server siehe beispielsweise: Zisler, Harald. Computer-Netzwerke – Grundlagen, Funktionsweise, Anwendung. 2012, S. 122.

[39] Vgl. Boeddinghaus, Wilhelm/Meinel, Christoph/Sack, Harald: Einführung von IPv6 in Unternehmensnetzen. Ein Leitfaden. Technische Berichte Nr. 52 des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam. 2011, S. 18f. Online abrufbar unter: http://www.hpi.uni-potsdam.de/fileadmin/hpi/source/Technische_Berichte/HPI_52_ipv6_leitfaden.pdf sowie Bundesministerium für Wirtschaft und Technologie (Hrsg.): Das Internetprotokoll der Version 6 (IPv6) – Chancen und Herausforderungen für den Wirtschaftsstandort Deutschland – Abschlussbericht. Juni 2012. S. 12. Online abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/bmwi-internetprotokoll-ipv6,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

[40] Mobile IPv6 wird definiert in RFC 6275 – Mobility Support in IPv6. Online abrufbar unter: http://tools.ietf.org/html/rfc6275

[41] Protokoll des öffentlichen Expertengesprächs zum Thema „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012, S. 15. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Protokoll.pdf. Siehe auch die Ausführugen zu Mobile IPv6 in: Hagen, Silvia: IPv6 – Grundlagen, Funktionalität, Integration. 2009, S. 278ff.

[42] IPsec wird definiert in RFC 4301 – Security Architecture for the Internet Protocol. Online abrufbar unter: http://tools.ietf.org/html/rfc4301

[43] Eckert, Claudia: IT-Sicherheit. 2012, S. 762.

Die Nutzung von IPsec war zwar bereits unter IPv4 möglich, musste jedoch manuell implementiert werden. Unter IPv6 ist IPsec hingegen ein integrierter Bestandteil.

Die Sicherheitsaspekte, die im Zusammenhang mit der Vergrößerung des Adressraums, der Wiederherstellung des Ende-zu-Ende-Prinzips und dem Wegfall von NAT, der Autokonfiguration sowie dem unterbrechungsfreien Roaming in ein anderes Netz stehen, werden in Kapitel I.2.2.2.2, Abschnitt Herausforderungen, erläutert.

I.2.2.2.1.7 Notwendigkeit der Umstellung auf IPv6

Die weltweite Einführung von IPv6 schreitet immer schneller voran.[44] „Zu Beginn wurde die Einführung von IPv6 stark aus Asien heraus getrieben, da dort verhältnismäßig wenig IPv4-Adressraum vorhanden war, jedoch aufgrund zahlreicher aufstrebender Länder ein enormer Adressbedarf entstand. Mittlerweile hat das Thema IPv6 auch in den USA Fahrt aufgenommen. Dort sind zum einen viele Hersteller von Netzwerkkomponenten, Betriebssystemen und weiterer Software mit IPv6-Support angesiedelt, zudem treiben seit kurzem viele bekannte Content Provider wie Akamai, Google, Facebook oder Yahoo! das Thema IPv6 voran.“[45]

Auch in Deutschland ist die Auseinandersetzung mit dem Thema IPv6 geboten. Zum einen ist es notwendig, dass vor allem die großen deutschen ISP beginnen IPv6 einzuführen.[46] Nur so können die Anwender die zunehmend auch über IPv6 angebotenen Dienste nutzen.[47] „Erst wenn [die großen Zugangsprovider] eine nennenswerte Anzahl von Endkunden (auch) über IPv6 anbinden, wird sich die Gesamtdurchdringung erkennbar erhöhen.“[48] Zum anderen ist

---

[44] Im Jahr 2010 waren weltweit circa 54 Milliarden /56-Präfixe verteilt, wohingegen diese Zahl ein Jahr später auf über 159 Millarden angestiegen ist. Siehe dazu beispielsweise die Statistik der APNIC zur weltweiten Zuweisung von IPv6-Adressen unter http://www.apnic.net/publications/research-and-insights/stats/ipv6-distribution. Siehe auch: Kühne, Mirjam: Networks with IPv6 - One Year Later. 5. Mai 2012. Online abrufbar unter: https://labs.ripe.net/Members/mirjam/networks-with-ipv6-one-year-later

[45] Schriftliche Stellungnahme von Wolfgang Fritsche im Rahmen des öffentlichen Expertengespräches „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 2. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Stellungnahme_Fritsche.pdf

[46] Vgl. IPv6 German Council: Nationaler IPv6-Aktionsplan für Deutschland. Potsdam, 14. Mai 2009, S. 8. Online abrufbar unter: http://www.ipv6council.de/fileadmin/summit09/Aktionsplan.pdf

[47] Am 6. Juni 2012 fand der World IPv6 Launch Day statt. An diesem Tag haben verschiedene Internet Service Provider, Hersteller von Netzwerkkomponenten (Router) sowie Inhalteanbieter IPv6 permanent eingeführt. Zur Übersicht über die Teilnehmer am World IPv6 Launch Day siehe: http://www.worldipv6launch.org/participants/

[48] Schriftliche Stellungnahme von Ulrich Kühn im Rahmen des öffentlichen Expertengespräches „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 2. Online abrufbar unter:

die „Einführung von IPv6 in Deutschland auch eine Standortfrage“.[49] Die deutsche Wirtschaft muss sich – insbesondere auch im Hinblick auf Exporte – auf den „zukünftigen Bedarf an IPv6-basierten Diensten, Anwendungen und Geräten“ einstellen, „um so einen drohenden Wettbewerbsnachteil auf dem Weltmarkt abzuwenden“.[50]

I.2.2.2.2 Chancen und Herausforderungen eines Umstiegs auf IPv6

I.2.2.2.2.1 Chancen

IPv6 gilt als Voraussetzung für viele innovative Anwendungen und birgt „ein enormes wirtschaftliches Potenzial“[51]. Durch IPv6 wird eine zunehmende Entwicklung des Internets der Dinge erwartet.[52] Verkehrsmittel, Haushaltsgeräte, Stromzähler, Maschinen usw. werden intelligent und „können über das Internet eigenständig Informationen austauschen, Aktionen auslösen und sich wechselseitig steuern“[53]. So entsteht zum Beispiel das Smart Home – das intelligente vernetzte Heim. Bereits heute bieten Unternehmen kommunikationsfähige Haushaltsgeräte an, die über das hauseigene WLAN oder das Internet bedient werden können. Fragen wie „Sind Fenster und Türen geschlossen? Ist der Herd ausgeschaltet, das Bügeleisen auf Null gestellt? Wie warm ist das Wasser im Wasserspeicher? Welche Leistung bringen die Solarkollektoren aktuell? Wie hoch ist die Raumtemperatur?“[54] können dann auch von unterwegs beantwortet werden. Der vergrößerte Adressraum von IPv6 und die Möglichkeit der direkten Kommunikation sind dafür jedoch unabdingbar.

---

http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Stellungnahme_Kuehn.pdf

[49] Bundesministerium für Wirtschaft und Technologie (Hrsg.): Strategiepapier zur Förderung der Einfühung von IPv6 – AG2 Sonderthemengruppe „Einführung von IPv6“. Nationaler IT-Gipfel München 2011, S. 6. Online abrufbar unter: http://www.it-gipfel.de/IT-Gipfel/Redaktion/PDF/strategiepapier-ag-2,property=pdf,bereich=itgipfel,sprache=de,rwb=true.pdf

[50] Ebd.

[51] Bundesministerium für Wirtschaft und Technologie (Hrsg.): Das Internetprotokoll der Version 6 (IPv6) – Chancen und Herausforderungen für den Wirtschaftsstandort Deutschland – Abschlussbericht. Juni 2012. S. 7. Online abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/bmwi-internetprotokoll-ipv6,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

[52] Vgl. ebd., S.17.

[53] Ebd.

[54] Boeddinghaus, Wilhelm/Meinel, Christoph/Sack, Harald: Einführung von IPv6 in Unternehmensnetzen. Ein Leitfaden. Technische Berichte Nr. 52 des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam. 2011, S. 18. Online abrufbar unter: http://www.hpi.uni-potsdam.de/fileadmin/hpi/source/Technische_Berichte/HPI_52_ipv6_leitfaden.pdf

Alternativtext der Fraktion der SPD sowie der Sachverständigen Alvar Freude und Constanze Kurz

Die Chancen von IPv6 liegen für den Endanwender nicht auf der Hand, ergeben sich aber daraus, dass IPv6 schlicht eine technische Notwendigkeit zur Überwindung des Engpasses bei IPv4-Adressen ist. Mittels IPv6 können aufgrund der hohen Anzahl verfügbarer IP-Adressen alle Geräte eigene öffentliche Adressen erhalten, anstatt wie bisher nur interne. Dadurch ist eine einfachere Kommunikation beliebiger Geräte untereinander denkbar.

Entwickler von Soft- und Hardware profitieren davon, dass der Aufwand für die Implementation von Kommunikation zwischen beliebigen Geräten sinkt. Häufig diskutierte Beispiele wie Heimautomation und Heizungssteuerung sind auch heute möglich, erfordern aber einen etwas höheren Aufwand bei der Implementierung der Kommunikationsprotokolle.

I.2.2.2.2.2 Herausforderungen

Die Einführung von IPv6 kann „als Umbau im Maschinenraum des Internets betrachtet werden“.[55] Als solcher betrifft er zunächst ISP, Anbieter von Hardware, Endgerätehersteller, Anbieter von Betriebssystemen und Anwendungssoftware sowie Dienste- und Inhalteanbieter.[56] Es zeichnen sich aber auch Folgewirkungen jenseits der unmittelbaren Technologieeinführung ab, die die Rechte von Beteiligten, insbesondere der Nutzerinnen und Nutzer, betreffen.

Die Herausforderungen, die sich den unterschiedlichen Akteuren stellen, werden im Folgenden dargestellt.

I.2.2.2.2.2.1 IPv6-fähige Hard- und Software

Bedingt durch die IPv4-Adressknappheit sind die ISP gezwungen, ihre Netze auf IPv6 umzustellen. Für ISP „ist die Migration auf IPv6 komplex und kostspielig“.[57] So sind

---

[55] Protokoll des öffentlichen Expertengesprächs zum Thema „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012, S. 3. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Protokoll.pdf

[56] Vgl. IPv6 German Council: Nationaler IPv6-Aktionsplan für Deutschland. Potsdam, 14. Mai 2009, S. 5. Online abrufbar unter: http://www.ipv6council.de/fileadmin/summit09/Aktionsplan.pdf

[57] Bundesministerium für Wirtschaft und Technologie (Hrsg.): Das Internetprotokoll der Version 6 (IPv6) – Chancen und Herausforderungen für den Wirtschaftsstandort Deutschland – Abschlussbericht. Juni 2012. S. 16. Online abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/bmwi-internetprotokoll-ipv6,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

beispielsweise Netzwerkkomponenten auszutauschen, Software anzupassen und Mitarbeiter zu schulen.[58] Ein früher und schleichender Umstieg kann sich dabei positiv auf die Kosten auswirken. So ist beispielweise bei der Neuanschaffung von Hard- und Software darauf zu achten, dass diese IPv6 unterstützt.[59]

Auch Unternehmen und Privatanwender sind gehalten, bei der Erneuerung ihrer Hardware, zum Beispiel einem Router, darauf zu achten, dass diese IPv6-fähig ist.[60]

Obwohl die Verbreitung von IPv6 immer weiter zunimmt, wird die Migration schätzungsweise noch 10 bis 15 Jahre andauern.[61] Da IPv4 und IPv6 nicht miteinander kompatibel sind, wird es während dieser Zeit zu einem Parallelbetrieb beider Protokolle kommen. Voraussetzung für diesen so genannten Dual-Stack-Modus ist, dass die miteinander kommunizierenden Geräte sowohl IPv4 als auch IPv6 nutzen können. Dazu müssen beide Protokolle auf den Geräten implementiert sein.

Damit das neue Protokoll flächendeckend eingesetzt werden kann, müssen auch die Router bei den Endkunden IPv6 unterstützen. Nur so können die Anwender auch neue Dienste, auf die möglicherweise nur über IPv6 zugegriffen werden kann, nutzen. Dies bedeutet zum einen,

---

[58] Vgl. Protokoll des öffentlichen Expertengesprächs zum Thema „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012, S. 24. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Protokoll.pdf sowie die schriftliche Stellungnahme von Martin Turba im Rahmen des öffentlichen Expertengespräches „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 2. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Stellungnahme_Turba.pdf

[59] Vgl. Protokoll des öffentlichen Expertengesprächs zum Thema „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012, S. 24. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Protokoll.pdf

[60] Im Expertengespräch der Projektgruppe zu „Ipv6 – Sicherheitsapekte“ weißt der Experte Björn A. Zeeb darauf hin, dass Anwender aktuell nicht wissen, „dass sie beim Neukauf eines Routers bereits nach IPv6 schauen müssten“. Protokoll des öffentlichen Expertengesprächs zum Thema „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012, S. 25. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Protokoll.pdf

[61] Vgl. Protokoll des öffentlichen Expertengesprächs zum Thema „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012, S. 7, 32. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Protokoll.pdf

dass die Hersteller von Netzwerkkomponenten[62] in diese IPv6 integrieren müssen, und zum anderen, dass die Router bei den Endkunden entweder ausgetauscht oder mittels Update IPv6-fähig gemacht werden müssen.[63]

I.2.2.2.2.2.2 Neue Angriffsvektoren

Mit der Einführung von IPv6 werden – vor allem in der Übergangsphase – teilweise neue Angriffsvektoren erwartet.[64] Die Angriffsfläche ist allerdings aufgrund der geringen Verbreitung von IPv6 noch gering. Wie Angriffsszenarien genau aussehen werden, kann nicht vorhergesagt werden. Als Ansatzpunkt für künftige Angriffe wird beispielsweise die Möglichkeit der Autokonfiguration gesehen.[65]

Eine wesentliche Auswirkung auf die Sicherheit wird im Wegfall des NAT-Verfahrens[66] gesehen.[67] Mit NAT geht der positive Nebeneffekt einher, dass eine IP-Adresse nicht mehr eindeutig zugeordnet werden kann. Der Rechner hinter dem Router kann nicht ohne Weiteres

---

[62] Siehe hierzu auch Fußnote 47.

[63] Vgl. Schriftliche Stellungnahme von Wolfgang Fritsche im Rahmen des öffentlichen Expertengespräches „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 1. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Stellungnahme_Fritsche.pdf

[64] Vgl. hierzu die unterschiedlichen Aussagen der Anhörpersonen des Expertengespräches „IPv6 – Sicherheitsaspekte“. Protokoll des öffentlichen Expertengesprächs zum Thema „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012, S. 11, 15, 16. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Protokoll.pdf sowie die schriftliche Stellungnahme von Christoph Weber im Rahmen des öffentlichen Expertengespräches „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 4. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Stellungnahme_Weber.pdf
Vgl. auch die Ausführungen des BMWi: Bundesministerium für Wirtschaft und Technologie (Hrsg.): Das Internetprotokoll der Version 6 (IPv6) – Chancen und Herausforderungen für den Wirtschaftsstandort Deutschland – Abschlussbericht. Juni 2012. S. 15. Online abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/bmwi-internetprotokoll-ipv6,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

[65] Vgl. Bundesministerium für Wirtschaft und Technologie (Hrsg.): Das Internetprotokoll der Version 6 (IPv6) – Chancen und Herausforderungen für den Wirtschaftsstandort Deutschland – Abschlussbericht. Juni 2012. S. 15. Online abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/bmwi-internetprotokoll-ipv6,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

[66] Siehe hierzu auch Kapitel I.2.2.2.1.6.

[67] Vgl. Protokoll des öffentlichen Expertengesprächs zum Thema „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012, S. 15. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Protokoll.pdf

identifiziert werden. Da mit IPv6 jedoch ausreichend viele Adressen zur Verfügung stehen, ist die Übersetzung von privaten in eine öffentliche IP-Adresse nicht mehr notwendig. Jedes Gerät kann nun eine eigene IP-Adresse erhalten und dadurch direkt adressiert werden. Für Dienste wie Voice over IP (VoIP) kann dies durchaus sinnvoll sein, birgt jedoch auch ein gewisses Sicherheitsrisiko.

Ergänzungstext der Fraktion der SPD sowie der Sachverständigen Alvar Freude und Constanze Kurz

Ebenso ist es ohne NAT für Server-Betreiber einfacher möglich festzustellen, von wie vielen Endgeräten innerhalb eines Haushalts oder Unternehmens Zugriffe kommen, da ohne NAT alle einzelne IP-Adressen haben. Daher kann es wünschenswert sein, dennoch NAT (NAT66) einzusetzen.

I.2.2.2.2.2.3 Sicherheitsanforderung an Endgeräte

So wurde im Expertengespräch zum Thema „IPv6 – Sicherheitsaspekte“ erklärt, dass es „ohne NAT […] möglich sein [werde], Pakete direkt an Endrechner zu transportieren, sofern keine Filterung durch andere Sicherheitsmechanismen erfolge. Damit steige der Anspruch an die Endanwender bzw. an die Anbieter von Produkten für Endanwender, über eine sichere Basiskonfiguration zu verfügen, die verhindere, dass Pakete aus dem Internet direkt an Endgeräte weitergeleitet werden.“[68] Künftig muss der Schutz verstärkt auf den Endgeräten der Anwender stattfinden. In diesem Zusammenhang wird auch diskutiert, ob Router eine integrierte Firewall beinhalten sollten.[69] Dies ist für stationär verwendete Rechner sicherlich ein relevanter Aspekt, jedoch darf dabei nicht vergessen werden, dass viele Anwender ihre Geräte zunehmend mobil nutzen. Sofern ein Anwender mit seinem Notebook in ein anderes Netz wechselt, muss dieses in der Lage sein, sich selbst zu schützen.[70] Es kann davon ausgegangen werden, dass es den „normalen“ Nutzer überfordert, eine sicherheitstechnische Konfiguration seiner Endgeräte eigenverantwortlich vorzunehmen. Folglich „muss die sichere Konfiguration der normale Betriebszustand sein, auf den sich der Benutzer beim typischen

---

[68] Ebd.

[69] Vgl. ebd., S. 22.

[70] Vgl. Schriftliche Stellungnahme von Christoph Weber im Rahmen des öffentlichen Expertengespräches „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 2. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Stellungnahme_Weber.pdf

Einsatz verlassen kann (security by default).“[71] Gleichwohl muss es dem technisch versierten Anwender möglich sein, diese Einstellungen seinen Bedürfnissen entsprechend zu verändern.

I.2.2.2.2.2.4 Statische und dynamische Adressvergabe

Die Vergabe einer IP-Adresse durch einen ISP kann auf zwei Arten erfolgen: statisch oder dynamisch.

Erfolgt die Zuweisung einer IP-Adresse statisch, so wird diese dauerhaft zugewiesen. Eine statische Vergabe kommt vor allem im Geschäftsbereich zum Einsatz, da zum Beispiel für das Betreiben eines eigenen Webservers eine feste IP-Adresse benötigt wird. Auch innerhalb eines Unternehmensnetzwerks erhalten beispielsweise Drucker eine statische IP. Im Endkundenbereich sind statische Adressen für Dienste wie Voice over IP (VoIP) oder Internet Protocol Television (IPTV) relevant.

Bei einer dynamischen IP-Adressvergabe wird die Adresse nur für einen begrenzten Zeitraum vergeben. Nach einer festgelegten Zeitspanne, zum Beispiel 24 Stunden, erfolgt eine automatische Trennung. Sollte eine weitere Internetnutzung gewünscht sein, erhält der Kunde vom ISP eine neue Adresse zugewiesen. Unter IPv4 ist die dynamische Vergabe von IP-Adressen aufgrund der Adressknappheit notwendig. Da sich mit IPv6 der Adressraum jedoch um ein Vielfaches vergrößert, ist dies nun nicht mehr zwingend.

Unter IPv6 wird dem Endkunden im Regelfall keine komplette IP-Adresse zugewiesen, sondern lediglich der erste Teil, das so genannte Global-Routing-Präfix.[72] Auch hier kann – wie unter IPv4 – entweder eine dynamische oder eine statische Vergabe erfolgen.

Sollte unter IPv6 künftig eine statische Vergabe erfolgen, kann dies aus Datenschutzsicht kritisch gesehen werden. Durch eine statische Zuweisung der IP-Adresse, „stiege das Risiko, dass Diensteanbietern die Person hinter der IP-Adresse bekannt wird. Sie könnte dann bei jedem Besuch einer Webseite wiedererkannt werden, auch wenn sie sich dort nicht namentlich anmeldet. Dies wäre das Ende jedweder Anonymität im Internet – im Ergebnis eine kleine Vorratsdatenspeicherung durch die Hintertür, weil die IP-Adresse dann als

---

[71] Bundesministerium für Wirtschaft und Technologie (Hrsg.): Das Internetprotokoll der Version 6 (IPv6) – Chancen und Herausforderungen für den Wirtschaftsstandort Deutschland – Abschlussbericht. Juni 2012. S. 15. Online abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/bmwi-internetprotokoll-ipv6,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

[72] Siehe zum Aufbau von IPv6-Adressen Kapitel I.2.2.2.1.5.

Bestandsdatum dauerhaft gespeichert würde.“[73] Eine statische Vergabe zöge rechtliche Folgen nach sich, da die IP-Adresse damit zum Bestandsdatum würde.[74]

Ob die Zuweisung der IP-Adresse in Zukunft statisch oder dynamisch erfolgt, ist vom jeweiligen Anwendungsszenario abhängig zu machen.[75] Bei Diensten wie VoIP oder IPTV ist eine statische Vergabe durchaus wünschenswert, da eine mit der dynamischen Zuweisung einhergehende Zwangsunterbrechung zu Problemen führen kann (Unterbrechung eines Telefonats, möglicherweise eines Notrufs; Unterbrechung eines TV-Streams).

Beispiel für eine am Markt mögliche Lösung zur Einführung von IPv6

Auf dem Symposium „Internetprotokoll Version 6 (IPv6) – Wo bleibt der Datenschutz?“ des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 22. November 2011 stellte der Referent ein großen deutsches Telekommunikationsunternehmen das von diesem geplante Vorgehen hinsichtlich der Einführung von IPv6 vor.[76] So sollen die Kunden des Unternehmens aus „einem sehr großen regionalen Pool an IPv6-Präfixen einen eigenen kleinen Pool“ mit „256 individuellen Präfixen“ erhalten.[77] Technisch bedeutet dies, dass dem Anwender kein komplettes 64 Bit Präfix zugewiesen wird, sondern in diesem Fall ein 56 Bit umfassendes Präfix (Global-Routing-Präfix). Die restlichen 8 Bit (Subnet Identifier) stehen dem Nutzer zur Verfügung, um eigene Subnetze zu bilden. Der von dem Telekommunikationsunternehmen ausgelieferte Router soll den Subnet Identifier regelmäßig

---

[73] Schriftliche Stellungnahme von Ulrich Kühn im Rahmen des öffentlichen Expertengespräches „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 3. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Stellungnahme_Kuehn.pdf

[74] Vgl. MMR-Aktuell 2012, 329884 vom 21.03.2012, Ausgabe 6/2012 vom 27. März 2012

[75] Vgl. Schriftliche Stellungnahme von Ulrich Kühn im Rahmen des öffentlichen Expertengespräches „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 3. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Stellungnahme_Kuehn.pdf

[76] Vgl. hierzu die Ausführungen von Jan Lichtenberg, Deutsche Telekom, in: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Schaar, Peter (Hrsg.): Internetprotokoll Version 6 (IPv6) – Wo bleibt der Datenschutz? – Tagungsband, 22. November 2011, Berlin, S. 36. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/TagungsbandSymposiumIPv6.pdf?__blob=publicationFile

[77] Vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Schaar, Peter (Hrsg.): Internetprotokoll Version 6 (IPv6) – Wo bleibt der Datenschutz? – Tagungsband, 22. November 2011, Berlin, S. 36. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/TagungsbandSymposiumIPv6.pdf?__blob=publicationFile

neu erzeugen, das heißt aus dem Pool der 256 Subnetze auswählen.[78] Zusätzlich soll es dem Nutzer durch einen so genannten Privacy Button möglich sein, ein „komplett neues [56 Bit] Präfix zugewiesen [zu] bekommen“.[79] Diese Neuzuweisung kann der Anwender entweder manuell auslösen oder automatisiert, zum Beispiel alle 24 Stunden immer um 1 Uhr nachts, durchführen lassen. Dem Kunden soll damit die Möglichkeit eingeräumt werden, sein gewünschtes Datenschutzniveau selbst festlegen zu können.[80] Von einer vom Provider durchgeführten Zwangstrennung, wie sie bei IPv4 üblich ist, will das Unternehmen Abstand nehmen. Dies liegt zum einen an den zukünftigen All-IP-Anschlüssen unter IPv6[81]: Würde man hier eine Zwangstrennung der Datenleitung vornehmen, würden auch Telefongespräche – schlimmstenfalls ein Notruf – unterbrochen. Zum anderen führe eine Neuzuweisung der IP-Adresse auch zur Unterbrechung von Diensten wie IPTV oder VoIP.[82]

Vor dem Hintergrund, dass die IP-Adresse nicht zwangsweise dynamisch neu zugewiesen wird, sondern den aktiven Eingriff des Nutzers erfordert, kann kritisiert werden, dass der Subnet Identifier mit 8 Bit zu kurz gewählt ist.[83] In diesem Fall stehen nur 256 Möglichkeiten zur Verfügung, mit denen der Global-Routing-Präfix ergänzt werden kann. Bleibt der Global-Routing-Präfix nämlich über einen längeren Zeitraum konstant, so besteht – wie bei einer statischen Adressvergabe – die Möglichkeit die IP einem Anschluss eindeutig zuzuordnen. Wird der Global-Routing-Präfix jedoch regelmäßig neu vergeben, besteht dieses Risiko nicht. Von Seiten des Unternehmens wird eingeräumt, dass es sich bei der geplanten Vorgehensweise um eine zum jetzigen Zeitpunkt realisierbare Lösung handelt, die sich in den nächsten Jahren weiterentwickeln und verändern kann.[84]

---

[78] Vgl. ebd.

[79] Ebd., S. 36f.

[80] Vgl. ebd., S. 37.

[81] All-IP-Anschluss bedeutet, der Kunde erhält nur noch eine Leitung für Telefonie und Datentransfer. Die Telefonie erfolgt über VoIP. Vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Schaar, Peter (Hrsg.): Internetprotokoll Version 6 (IPv6) – Wo bleibt der Datenschutz? – Tagungsband, 22. November 2011, Berlin, S. 33f. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/TagungsbandSymposiumIPv6.pdf?__blob=publicationFile

[82] Vgl. Protokoll des öffentlichen Expertengespräches zum Thema „IPv6 – Sicherheitsaspekte“ der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012, S. 16. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Protokoll.pdf

[83] Vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Schaar, Peter (Hrsg.): Internetprotokoll Version 6 (IPv6) – Wo bleibt der Datenschutz? – Tagungsband, 22. November 2011, Berlin, S. 53f., 61. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/TagungsbandSymposiumIPv6.pdf?__blob=publicationFile

[84] Vgl. ebd., S. 50.

Die 33. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre empfiehlt eine standardmäßig dynamische Präfixvergabe.[85] Dennoch muss dem Endkunden auch die Möglichkeit eingeräumt werden, auf Wunsch eine statische Adresse zu erhalten.

In den vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Peter Schaar, und dem Deutschen IPv6-Rat veröffentlichten Leitlinien „IPv6 und Datenschutz“ heißt es dazu: „Für den Benutzer muss je nach Notwendigkeit die Möglichkeit bestehen, sowohl mit statisch vergebenen IPv6 Adressen, d.h. dauerhaft identifizierbar, Transaktionen im Internet durchzuführen, als auch (teil-)anonymisiert und damit nicht (einfach) zurückverfolgbar, z.B. vermittels von dynamisch vergebenen Anteilen im IPv6 Adresspräfix oder vermittels dynamischer neu vergebener Präfixe auf Kundenwunsch z.B. per Knopfdruck, sein. Die jeweilige Entscheidung darüber soll/muss beim Benutzer liegen.“[86]

I.2.2.2.2.5 Privacy Extensions

Ein weiterer aus Datenschutzsicht zu betrachtender Aspekt geht mit der Generierung des Interface Identifier einher. Dieser dritte Teil einer IPv6-Adresse dient der eindeutigen Identifizierung eines Endgeräts innerhalb eines Netzwerks. Die Bildung des Interface Identifier kann entweder auf Basis der weltweit einmaligen MAC-Adresse des Endgerätes[87] oder auf Basis regelmäßig neu erzeugter Zufallszahlen mittels Privacy Extensions erfolgen.[88]

„Die ‚Privacy Extension‘ verhindern wirksam eine eindeutige Identifikation eines bestimmten Endgerätes anhand seiner IPv6-Adresse.“[89] Bei deaktivierten Privacy Extensions ist jedoch durch Mobile IPv6[90] ein Tracking des Nutzers über Netzwerkgrenzen hinweg möglich. Tracking kann jedoch auch über den Einsatz so genannter Cookies erfolgen. Durch die

---

[85] Vgl. 33. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre: Entschließung – Die Verwendung eindeutiger Kennungen bei der Nutzung von Internet Protokoll Version 6 (IPv6), 1. November 2011, S. 2. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/IntDSK/2011InternetIPv6.pdf?__blob=publicationFile

[86] IPv6 German Council: Leitlinien IPv6 und Datenschutz. 16. März 2012. Online abrufbar unter: http://www.ipv6council.de/documents/leitlinien_ipv6_und_datenschutz.html

[87] Siehe Fußnote 29.

[88] Siehe Fußnote 30.

[89] Schriftliche Stellungnahme von Gert Döring im Rahmen des öffentlichen Expertengespräches zum Thema „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 1. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Stellungnahme_Doering.pdf

[90] Siehe Kapitel I.2.2.2.1.6.

europäische Richtlinie (2009/136/EG)[91], so genannte Cookie-Richtlinie[92], könnte das Cookie-Tracking jedoch unwichtiger werden, wodurch das Interesse an IPv6-Tracking steigen könnte.[93]

Um die Privatsphäre des Nutzers zu schützen, wird daher im Sinn des Privacy by Design eine Implementierung der Privacy Extensions in Betriebssystemen und auf mobilen Endgeräten gefordert.[94] Zudem sollten diese standardmäßig aktiviert werden (Privacy by Default).[95] Es sind bereits Betriebssysteme sowie Mobilgeräte verfügbar, auf denen die Privacy Extensions genutzt werden können.

In dem von der Projektgruppe durchgeführen Expertengespräch „IPv6 – Sicherheitsaspekte“ haben sich mehrere Anhörpersonen dafür ausgesprochen, dass für den Endanwender eine einfache Möglichkeit, beispielsweise ein leicht zugänglicher und intuitiv bedienbarer Button, vorhanden sein sollte, um zwischen ein- und ausgeschalteten Privacy Extensions wechseln zu können.[96]

---

[91] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elekotronischen Kommunikationsnetzen und –diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz. Online abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:De:PDF

[92] Die Cookie-Richtlinie besagt, dass Cookies nur noch mit ausdrücklicher Genehmigung des Nutzers (Opt-In-Verfahren) zum Einsatz kommen dürfen.

[93] Vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Schaar, Peter (Hrsg.): Internetprotokoll Version 6 (IPv6) – Wo bleibt der Datenschutz? – Tagungsband, 22. November 2011, Berlin, S. 33. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/TagungsbandSymposiumIPv6.pdf?__blob=publicationFile

[94] Vgl. beispielsweise die schriftliche Stellungnahme von Ulrich Kühn im Rahmen des öffentlichen Expertengespräches „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 4. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Stellungnahme_Kuehn.pdf

[95] Vgl. 33. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre: Entschließung – Die Verwendung eindeutiger Kennungen bei der Nutzung von Internet Protokoll Version 6 (IPv6), 1. November 2011, S. 2. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/IntDSK/2011InternetIPv6.pdf?__blob=publicationFile

[96] Vgl. Protokoll des öffentlichen Expertengesprächs zum Thema „IPv6 – Sicherheitsaspekte“ der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 12, 16. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Protokoll.pdf

I.2.2.2.2.6 Sensibilisierung der Nutzerinnen und Nutzer

Mit der Einführung von IPv6 ergeben sich technische Neuerungen. Diese bieten Vorteile, bringen aber – wie dargestellt – auch einige sicherheits- und datenschutzrelevante Herausforderungen mit sich.

Vor diesem Hintergrund wird der Sensibilisierung und Aufklärung der Nutzerinnen und Nutzer eine besondere Rolle zuteil.[97]

Der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Peter Schaar, spricht sich dafür aus, dass zunächst der Selbstregulierung vor einer zu frühzeitigen Reglementierung der Vorzug zu geben ist. Für ihn stehen datenschutzfreundliche Grundeinstellung sowie die Aufklärung der Nutzerinnen und Nutzer im Mittelpunkt. So erklärt er: „Lassen Sie mich noch einen Schlenker machen zum Thema „rechtlicher Rahmen". Wir als Datenschützer sind ja bekannt dafür, dass wir immer wieder nach neuen Gesetzen rufen. Hier würde ich mal sagen, tun wir das so nicht. Wir setzen darauf, dass wir über entsprechende Mechanismen, vielleicht auch die Selbstregulierung, datenschutzfreundliche Standards umsetzen werden. Wenn das nicht klappt, dann muss man natürlich überlegen, auch im Einzelfall, ob es ausreichend ist, auf Selbstregulierungsmechanismen zu setzen. Entscheidend ist für mich, dass für den Betroffenen, der als Nutzer, als Kunde Internetdienste in Anspruch nimmt, zunächst einmal eine datenschutzfreundliche Einstellung präsentiert wird, die ein Tracking und Tracing eben nicht standardmäßig ermöglicht und zweitens, dass das ganze System für ihn transparent ist. D.h., wenn er sich für ein bestimmtes Modell entscheidet, dass er auch weiß, welche Konsequenzen das hat. Wenn er im vollen Bewusstsein, dass es da vielleicht auch Datenschutzrisiken gibt, sich entscheidet, diese Risiken in Kauf zu nehmen, weil es Vorteile gibt, auf die er nicht verzichten möchte, dann

---

[97] Vgl. Schriftliche Stellungnahme von Björn A. Zeeb im Rahmen des öffentlichen Expertengespräches „IPv6 – Sicherheitsaspekte" der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 2. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Stellungnahme_Zeeb.pdf sowie Protokoll des öffentlichen Expertengesprächs zum Thema „IPv6 – Sicherheitsaspekte" der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages vom 21. Mai 2012. S. 12, 26. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/PGZuStrSi_2012-05-21_Protokoll.pdf

denke ich, werden wir ihn nicht bevormunden wollen. Aber Transparenz und Privacy by Design / Default, das ist, glaube ich der Schlachtruf dieser Revolution.“[98]

I.3. Zugang zum Internet: Wettbewerb und Breitbandverfügbarkeit

Ein leistungsfähiger Zugang zum Internet ist heute in vielen Lebensbereichen eine wesentliche Voraussetzung für eine gleichberechtigte Teilhabe an den gesellschaftlichen und wirtschaftlichen Möglichkeiten, die das Internet schafft. Dies gilt gleichermaßen für den privaten Bereich und die Rolle als Verbraucher als auch für jedwede Form gewerblicher Tätigkeit – ob nun als Großunternehmen, kleines oder mittelständisches Unternehmen oder Freiberufler. Die flächendeckende Verfügbarkeit einer Breitbandgrundversorgung hat deshalb auch zu Recht hohe politische Priorität, um gleichwertige Lebensverhältnisse zu sichern und eine digitale Spaltung der Gesellschaft zu verhindern.

Neben der Verfügbarkeit eines Breitbandanschlusses spielen für den Kunden aber auch der Preis und eine einfache Handhabung eine wichtige Rolle. Zudem ist der Nutzen eines Internetzugangs ohne interessante und vielfältige Dienste gering. Die Schaffung von vielfältigen und nachfrageorientierten Angeboten kann am besten durch einen funktionierenden Wettbewerb in den Märkten für diese Dienste gewährleistet werden. Die Frage der Verfügbarkeit ist daher untrennbar mit der Frage nach einem funktionsfähigen Wettbewerb im Telekommunikationsmarkt verbunden.

Um Deutschland als Dienstleistungsgesellschaft infrastrukturell fit zu machen, braucht es schnelles Handeln. Für die wirtschaftliche Entwicklung ist der Breitbandausbau elementar, denn die Breitbandkommunikation trägt in hochentwickelten Ländern bis zu einem Drittel des Produktivitätswachstums bei.[99] Schnelles Breitband flächendeckend könnte allein durch den Ausbau der Netzwerkinfrastruktur im Zehnjahreszeitraum 2010 bis 2020 zu einem direkten Anstieg des Bruttoinlandsprodukts (BIP) von 33,4 Milliarden Euro führen. Durch die mit dem Netzwerkausbau verbundenen Effekte auf die deutsche Wirtschaft wird zudem von einem

---

[98] Vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Schaar, Peter (Hrsg.): Internetprotokoll Version 6 (IPv6) – Wo bleibt der Datenschutz? – Tagungsband, 22. November 2011, Berlin, S. 12. Online abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/TagungsbandSymposiumIPv6.pdf?__blob=publicationFile

[99] Vgl. Heng, Stefan: Breitbandinfrastruktur. Auf ordnungspolitischen Rahmen, Markttransparenz und Risikopartnerschaften kommt es an. Deutsche Bank Research. 7. April 2010, S. Online abrufbar unter: http://www.dbresearch.de/PROD/DBR_INTERNET_DE-PROD/PROD0000000000255855.pdf . Zu den Details der ökonomischen Auswirkungen des Breitbandausbaus vgl. OECD Ministerial Background Report “Broadband and the Economy”, DSTI/ICCP/IE(2007)3/FINAL, online abrufbar unter http://www.oecd.org/sti/40781696.pdf

mittelbaren Anstieg des BIP von weiteren 137,5 Milliarden Euro ausgegangen. Insgesamt wird die Auswirkung auf das BIP auf 170,9 Milliarden Euro geschätzt. Auch auf die Beschäftitung wirkt sich der Breitbandausbau positiv aus. Es wird prognostiziert, dass nur durch den Ausbau des Netzes im Zehnjahreszeitraum 2010 bis 2020 bis zu 541 000 neue Arbeitsplätze in Deutschland entstehen werden; mittelbar wird von weiteren 427 000 Arbeitplätzen ausgegangen. Insgesamt sollen durch den Breitbandausbau 968 000 neue Arbeitplätze geschaffen werden.[100] Beim Breitbandausbau ist zu beachten, dass in Deutschland ein historisch gewachsenes Telefon- und Kabelnetz auf Kupferbasis existiert. Durch technische Innovationen (DSL, VDSL, EuroDOCSIS 3.0) können unter Nutzung und Ergänzung der bestehenden Infrastruktur höhere Übertragungsraten erreicht werden. Nach Angaben der Bundesregierung standen bereits im Jahr 2011 für 40 Prozent der deutschen Haushalte Hochgeschwindigkeitsanschlüsse von 50 Mbit/s oder höher zur Verfügung.[101] Damit unterscheidet sich die Ausgangssituation in Deutschland grundlegend von der anderer Staaten und insbesondere von solchen Ländern, die erstmals moderne Telekommunikationsinfrastrukturen (TK-Infrastrukturen) ausbauen oder dies kürzlich getan haben und für den flächdeckenden Anschluss der Haushalte mit TK-Infrastrukturen auf Glasfaser setzen.

In Deutschland können über eine – zumindest partielle – Weiterverwendung von Kupferleitungen auf der letzten Meile hohe Übertragungsraten erreicht werden. Beim so genannten FTTC(Fiber-to-the-Curb)-Ausbau etwa werden Glasfaserkabel bis zu den Kabelverzweigern verlegt. Für die letzte Meile wird die vorhandene Kupferkabelinfrastruktur genutzt. Der Vorteil dieser Ausbauvariante eines Next-Generation-Access(NGA)-Netzes ist, dass die Kosten, im Vergleich zum Verlegen von Glasfaserkabeln bis zum Gebäude des Teilnehmers (Fiber-to-the-Building, FTTB), vergleichsweise niedrig ausfallen und schneller realisiert werden können. Es erfolgt dennoch ein Glasfaserausbau bis zum Kabelverzweiger und damit sehr nahe an den Endkunden. Daneben stellt LTE einen wichtigen Baustein für die Breitbandgrundversorgung – insbesondere in entlegenen und dünnbesiedelten Regionen – dar.

---

[100] Vgl. Katz, Raul et al.: Die Wirkung des Breitbandausbaus auf Arbeitsplätze und die deutsche Volkswirtschaft. 2009. S. 1ff; 8. Online abrufbar unter: http://www.polynomics.ch/dokumente/Polynomics_Breitbandausbau_Broschuere_D.pdf. Die gesamte Studie steht in Englisch online zur Verfügung unter: http://www.polynomics.ch/dokumente/Polynomics_Broadband_Study_E.pdf

[101] Vgl. Bundesministerium für Wirtschaft und Technologie: Zweiter Monitoringbericht zur Breitbandstrategie des Bundes. November 2011, S. 7. Online abrufbar unter: http://www.bmwi.de/Dateien/BMWi/PDF/zweiter-monitoringbericht-zur-breitbandstrategie-des-bundes,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf

Nach Angaben der Bundesregierung[102] betrug die Breitbandverfügbarkeit bezogen auf alle Haushalte in Deutschland Mitte 2011:

- für eine Geschwindigkeit von ≥ 1 Mbit/s 98,7 Prozent;
- für eine Geschwindigkeit von ≥ 2 Mbit/s 94,2 Prozent;
- für eine Geschwindigkeit von ≥ 6 Mbit/s 84,4 Prozent.

Seitdem hat jedoch der LTE-Ausbau große Fortschritte gemacht. Nach einer Erhebung des Branchenverbandes BITKOM konnten im April 2012 bereits über 13 Millionen Haushalte[103], insbesondere in ländlichen Regionen, mit Breitbandinternet versorgt werden. Der Breitbandausbau in Deutschland ist gerade ein Beispiel dafür, wie durch entsprechende regulatorische Rahmenbedingungen privatwirtschaftliche Investitionen ausgelöst werden. In anderen Staaten ist ein flächendeckender Glasfaserausbau dagegen in der Regel das Ergebnis einer entsprechenden Industriepolitik samt eines umfassenden Einsatzes von Steuermitteln.

I.3.1 Breitbandzugangstechnologien – Arten, Leistungsfähigkeit und Verbreitung

Der Wettbewerb im Telekommunikationsmarkt hat zur Entstehung einer breiten Palette alternativer Zugangstechnologien geführt, die in ihrer Leistungsfähigkeit einer dynamischen technischen Weiterentwicklung unterliegen.

I.3.1.1 Zugangstechnologien im Festnetz

Heute und auch in Zukunft kommt dem kabelgebundenen Zugang zum Internet eine hohe Bedeutung zu. In der Regel bietet dieser gegenüber dem kabellosen Zugang noch höhere Übertragungsraten, wenngleich alle Technologien von einer stetigen Steigerung der Übertragungsraten infolge der technischen Fortentwicklung geprägt sind.

I.3.1.1.1 DSL

Geradezu beispielhaft für die Erschließung neuer Bandbreitenkapazitäten ist die mit etwa 23 Millionen Anschlüssen heute am weitesten verbreitete Internetzugangstechnologie DSL

---

[102] Vgl. Bundesministerium für Wirtschaft und Technologie: Zweiter Monitoringbericht zur Breitbandstrategie des Bundes. November 2011, S. 43. Online abrufbar unter:: http://www.bmwi.de/Dateien/BMWi/PDF/zweiter-monitoringbericht-zur-breitbandstrategie-des-bundes,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf

[103] Vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM): Mobiles Breitband bereits für 13 Millionen Haushalte. Pressemitteilung. 2. April 2011. Online abrufbar unter: http://www.bitkom.org/de/presse/8477_71710.aspx

(Digital Subscriber Line).[104] Sie beruht auf traditionellen Kupferleitungen, die als Basis des größtenteils noch von der Deutschen Bundespost errichteten Telefonnetzes in Westdeutschland nahezu flächendeckend und in Ostdeutschland inzwischen weitgehend verlegt sind. Die Technologie beruht auf einer Aufsplittung des auf der Kupferdoppelader transportierbaren Frequenzbereichs. Dieser teilt sich auf in den für die Sprachübertragung benötigten Frequenzbereich und in einen hochfrequenten Übertragungsbereich, der für die Datenübertragung verwandt werden kann.

Die Aufsplittung erfolgt zwischen den in den Haushalten eingesetzten DSL-Splittern und den zunächst meist in den Hauptverteilern aufgestellten DSLAMs (Digital Subscriber Line Access Multiplexer), von wo aus der Datenverkehr in das Aggregationsnetz des Netzbetreibers übergeben wird. Je länger jedoch die Strecke zwischen Endkundenanschluss und DSLAM ist, desto geringer ist die über DSL technisch realisierbare Bandbreite. Daneben haben auch die Qualität der genutzten Endleitung sowie andere potenzielle Störfaktoren Einfluss auf die tatsächlich erreichbare Bandbreite.

Bei dem am weitesten verbreiteten asynchronen DSL (ADSL – Assymmetric Digital Subscriber Line) stehen unterschiedliche Bandbreiten für den Down- und den Upload zur Verfügung. Hiermit können Download-Bandbreiten von bis zu 16 Mbit/s realisiert werden; im Upload in der Regel bis zu 1 Mbit/s. Alternativ steht auch die SDSL-Technologie (Symmetric Digital Subscriber Line) für eine synchrone Anbindung gleicher Up- und Download-Bandbreite zur Verfügung, die in erster Linie im Geschäftskundenbereich Verwendung findet.

Neuere Technologien wie VDSL (Very High Speed Digital Subscriber Line) erlauben inzwischen auch die Realisierung deutlich höherer Bandbreiten. Auf dem Markt sind bereits Angebote mit bis zu 50 Mbit/s verfügbar; technologisch können inzwischen über DSL-Technik aber schon mehr als 100 Mbit/s auf einer einfachen Kupferdoppelader, bei Bündelung mehrerer Fasern sogar noch deutlich höhere Werte, realisiert werden. Derzeit steht diese DSL-basierte Technologie für etwa 30 Prozent der Haushalte in Deutschland zur Verfügung[105] und ermöglicht damit auch bandbreitenintensive Anwendungen wie hochqualitatives HD- und 3D-TV via Internet.

---

[104] Vgl. Bundesnetzagentur: Tätigkeitsbericht Telekommunikation 2010/2011. 2011. S. 36. Online abrufbar unter: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/TaetigkeitsberichtTK20102011pdf.pdf?__blob=publicationFile

[105] Vgl. ITU-News: Germany's Broadband Strategy. Juni 2011. Online abrufbar unter http://www.itu.int/net/itunews/issues/2011/05/19.aspx

Durch einen kontinuierlichen, zunehmend auch außerhalb der Hauptverteiler und damit näher am Endkunden (zum Beispiel in den Kabelverzweigern, so genannten Outdoor DSLAMs) stattfindenden Ausbau der DSLAMs, der zuletzt auf der Basis von Maßnahmen aus dem Konjunkturpaket II erfolgte, können immer mehr Kunden auch mit hochbitratigen Angeboten über DSL versorgt werden.

I.3.1.1.2 TV-Kabel (Koaxialkabel)

Eine alternative leitungsgebundene Internetzugangsinfrastruktur besteht für viele Haushalte mit dem digital aufgerüsteten TV-Kabel. Die notwendige Aufrüstung ist mittlerweile weit fortgeschritten.[106] Bereits heute sind entsprechende Anschlüsse für über 24 Millionen Haushalte in Deutschland verfügbar[107] – darunter auch mehr als zwei Millionen bislang unterversorgte Haushalte im ländlichen Raum.[108]

Durch Aufrüstung der Netze auf den Datenübertragungsstandard EuroDOCSIS[109] 3.0 sind Anschlussbandbreiten von über 100 Mbit/s realisierbar.[110] Nach Angaben der Kabelnetzbetreiber wird bis Ende 2012 eine Verfügbarkeit dieser Hochgeschwindigkeitsangebote für zwei Drittel aller Haushalte in Deutschland angestrebt.[111]

Die Kabelnetze liefern damit einen wichtigen Beitrag für den notwendigen Wettbewerb der Infrastrukturen, wobei die Wettbewerbssituation innerhalb dieser Technologie von wenigen großen Unternehmen und einer regionalen Marktaufteilung geprägt ist.

Dabei ist zu beachten, dass wesentliche Anteile der Bandbreite beim Fernsehkabel für den Transport der TV-Programme belegt sind und das Koaxialkabel technologisch eine geteilte Ressource ist, bei der eine Rivalität der verschiedenen in einem Bereich angeschlossenen

---

[106] Bei Kabel BW sind bereits 100 Prozent der Kabelkunden auch mit Telekommunikationsdiensten versorgbar; Kabel Deutschland plant zeitnah zumindest 90 Prozent (Stand: Januar 2012).

[107] Vgl. Verband Deutscher Kabelnetzbetreiber e.V. (ANGA): Das deutsche Breitbandkabel. 2011, S. 6. Online abrufbar unter: http://www.anga.de/media/file/4.ANGA_Das_deutsche_Breitbandkabel_2011_01.pdf

[108] Vgl. Verband Deutscher Kabelnetzbetreiber e.V. (ANGA): Positionspapier zur „Breitbandpolitik und Breitbandförderung“. 2009, S. 4. Online abrufbar unter: http://anga.de/media/file/6.ANGA_Positionspapier_zu_Breitbandpolitik_und_Breitbandfoerderung_Dezember_2009.pdf

[109] DOCSIS steht für Data Over Cable Service Interface Specification. Der Datenübertragungsstandard EuroDOCSIS wurde, basierend auf dem US-amerikanischen DOCSIS, für den europäischen Raum angepasst.

[110] Aktuell bietet Kabel Deutschland Anschlüsse mit bis zu 100 Mbit/s im Download sowie bis zu 4 Mbit/s im Upload an. Kabel BW stellt Anschlüsse mit bis zu 100 Mbit/s im Download und bis zu 2,5 Mbit/s im Upload zur Verfügung. Unitymedia und Tele Columbus realisieren sogar Anschlüsse mit bis zu 128 Mbit/s im Download und bis zu 5 beziehungsweise 4 Mbit/s im Upload. (Stand: Januar 2012)

[111] Vgl. Verband Deutscher Kabelnetzbetreiber e.V. (ANGA): Das deutsche Breitbandkabel. 2011, S. 7. Online abrufbar unter http://anga.de/media/file/4.ANGA_Das_deutsche_Breitbandkabel_2011_01.pdf

Nutzer bei der Nutzung der Bandbreite besteht. Dies führt – im Gegensatz zur DSL- oder Glasfaser-Technologie mit dedizierten Anschlusssegmenten, allerdings vergleichbar mit mobilen Zugangstechnologien – dazu, dass sich die tatsächlich für den einzelnen Nutzer zur Verfügung stehende Bandbreite im Falle starker Nutzung durch konkurrierende Nachfrage reduzieren kann.

Nach Angaben der Kabelnetzbetreiber werden die Netze derzeit so ausgebaut, dass die bisher eingesetzten Koaxialkabel schrittweise und nachfragegetrieben durch Glasfaserkabel ersetzt und an Gebäude herangeführt werden. Aus der Verbindung der Zugangstechnologien entstehen hybride Netze aus Koaxialkabel und Glasfaser – Hybrid Fiber Coax (HFC)-Netzwerke, die einen schnelleren Transport großer Datenmengen gewährleisten sollen.[112]

I.3.1.1.3 Glasfaser (FTTx)

Die Zukunftstechnologie im Bereich der kabelgebundenen Telekommunikationszugänge wird auf lange Sicht die Glasfaser sein: Ihr entscheidender Vorteil ist, dass hier ein quasi verlustfreier Datentransport auch über weite Strecken möglich ist.

Der Wechsel von der bisherigen Kupfernetzarchitektur auf Glasfaser bringt allerdings einen hohen Investitionsbedarf mit sich. Eine Studie des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste (WIK) für das NGA-Forum der Bundesnetzagentur geht von einem Investitionsbedarf von über 70 Milliarden Euro für einen flächendeckenden Glasfaserausbau aus.[113] In dieser Dimension werden ein kurzfristiger Ausbau und ein schneller, vollständiger Umstieg von Kupfer- auf Glasfaserleitungen nicht erreichbar sein. Vielmehr ist eine graduelle Aufrüstung zu erwarten, sodass der Ausbau mit Glasfaser vielmehr sukzessiv zum Endkunden vorangetrieben wird (zunächst zum Kabelverzweiger als Basis für leistungsfähigere VDSL-Anbindungen (Fiber-to-the-Curb, FTTC) und gegebenenfalls erst später die vollständige Erschließung bis zum Gebäude beziehungsweise zur Wohnung (Fiber-to-the-Building/to-the-Home, FTTB / FTTH)). Vor diesem Hintergrund werden die herkömmlichen Zugangstechnologien, insbesondere das bestehende Kupfernetz, auf absehbare Zeit ihre Bedeutung beibehalten.

---

[112] Vgl. ebd., S. 9.

[113] Vgl. Präsentation des WIK: Implikationen eines flächendeckenden Glasfaserausbaus und sein Subventionsbedarf – Zusammenfassung der Ergebnisse eines Forschungsprojektes. 2011, S. 37. Online abrufbar unter: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/NGAForum/15teSitzung/NGAForum201109_WIKStudieFolien.pdf?__blob=publicationFile

Dies ist auch deshalb zu erwarten, da heutzutage eine Nachfrage nach ultrabreitbandigen Internetanschlüssen auf Basis eines vollständigen Glasfaserausbaus bei den meisten Endkunden noch nicht gegeben und auch die Zahlungsbereitschaft entsprechend schwach ausgeprägt ist.[114] Zurzeit fehlt es noch an massenwirksamen Anwendungen, die tatsächlich einen praktischen Nutzen von entsprechend leistungsfähigen Internetzugängen für die Mehrzahl der Nutzer nachvollziehbar macht. Erst die Entwicklung innovativer Dienste, etwa Video-Anwendungen auf HD- oder 3D-Basis werden hier einen wesentlichen Impuls für eine entsprechende Nachfrage setzen.

Eine Folge dieser aktuellen Marktlage ist die zurzeit noch relativ gering erscheinende Versorgung mit Glasfaseranschlüssen in Deutschland (circa 2,5 Prozent[115]), die insbesondere in der fortgeschrittenen technologischen Erschließung auf Basis alternativer Technologien (Kupfer- und Koaxialkabel) begründet liegt. Im Laufe der nächsten Jahre ist hier allerdings mit einem stetigen und auch in der Geschwindigkeit zunehmenden Wachstum zu rechnen.

I.3.1.2 Kabellose Zugangstechnologien

Eine immer größere Rolle übernehmen kabellose Zugangstechnologien. Dies gilt zum einen für die zunehmende Nutzung des Internets über mobile Endgeräte. Zum anderen können kabellose Zugangstechnologien durch die enorm gestiegene Leistungsfähigkeit der hierüber möglichen Datenübertragung zunehmend zu einer validen Alternative zu kabelgebundenen Internetzugängen auch bei stationärer Nutzung werden. Dies gilt vor allem für stark mobile Bevölkerungsgruppen wie Studierende oder auch alleinstehende Personen, die immer häufiger komplett auf einen kabelgebundenen Internetanschluss verzichten. Daneben bekommen kabellose Zugangstechnologien eine besondere Bedeutung für Gebiete, in denen kabelgebundene Breitbandanschlüsse aufgrund der hohen Investitionskosten noch nicht verfügbar sind. Damit leisten kabellose Zugangstechnologien auch einen wesentlichen Beitrag zur Erreichung der Zielsetzung einer flächendeckenden Breitbandversorgung.

---

[114] Vgl. Marktstudie der United Internet Media für das NGA-Forum der Bundesnetzagentur: Marktforschung zu Kundenerwartungen an Breitband der Zukunft. 3. November 2011. Online abrufbar unter: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/NGAForum/7teSitzung/Hoffmann_NGAForum_20101103.pdf?__blob=publicationFile

[115] Vgl. Bundesnetzagentur: Tätigkeitsbericht Telekommunikation 2010 und 2011. 2011, S.75. Online Abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/TaetigkeitsberichtTK20102011pdf.pdf?__blob=publicationFile

I.3.1.2.1 Mobilfunklösungen

Schon UMTS (Universial Mobile Telecommunications System), der Mobilfunkstandard der dritten Generation, hat die Basis für weitreichende mobile Internetnutzung gelegt. Bandbreiten von bis zu 14 Mbit/s sind heute ein gängiges Angebot; höhere Bandbreiten sind technisch inzwischen möglich.

Mit LTE (Long Term Evolution), dem Mobilfunkstandard der vierten Generation, sind endgültig auch hochbreitbandige Anbindungen möglich. Bandbreiten von bis zu 150 Mbit/s pro Funkzelle sind hier bereits Realität; weit mehr wird mit dem bereits in der Entwicklung befindlichen Nachfolgestandard LTE-Advanced technisch möglich sein: Verbesserte Möglichkeiten der Integration kleiner Zellen in heterogenen Netzen mit intelligentem Interferenzmanagement und unter Ausnutzung auch hoher Trägerfrequenzen wie zum Beispiel bei 3.5 GHz erlauben gesicherte Datenraten von 50 Mbit/s pro Nutzer auch für solche Teilnehmer in Randgebieten einer Zelle ohne Einsatz spezieller Antennenlösungen. Dedizierte Antennenlösungen wie Außen- und Dachantennen mit Richtgewinn können zur weiteren Verbesserung dort eingesetzt werden, wo widrige Empfangsbedingungen vorliegen.

Neben den Übertragungsraten sind bei der Nutzung auch die Latenzzeiten von Bedeutung, die für die Nutzerinnen und Nutzer zum Beispiel beim Aufbau von Internetseiten ein Gradmesser für die Geschwindigkeit ihres Anschlusses sind. Die Latenzzeit stellt gemeinhin die Zeit zwischen dem Absenden eines Datenpakets und der Antwort des angesprochenen Servers dar. Lange waren in diesem Punkt leitungsgebundene Zugangstechnologien den drahtlosen Zugangstechnologien mit einer geringen Latenzzeit deutlich überlegen, was sich mit der Entwicklung des LTE-Standards geändert hat. Dieser weist mit 10 bis 50ms eine Latenzzeit auf dem Niveau eines leitungsgebundenen DSL-Anschlusses auf.

Der Internetzugang über Mobilfunk ist – wie auch das Fernsehkabel ein so genanntes Shared Medium, dass heißt eine geteilte Ressource. Die rivalisierende Nutzung kann zu einer Minderung der für den Einzelnen verfügbaren Bandbreite führen. Infolgedessen werden die in der Praxis technisch möglichen Bandbreiten nicht immer erreicht. Dennoch sind heute in LTE-Ausbaugebieten sichere Mindestbandbreiten auf DSL-Niveau Standard.

Auch deswegen ist es sinnvoll gewesen, dass die Vergabe der Frequenzen für die vierte Mobilfunkgenerationen mit Auflagen zu einer vorrangigen Versorgung „weißer Flecken“ verbunden wurde, um auf diese Weise die flächendeckende Breitbandversorgung voranzutreiben. Im August 2012 hat die Bundesnetzagentur festgestellt, dass die

Versorgungsauflagen zu diesem Zeitpunkt bereits für zwölf der dreizehn Flächenländer erfüllt war.[116]

In den kommenden Jahren werden die einzelnen Mobilfunkstationen zudem mit Glasfaser angebunden werden, um das zu erwartende stetig steigende Datenaufkommen von den Stationen in das ohnehin glasfaserbasierte Backbone-Netz abführen zu können. Schließlich ist für die bereits in der Entwicklung befindliche LTE-Nachfolgegeneration, LTE-Advanced, eine solche Glasfaseranbindung zwingend notwendig. Somit tragen auch die aktuellen und künftigen Mobilfunklösungen dazu bei, Glasfaser in die Fläche und damit näher an die Endkunden zu bringen.

Alternativtext der Fraktion der SPD

UMTS (Universal Mobile Telecommunications System), der Mobilfunkstandard der dritten Generation, hat die Basis für weitreichende mobile Internetnutzung gelegt. Bandbreiten von bis zu 7,2 oder 14 Mbit/s sind heute ein gängiges Angebot; Bandbreiten bis 21 MBit sind mit der UMTS-Erweiterung HSPA+ möglich. In der Praxis werden, vor allem im mobilen Betrieb, weitaus geringere Bandbreiten erreicht.

Mit LTE (Long Term Evolution), dem Mobilfunkstandard der vierten Generation, sind auch Anbindungen mit höheren Bandbreiten möglich. Bandbreiten von bis zu 100 Mbit/s pro Funkzelle werden vereinzelt angeboten. Der LTE-Standard sieht bis zu 300 MBit vor, LTE-Advanced bis zu 1000 MBit. Die Provider versprechen gesicherte Datenraten von 50 Mbit/s pro Nutzer auch für solche Teilnehmer in Randgebieten einer Zelle ohne Einsatz spezieller Antennenlösungen. Dezidierte Antennenlösungen wie Außen- und Dachantennen mit Richtgewinn können zur Verbesserung dort eingesetzt werden, wo widrige Empfangsbedingungen vorliegen. In der Praxis werden nach einer Analyse vom August 2012 im Mittel Datenraten von 1,3 bis 8 MBit bzw. 2,6 bis 8,9 MBit erreicht.[117] Eine Untersuchung der Fachzeitschrift c't ergab kurzzeitige Spitzenwerte von 70 MBit im Telekom-Netz und 50

[116] Vgl. Bundesnetzagentur: Pressemitteilung – Versorgungsauflage im 800-MHz-Bereich nunmehr auch in Mecklenburg-Vorpommern erfüllt. 8. Okotber 2012. Online abrufbar unter: : http://www.bundesnetzagentur.de/cln_1911/SharedDocs/Pressemitteilungen/DE/2012/121008_BreitbandausbauMeckVPom.html?nn=65116

[117] „Analyse: So schnell ist LTE in der Praxis“ http://www.lte-anbieter.info/presse/12/studie-lte-speed.pdf

MBit im Vodafone-Netz, die allerdings nicht dauerhaft und nur in der Nähe der Funkmasten zu erreichen waren.[118]

Neben den Übertragungsraten sind bei der Nutzung auch die Latenzzeiten von Bedeutung, die für die Nutzer zum Beispiel beim Aufbau von Internetseiten ein Gradmesser für die Geschwindigkeit ihres Anschlusses und für die Nutzung von vielen Online-Spielen unabdingbar sind. Die Latenz- oder Pingzeit stellt gemeinhin die Zeit zwischen dem Absenden eines Datenpakets und der Antwort des angesprochenen Servers dar. Lange waren in diesem Punkt leitungsgebundene Zugangstechnologien den drahtlosen Zugangstechnologien mit einer geringen Latenzzeit deutlich überlegen, mit dem LTE-Standard sind aber vergleichsweise geringe Latenzen möglich. Provider versprechen mit 10 – 50ms eine Latenzzeit auf ähnlichem Niveau leitungsgebundener DSL-Anschlüsse, die in der Praxis üblicherweise Ping-Zeiten von 20 ms erreichen, teilweise bis hin zu 10ms. In der Praxis erreicht LTE aber je nach Provider und Analyse im Schnitt eine Ping-Zeit von 60 bis 100ms[119] bzw. 40 bis 60ms.[120]

Der Internetzugang über Mobilfunk ist jedoch – wie auch das Fernsehkabel – eine geteilte Ressource (so genanntes shared medium). Die rivalisierende Nutzung innerhalb einer Funkzelle führt zu einer Minderung der für den Einzelnen verfügbaren Bandbreite. Infolgedessen werden die in der Praxis technisch möglichen Bandbreiten und Ping-Zeiten nicht immer erreicht. Dennoch sind in LTE-Ausbaugebieten und Gegenden mit schwachem (oder gar keinem) DSL-Ausbau höhere Bandbreiten als mit DSL möglich. Diese maximal erreichbaren Bandbreiten stehen jedoch – abhängig vom gewähltem Tarif – nur für ein begrenztes monatliches Datenvolumen (beispielsweise zehn Gigabyte) zur Verfügung. Wenn das monatlich zulässige Volumen ausgeschöpft ist, wird der Anschluss des Endkunden beispielsweise auf 384 Kbit/s beim Downstream und 64 Kbit/s beim Upstream[121] oder 64 kBit beim Downstream und 16 kBit beim Upstream[122] gedrosselt. Der schnellste derzeitige[123] Tarif von Vodafone[124] bietet bei 50 MBit 30 GB pro Monat. Bei voller Ausnutzung der Bandbreite ist das für den ganzen Monat zur Verfügung stehende Volumen nach eineinhalb bis zwei

[118] Alexander Spier: „Darf's ein bisschen schneller sein? – Wie sich LTE im mobilen Alltag schlägt“, in: c't 22/2012, Seite 84ff

[119] „Analyse: So schnell ist LTE in der Praxis“, a.a.O.

[120] Alexander Spier, a.a.O.

[121] So die Angaben der Deutschen Telekom AG beim LTE-Angebot „Call&Surf via Funk“.

[122] So die Angaben der Deutschen Telekom AG beim LTE-Angebot „Business Mobile Data XL“

[123] August 2012

[124] Der Tarif „Vodafone LTE Zuhause“

Stunden aufgebraucht. Dieses Verhältnis ist beim derzeit[125] schnellsten stationären LTE-Privatkunden-Tarif[126] der Telekom schlechter: bei maximal 100 MBit Bandbreite und 30 GB Volumen reicht dieses bei voller Bandbreite rund weniger als eine Stunde. Mobile Tarife beinhalten häufig deutlich geringere monatliche Volumen. Der teurere Geschäftskundentarif der Telekom bietet die Möglichkeit, gegen weiteren Aufpreis die zur Verfügung stehende Bandbreite auch bei größerem Volumen hoch zu halten. Vodafone bietet ähnliches an, dort sind die Tarife aber nur für Rahmenvertragskunden erhältlich.

LTE ist gegenüber einem DSL-Anschluss mit weiteren Einschränkungen verbunden. So ist es nicht ohne Weiteres möglich eine feste, öffentliche IP-Adresse zu beziehen.[127] Dies kann jedoch für Anwender (beispielsweise Unternehmen), die einen Webserver oder ein VPN (Virtual Private Network) betreiben wollen, notwendig sein. Darüber hinaus wird die Nutzung innovativer Dienste, wie beispielsweise Voice-over-IP (VoIP), Instant Messaging, Peer-to-Peer-Kommunikation oder der Aufbau von Virtuellen Privaten Netzen (VPN) zur sicheren verschlüsselten Datenübertragung zwischen mehreren Endpunkten häufig vertraglich ausgeschlossen[128]

Die Vergabe der Frequenzen für die vierte Mobilfunkgenerationen (LTE) mit Auflagen zu einer vorrangigen Versorgung „weißer Flecken“ hat bewirkt, dass die flächendeckende Breitbandversorgung vorangetrieben wurde: Im April 2012 hat die Bundesnetzagentur festgestellt, dass die Versorgungsauflagen zu diesem Zeitpunkt bereits für acht Bundesländer erfüllt waren[129].

Insgesamt stellt LTE eine Alternative für die Anbindung von Gebieten, in denen in naher Zukunft kein DSL-Ausbau zu erwarten ist, dar. Die kabelgebundene Versorgung mit Internet bietet aber weiterhin prinzipbedingt einige Vorteile. Trotz aller Einschränkungen ist LTE

---

[125] Stand Januar 2013

[126] Der Tarif „Call & Surf Comfort via Funk“

[127] Bei Internet über Mobilfunk, so auch bei LTE, erhalten die Kunden in der Regel nur eine private IP-Adresse des Netzbetreibers. Bei der Kommunikation mit dem Internet wird mittels Network Adress Translation (NAT) die verbindung hergestellt. Dabei teilen sich oft mehrere tausend Nutzer eine öffentliche IP-Adresse. Es gibt jedoch Produkte von Drittanbietern, die den Bezug einer festen, öffentlichen IP-Adresse auch hinter NAT ermöglichen. Dazu wird ein VPN (Virtuelles privates Netzwerk) zu dem Anbieter aufgebaut, der dieses wiederum per NAT mit einer festen IP-Adresse ans öffentliche Netz anbindet. Dies ist mit weiteren Kosten, höherer Latenz und größerem Ausfallrisiko verbunden.

[128] So zum Beispiel bei den LTE-Datentarifen der Deutschen Telekom und Vodafone.

[129] Pressemitteilung der BNetzA: http://www.bundesnetzagentur.de/cln_1912/DE/Sachgebiete/Telekommunikation/RegulierungTelekommunikation/Frequenzordnung/OeffentlicherMobilfunk/VergabeVerfahrenDrahtlosNetzzugang/Versorgungsverpflichtung800MHzFreqs_Basepage.html

kurzfristig eine alternative Übergangslösung, bis mit weniger Restriktionen verbundene kabelgebundene Lösungen vorliegen.

I.3.1.2.2 Satellit

Weniger fur die Massenversorgung, aber doch für spezielle Aufgabengebiete – nicht zuletzt für die Versorgung sehr abgelegener Gebiete – ist auch die Anbindung über Satellit mit einem Downstream von bis zu 18 Mbit/s möglich. Diese geht jedoch mit einigen technisch bedingten Nachteilen einher, wie beispielsweise einer hohen Latenz beim Datentransport sowie relativ hohen Kosten, wenn auch der Upload mit hoherer Bandbreite über eine sendefähige Satellitenantenne erfolgen soll. Bei einigen Anbietern sind zudem die Übertragungsgeschwindigkeiten sehr ungleichmaßig. Dadurch ist fraglich, inwieweit diese Technik gerade den Anforderungen bestimmter Unternehmen gerecht werden kann. Für die Endverbraucher liegen die Monatstarife über denen von DSL-Anschlüssen. Am ehesten kommt daher ein Einsatz an abgelegenen Orten in Betracht. Zunehmend ist hier jedoch eine Verdrängung durch die wachsende Verbreitung mobiler Versorgung der neuesten Generation (LTE) zu erwarten.

I.3.1.2.3 Sonstige Funkzugangstechnologien

Die so genannten freien Funknetze stellen eine weitere Alternative dar. Es handelt sich um WLAN(Wireless Local Area Network)-basierte Funknetze, die nicht von kommerziellen Anbietern, sondern von Privatpersonen, Vereinen oder ähnlichen Organisationen betrieben werden. Zum Beispiel stellt beim Freifunk[130] jeder Nutzer seinen WLAN-Router für den Datentransfer der anderen Teilnehmer zur Verfügung. Im Gegenzug kann er ebenfalls Daten über das interne Freifunk-Netz übertragen oder von Teilnehmern eingerichtete Dienste nutzen wie Chat, Telefonie, Onlinegaming. Viele Teilnehmer stellen außerdem ihren Internetzugang zur Verfügung und ermöglichen so den anderen Teilnehmern erst den Zugang. Freifunk wird oft in Kombination mit Richtfunk betrieben, so dass Reichweiten von mehreren Kilometern realisiert werden können. Leider steht das Freifunk-Modell durch die geltenden Haftungsregelungen unter Druck, da nicht ausgeschlossen werden kann, dass der Anschlussinhaber für Rechtsverletzungen zur Verantwortung gezogen wird, die über sein offenes WLAN begangen werden. In der Praxis betrifft dies vor allem Urheberrechtsverletzungen. Im Spannungsfeld zwischen „Abmahnwahn“ und

[130] Vgl. Website start.freifunk.net. Online abrufbar unter: http://start.freifunk.net/

Providerhaftung stellt das offene WLAN ein besonderes und bis dato ungelöstes Rechtsproblem dar.[131] Die Freifunk-Community ist Teil einer globalen Bewegung für freie Infrastrukturen, deren Vision die Demokratisierung der Kommunikationsmedien durch freie Netzwerke ist.

Andere Funkzugangstechnologien, wie zum Beispiel Richtfunk, haben kaum Relevanz für Einzelanbindungen im Privatgebrauch. Auch sie können aber für spezialisierte Zwecke im gewerblichen Bereich oder aber für Sammelanbindungen abgelegener Ortschaften eingesetzt werden, um die mangelnde Rentabilität eines kabelgebundenen Anschlusses zumindest für einen Übergangszeitraum auszugleichen.

I.3.2 Wettbewerb im Internetzugangsmarkt

Wie bereits dargelegt wurde, kommt einem funktionsfähigen Wettbewerb im Telekommunikationsmarkt eine hohe Bedeutung für die Erreichung verschiedenster Zielsetzungen zu: Neben der Steigerung von Qualität und der Gewährleistung wettbewerbsorientierter Endkundenpreise trägt ein intensiver Wettbewerb insbesondere auch wesentlich zur Schaffung eines flächendeckenden Zugangs zum Internet bei. Trotzdem gibt es Gebiete, in denen bisher noch kein breitbandiger Internetzugang zur Verfügung steht. Durch die Vorgabe bei der Frequenzzuteilung, bisher unterversorgte Gebiete zuerst mit Mobilfunk der vierten Generation zu versorgen, konnte dies aber teilweise kompensiert werden.

Dies gilt gleichermaßen für den Wettbewerb der Infrastrukturen untereinander als auch für den Wettbewerb der über eine einzelne Infrastruktur realisierten Dienste. Letzterer erlangt dort besondere Bedeutung, wo aus ökonomischen Gründen der parallele Aufbau mehrerer Infrastrukturen wirtschaftlich nicht möglich ist. Gerade beim Ausbau von Ultra-Breitband sind oft derart hohe Investitionen notwendig, dass ein Ausbau nur unter Nutzung von Synergien zwischen den Infrastrukturbetreibern sinnvoll erscheint. Für eine hinreichende Auslastung einer neu errichteten Netzinfrastruktur als Voraussetzung für deren Amortisierung sind häufig Penetrationsraten notwendig, die im Falle einer weiteren, ebenso leistungsfähigen Konkurrenzinfrastruktur nur schwer zu erreichen sind. Um unter diesen Gegebenheiten einen funktionsfähigen Wettbewerb zu ermöglichen, ist es zwingend notwendig, die Realisierung

[131] Dem Petitionsausschuss des Deutschen Bundestages liegt eine Petition (Netzzugang – Rechtsnorm für Zugang zu kabellosen Netzwerken, 4. Januar 2011, Nr. 15983) zu diesem Thema vor. Die Petition befindet sich zur Zeit bei den Berichterstattern zur Prüfung. Die Petition ist online abrufbar unter: https://epetitionen.bundestag.de/epet/petition/pdfdownload?petition=15983

von im Wettbewerb stehenden Diensten durch verschiedene Diensteanbieter auf der Infrastruktur zu ermöglichen.

Die Anbieterstruktur hat sich seit Mitte der 1990er Jahre stark verändert: Damals war sie geprägt durch viele kleine lokale Anbieter, die aber keine eigene Leitungsinfrastruktur betrieben. Die Einwahl ins Internet erfolgte über das normale Telefonnetz; die verfügbaren Modems modulierten die Datenübertragung mit Tönen im hörbaren Bereich. Die letzte Meile bis zum Endkunden wurde also in der Regel über die normale Telefonleitung des ehemaligen Monopolisten betrieben. Mit dem Einsatz neuer Technologien wie DSL und dem Einstieg bundesweiter Internetzugangsanbieter änderte sich dies: Der harte Wettbewerb und niedrige Gewinnmargen im Endkundengeschäft sorgten dafür, dass viele kleine Anbieter nicht mehr mithalten konnten und nun nur noch spezielle Nischen bedienen oder ganz verschwunden sind. Der Markt wird im Wesentlichen von sieben Providern[132] beherrscht, wobei die Telekom als Ex-Monopolist auf rund 50 Prozent Marktanteil kommt. Im Gegensatz zu den 1990er Jahren herrscht in gut ausgebauten Gebieten allerdings ein Wettbewerb auf der letzten Meile sowie verschiedener Infrastrukturen. Die für Endkunden sichtbarste Folge der Veränderungen sind insgesamt drastisch gefallene Kosten.

I.3.2.1 Wettbewerb verschiedener Infrastrukturen

Die dargestellte technische Entwicklung erlaubt in städtischen Gebieten zunehmend auch einen intensiven Wettbewerb verschiedener Infrastrukturen, die alle eine nachfragegerechte Breitbandversorgung ermöglichen. Dies schließt in jedem Fall die oft parallel ausgebauten Festnetztechnologien Kupfer- und TV-Kabel, zunehmend auch Glasfaserkabel, ein. Hinzu tritt die dank neuer Mobilfunkgenerationen immer leistungsfähiger werdende Mobilfunkversorgung, die mit LTE sogar zu einer validen Alternative zu einem Festnetzanschluss wird.

Diese heterogene Infrastruktur aus regionalen, teilweise auch lokalen Glasfaser- und glasfaserbasierten TV-Kabelnetzen sowie den Mobilfunknetzen wird die Markt- und Wettbewerbslandschaft künftig genauso prägen wie die Vielschichtigkeit der Marktteilnehmer. Neben klassischen Telekommunikationsunternehmen und reinen Dienstleistungsanbietern beteiligen sich zunehmend zum Beispiel auch Stadtwerke und Energieversorgungsunternehmen mit einer Vielzahl unterschiedlicher Kooperations- und

[132] Vgl. dazu die Ausführungen unter: http://www.onlinekosten.de/breitband/breitbandkunden

Risikoteilungsmodellen am Aufbau und Betrieb aktiver und passiver Infrastrukturen. Trotz der mit Kooperationen erzielbaren Synergieeffekte und Wirtschaftlichkeitsvorteile ist ein paralleler Aufbau mehrerer Hochgeschwindigkeitsnetze mit Blick auf den hohen Fixkostenanteil gerade in dünn besiedelten Regionen ökonomisch häufig aber nicht sinnvoll. Deshalb bedarf es neben dem Infrastrukturwettbewerb vor allem in diesen Bereichen des zusätzlichen Wettbewerbs auf der Ebene der über diese Infrastrukturen realisierten Telekommunikations- und Telemediendienste.

Insbesondere beim künftigen Glasfaserausbau zeigt die bereits zitierte WIK-Studie für das NGA-Forum der Bundesnetzagentur, dass ein wirtschaftlicher Ausbau oft erst bei Penetrationsraten von mindestens 60 Prozent möglich ist und Kooperationen beim Aufbau und Betrieb daher von zentraler Bedeutung sind.[133]

Um für die Endkunden trotz der gegebenenfalls vorhandenen Dominanz einer einzelnen kabelgebundenen Glasfaserinfrastruktur in der betreffenden Region ein umfassendes und vielfältiges Diensteangebot mit möglichst gleichgearteten Leistungsmerkmalen sicherstellen zu können, stehen grundsätzlich freiwillige oder regulierte Open Access-Zugangmodelle auf Vorleistungsebene zur Wahl. Unter Open Access wird ein Konzept zum Zugang zu Vorleistungsprodukten eines Infrastrukturinhabers verstanden.[134] Freiwillige Zugangsmodelle basieren auf den Prinzipien der Freiwilligkeit, Transparenz und Diskriminierungsfreiheit und setzen zunächst auf freiwillige Angebote, Kooperationen und Verhandlungslösungen der Marktteilnehmer selbst. Regulierte Zugangsmodelle basieren demgegenüber auf regulatorischen Vorabverpflichtungen, mit denen diskriminierungsfreie Zugangs- und Nutzungsbedingungen für alle Marktteilnehmer durch die nationalen Regulierungsbehörden ex ante geschaffen werden. Beide Modelle zielen in unterschiedlichem Maße darauf ab, dass Provider und Diensteanbieter ohne eigene Infrastruktur vor Ort den Endkunden weiterhin attraktive Angebote unterbreiten können, die Auslastung und Effizienz der errichteten Netze erhöht wird und der Wettbewerb aufrechterhalten bleibt.

---

[133] Vgl. Präsentation des WIK: Implikationen eines flächendeckenden Glasfaserausbaus und sein Subventionsbedarf – Zusammenfassung der Ergebnisse eines Forschungsprojektes. 2011, S. 32ff. Online abrufbar unter: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/NGAForum/15teSitzung/NGAForum201109_WIKStudieFolien.pdf?__blob=publicationFile

[134] Hinweis: Der Begriff Open Access wird auch im Kontext mit Wissenschaft und Forschung verwandt. Dort bezeichnet er die für Nutzer kostenfreie und öffentlich zugängliche Bereitstellung wissenschaftlicher Publikationen und Daten im Internet. Siehe hierzu den Bericht der Projektgruppe Bildung und Forschung (BT-Drucksache 17/XXXX). Online abrufbar unter: www….

Beim Glasfaserausbau wird angesichts der bereits erwähnten hohen Investitionskosten eine zusätzliche Komplexität entstehen. Anders als bei der Errichtung des Kupferkabelnetzes durch den damaligen Staatsmonopolisten gibt es beim Aufbau eines bundesweit flächendeckenden Glasfasernetzes nicht mehr nur einen zentralen Akteur. Wie bereits ausgeführt, werden häufig lokal und regional eigenständige Unternehmen den Ausbau vorantreiben, oft dabei auch Unternehmen aus anderen Branchen, etwa Energieunternehmen oder Stadtwerke. Beim Aufbau und Betrieb dieser Breitbandinfrastrukturen wird der Gewährleistung von Interoperabilität eine essenzielle Bedeutung zukommen. Die steigende Anzahl lokaler Breitbandnetze erfordert die technische Standardisierung von Schnittstellen und Prozessen, um den Netzzugang zu ermöglichen. Eine zu große Vielfalt von Schnittstellen und Prozeduren wird nicht mehr praktikabel sein. Deshalb ist eine bundesweite Definition standardisierter Schnittstellen und Prozesse von erheblicher Bedeutung, um Zugang und damit einen intensiven Wettbewerb bei den auf der Infrastruktur realisierten Diensten zu erreichen.[135]

I.3.2.2 Fortdauernde Bedeutung des Dienstewettbewerbs innerhalb einer Infrastruktur

Im Rahmen der Liberalisierung des Telekommunikationssektors hat der Dienstewettbewerb, das heißt bei Verwendung zumindest teilweise derselben Infrastruktur, einen wesentlichen Beitrag zur Entstehung eines intensiven Wettbewerbs geleistet. Deutschland steht hier – gerade auch dank der entsprechenden regulatorischen Vorgaben – im internationalen Vergleich mit einem grundsätzlich guten Wettbewerbsergebnis dar.[136] In der Betrachtung der Bedeutung des Dienstewettbewerbs ist daher zwischen Auf- oder auch Ausbau der Netzinfrastruktur auf der einen und Betrieb von Netzinfrastruktur auf der anderen Seite zu unterscheiden. Während es beim Auf- und Ausbau um die Schaffung von

---

[135] Zum Thema Interoperabilität siehe den Bericht der Projektgruppe Interoperabilität, Standards, Freie Software (BT-Druchsache 17/XXXX). Online abrufbar unter: http://... .

[136] So ist etwa im internationalen Vergleich des von der Organisation for Economic Co-operation and Development (OECD) herausgegebenen OECD Communications Outlook 2011 der Marktanteil von neuen Marktteilnehmern im Wettbewerb („New entrants“) an den Festnetzanschlüssen für Deutschland im Jahr 2009 mit 33 Prozent ausgewiesen und hat damit im europäischen Vergleich einen der höchsten Werte. Vgl. OECD Communications Outlook 2011, S. 57. Online abrufbar unter: www.oecd.org/sti/telecom/outlook. Der Anteil hat sich seitdem in Deutschland weiter erhöht (38 Prozent im Jahr 2011 nach dem Tätigkeitsbericht Telekommunikation 2010/11 der Bundesnetzagentur, S. 31 ff. Online abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/TaetigkeitsberichtTK20102011pdf.pdf?__blob=publicationFile. Hinzu kommt ein steigender Wettbewerbsabteil der Kabelanbieter. Unverändert verfügt aber der Incumbent Deutsche Telekom in relevanten Märkten über erhebliche Marktmacht im Sinne der EU-TK-Marktregulierung.

Infrastruktuwettbewerb geht, gilt beim Betrieb, dass hier auch ein reiner Dienstewettbewerb seine eigenständige Relevanz zur Sicherung vielfältiger und attraktiver Angebote für den Endkunden auch bei sich entwickelndem Infrastrukturwettbewerb behält.

Von besonderer Bedeutung ist der Dienstewettbewerb insbesondere dort, wo aus wirtschaftlichen Gründen eine Dopplung von Infrastrukturen nicht zu erwarten ist. Hier kommt einem funktionierenden Dienstewettbewerb auf einer einheitlichen Infrastruktur eine zentrale Rolle zu. Beim gemeinsamen Aufbau und Betrieb von Telekommunikationsinfrastrukturen haben die Gewährleistung von Interoperabilität, die Förderung von Investitionen und Innovationen sowie die Sicherung von Wettbewerb und Wahlfreiheit der Endverbraucher im Mittelpunkt zu stehen. Künftig werden Unternehmen den Zugang zu Netzen Dritter nachfragen, um ein möglichst flächendeckendes Produktangebot zu erreichen, denn viele Marktakteure werden auch künftig Produkte bundesweit anbieten wollen und aus wirtschaftlicher Sicht sogar müssen.

Der Zugang zu Netzen Dritter sichert so einen diskriminierungsfreien Wettbewerb und sorgt damit für Angebote, die es den Endkunden ermöglichen, frei zwischen möglichst unterschiedlichen Produkten, Qualitäten, Preisen und Anbietern zu entscheiden.

An dieser Stelle kommt der Entwicklung von Marktlösungen in Form von freiwilligen oder regulierten Kooperationsmodellen eine zentrale Bedeutung zu – das Stichwort lautet Open Access beim Netzzugang. Dort, wo sich und soweit sich Infrastrukturinhaber und Nachfrager unter Beachtung der Prinzipien Freiwilligkeit, Transparenz und Diskriminierungsfreiheit auf Leistungsspezifika und Preise für einen Zugang einigen, kann freiwilliges Open Access auch als marktgerechte und wettbewerbsfördernde Alternative zur herkömmlichen Regulierung angesehen werden. Das freiwillige Open Access-Konzept ist jedoch keinesfalls mit symmetrischer Regulierung gleichzusetzen oder zu verwechseln. Im Fall der Nichteinigung auf kommerzieller Basis können regulatorische Instrumente zur Anwendung kommen, wie zum Beispiel die Anordnung von Zugangsansprüchen oder eine Entgeltregulierung im Rahmen der entsprechenden rechtlich-regulatorischen Voraussetzungen, etwa nach den Regelungen und Verfahren des Telekommunikationsgesetzes (TKG).

Zwar ist im Telekommunikationsgesetz die Regulierung einer marktbeherrschenden Stellung der wesentliche Ansatz. Darüber hinaus ist es nach den neuen EU-Richtlinien, insbesondere

nach Artikel 12 der Rahmenrichtlinie[137], aber auch möglich, Unternehmen beziehungsweise Eigentumsrechteinhabern symmetrische Regulierungsverpflichtungen aufzuerlegen.

„Die nationale Regulierungsbehörde kann demnach unter Beachtung der Verhältnismäßigkeit die gemeinsame Nutzung [vorhandener Infrastruktur] vorschreiben, wozu unter anderem Gebäude, Gebäudezugänge, Verkabelungen in Gebäuden, Masten, Antennen, Türme oder andere Trägerstrukturen, Leitungsrohre, Leerrohre, Einstiegsschächte und Verteilerkästen gehören.“ [138] In anderen europäischen Ländern (zum Beispiel Frankreich oder Portugal) haben die nationalen Regulierungsbehörden bereits entsprechende Zugangsverpflichtungen für die Inhaus-Verkabelung erlassen, welche als Engpass beziehungsweise notwendige Voraussetzung betrachtet wird. Ein Gutachten des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste (WIK) vom Februar 2011 schlägt entsprechende Maßnahmen auch für Deutschland vor. Exklusivvereinbarungen mit Kabelnetzbetreibern halten die Autoren hingegen für „regulierungsökonomisch problematisch“.[139]

I.3.2.3 Auswirkung zunehmender Verbreitung integrierter Geschäftsmodelle

Schon heute ist zu beobachten, dass viele Telekommunikationsanbieter neben den reinen Transportleistungen und der Sprachtelefoniefunktion auch weiterführende Dienste, etwa Fernsehen/Video im Paket anbieten (Triple-Play/Quadruple-Play[140]). Es ist anzunehmen, dass diese Entwicklung auch in Zukunft weiter voranschreiten wird, da eine Refinanzierung der immer leistungsfähigeren Internetzugangsdienste erleichtert wird, wenn zusätzliche Erlöse über weitere Dienste erzielt werden können. Zugleich steigt die Zahlungsbereitschaft der Kunden, wenn sie den Mehrwert einer höheren Leistungsbereitschaft der Anschlüsse durch leistungsfähigere Dienste erkennen. Die Bereitstellung verschiedener Dienste aus einer Hand ist dabei keine Notwendigkeit, aber ein von den Kunden besonders gern akzeptiertes Modell, da dieses Klarheit über den Ansprechpartner, eine vereinfachte Abrechnung und technisch voll integrierte Gesamtangebote erlaubt.

---

[137] 2002/19/EG, 7. März 2002, Zugangsrichtlinie

[138] Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (WIK): Symmetrische Regulierung: Möglichkeiten und Grenzen im neuen EU-Rechtsrahmen. Autoren: Lorenz Nett, Ulrich Stumpf. Bad Honnef, Februar 2011. S. III.

[139] Ebd., S. 27.

[140] Triple-Play ist ein Begriff des Marketing und bezeichnet die Bündelung von drei Diensten (TV, Internet und Telefonie) in einem Angebot. Beim Quardruple-Play ist zusätzlich die Mobilkommunikation enthalten.

Den Vorteilen von integrierten Geschäftsmodellen für den Endkunden stehen aber auch potenzielle Bedrohungen für den Wettbewerb sowie die Wahrung der Netzneutralität gegenüber. Dies gilt etwa für den theoretischen Fall, dass ein Netzbetreiber seine eigenen Dienste beim Zugang zu Vorleistungen/Infrastrukturleistungen bevorzugen würde.[141] Auch aus einer bevorzugten Positionierung oder gesonderten Verkaufsförderung eigener beziehungsweise verbundener Dienste im Rahmen von Orientierungshilfen im Netz (zum Beispiel Suchmaschinen, Benutzeroberflächen, App Stores, Elektronischen Programmführern (Electronic Program Guide – EPG)) können Gefahren für den Wettbewerb erwachsen.

Gegen solche Missbräuche stehen bereits heute Schutzmechanismen zur Verfügung. Sie reichen von einfachen Nichtdiskriminierungsauflagen oder auch konkreten Zugangsansprüchen über Transparenzpflichten bis hin zu einschneidenden Maßnahmen wie der Untersagung integrierter Geschäftsmodelle oder gar die Aufspaltung entsprechender Unternehmen. Letztere kommen aber nur als Ultima Ratio in Betracht.

I.3.3 Staatliche Handlungsoptionen zur Förderung von Breitbandverfügbarkeit

Neben der Rolle als Bewahrer von Wettbewerb und der Verhinderung von Fehlentwicklungen im Markt kann der Staat auch aktiv eine Rolle zur Förderung der Verfügbarkeit leistungsfähiger Internetzugänge übernehmen.

I.3.3.1 Berücksichtigung der Nachfrageentwicklung

Eine möglichst flächendeckende Verfügbarkeit hochleistungsfähiger Kommunikationsinfrastruktur zu erreichen, wird zu einem zentralen Ziel für die Wettbewerbsfähigkeit einer hoch entwickelten Industrienation. Bei der Bestimmung des nur stufenweise erreichbaren Ziels muss jedoch auch immer die tatsächlich bestehende Nachfrage berücksichtigt werden. Diese ist bestimmender Faktor für die Wirtschaftlichkeit bei der Schaffung entsprechender Angebote. Marktuntersuchungen zeigen, dass bislang nur eine geringe Ausprägung der auch durch zusätzliche Zahlungsbereitschaft hinterlegten Nachfrage

---

[141] Dies würde zudem einen Verstoß gegen das in der zuständigen Projektgruppe und im Rahmen des nationalen IT-Gipfels erarbeitete Verständnis von Netzneutralität darstellen. Vgl. hierzu den vierten Zwischenbericht der Enquete-Kommission Internet und digitale Gesellschaft – Netzneutralität, Bundestagsdrucksache 17/8536. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zwischenberichte/Zwischenbericht_Netzneutralitaet_1708536.pdf sowie Bundesministerium für Wirtschaft und Technologie: Netzneutralität – 11 Thesen für eine gesellschaftspolitische Diskussion. 2010. S. 2, These 10. Online abrufbar unter: http://www.it-gipfel.de/Dateien/BMWi/PDF/IT-Gipfel/it-gipfel-2010-netzneutralitaet,property=pdf,bereich=itgipfel,sprache=de,rwb=true.pdf

der Kunden nach noch leistungsfähigeren Anschlüssen besteht, wenn bereits ein Anschluss mit einer Bandbreite zur Nutzung der gängigen Anwendungen vorhanden ist.[142] Erst das schrittweise Entstehen immer neuer Verwendungsformen und attraktiver Diensteangebote könnte diese Zahlungsbereitschaft langsam steigen lassen. Insofern kommt der Entwicklung innovativer Dienste eine ebenso große Bedeutung für den Breitbandausbau zu wie dem eigentlichen Ausbau der Infrastruktur; beide können nur Hand in Hand erfolgen. Demzufolge kann auch die Entwicklung entsprechender staatlicher Angebote, etwa in den Bereichen E-Government[143], E-Learning[144] oder E-Health[145], eine fördernde Wirkung auf die Nachfrage nach Breitbanddiensten und damit auf den Ausbau von Hochgeschwindigkeitsnetzen haben.

I.3.3.2 Förderung von Kooperationen

Angesichts der hohen Investitionssummen, die für den weiteren Ultra-Breitband-Ausbau in Deutschland erforderlich sind, wird Kooperationen verschiedener Unternehmen eine immer größere Bedeutung zukommen. Von den Kosten für den Ausbau der Festnetzinfrastruktur entfallen etwa 70 Prozent auf den Tiefbau.[146] Daher wird etwa in der *Breitbandstrategie der Bundesregierung* die Mitbenutzung bestehender passiver und aktiver Infrastrukturen angeregt.[147] Effiziente Investitionen und Innovationen im Bereich neuer und verbesserter Infrastrukturen können dabei auch dadurch gefördert werden, dass bei Regulierungsentscheidungen Investitionsrisiken berücksichtigt sowie kartellrechtlich unbedenkliche Vereinbarungen zur Verteilung des Investitionsrisikos zwischen Investoren und Zugangsbewerbern zugelassen werden.

Unterstützend wirkt, wenn Kooperationen von Netzbetreibern auf möglichst geringe administrative Hürden treffen. Gleichzeitig kann in einem solchen Fall der Wettbewerb gesichert werden, indem neben der Berücksichtigung der allgemeinen kartellrechtlichen

---

[142] Nach der bereits zitierten Markstudie der United Internet Media für das NGA-Forum der Bundesnetzagentur von November 2010 (vgl. Fußnote 114) hatten 38 Prozent der Befragten überhaupt keine Zahlungsbereitschaft, unter den überhaupt Zahlungsbereiten hatte die Mehrheit eine maximale Zahlungsbereitschaft von bis zu fünf Euro Aufpreis pro Monat.

[143] E-Government wird laut Duden bezeichnet als die „Durchführung von Prozessen, die zwischen staatlichen Institutionen oder zwischen staatlicher Institution und Bürger ablaufen, mithilfe der Informationstechnologie".

[144] E-Learning wird laut Duden bezeichnet als „computergestütztes Lernen, bei dem Schüler und Lehrer räumlich getrennt voneinander sind und vor allem über das Internet in Kontakt stehen".

[145] E-Health wird laut Duden bezeichnet als „Einsatz von Computern und Internet im Gesundheitswesen".

[146] Vgl. Bundesministerium für Wirtschaft und Technologie: Breitbandstrategie der Bundesregierung. Februar 2009, S. 10. Online abrufbar unter: http://www.bmwi.de/Dateien/BBA/PDF/breitbandstrategie-der-bundesregierung,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf

[147] Vgl. ebd., S. 10 f.

Diskriminierungsregeln auch Zugang für Dritte nach dem bereits beschriebenen Open Access-Grundsatz von den Kooperationspartnern gewährt wird.

Förderlich auf den Breitbandausbau kann sich auch die Sammlung, Aufbereitung und Bereitstellung von Informationen über bestehende und nutzbare Infrastrukturen auswirken, die entweder in staatlicher Hand ohnehin verfügbar sind oder die der Staat als Moderator zwischen den verschiedensten Beteiligten zusammentragen und veröffentlichen kann. Beispiele hierfür sind der bereits existierende Infrastrukturatlas[148] oder der zumindest in einzelnen Bundesländern bereits verwirklichte Grabungsatlas[149]. Durch die Nutzung geeigneter Infrastrukturen oder ohnehin geplanter und insoweit geeigneter Bauvorhaben für die Verlegung von Glasfaserinfrastrukturen lassen sich ökonomisch unsinnige Doppelgrabungen vermeiden und Belästigungen für die Anwohner durch Baulärm erheblich reduzieren. Der Wert solcher Datensammlungen steigt wesentlich, wenn eine Datenbank sämtliche relevanten und geeigneten Baumaßnahmen umfasst und nicht allein diejenigen öffentlicher Träger. Im Falle regionaler und lokaler Datenbanken hilft die Bereitstellung einheitlicher Schnittstellen, da diese die Datennutzung für ausbauwillige Unternehmen wesentlich erleichtert.

Weiterhin hat sich im Rahmen der Arbeit des NGA-Forums der Bundesnetzagentur in den letzten Jahren gezeigt, dass auch in der Förderung und der Moderation des Dialogs der Marktteilnehmer untereinander ein wesentlicher Beitrag des Staates liegen kann. Hierdurch ist es gelungen, nicht nur ein gemeinsames Verständnis von den zukünftigen technischen und wirtschaftlichen Herausforderungen des NGA-Ausbaus zu entwickeln, sondern ganz konkret Vereinbarungen zur Schaffung von Interoperabilität bei zukünftigen Kooperationen von Netzbetreibern auf der einen Seite und Diensteanbietern auf der anderen Seite zu treffen.[150] Dies ist als maßgeblicher Schritt für die künftige Entwicklung von NGA-Netzen anzusehen, da eine Standardisierung bei der technischen Interoperabilität und der Ausgestaltung von

---

[148] Weiterführende Informationen zum Infrastrukturatlas sind auf der Webseite der Bundesnetzagentur zu finden. Online abrufbar unter: http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Infrastrukturatlas/infrastrukturatlas_node.html

[149] Als Beispiel kann der Grabungsatlas des Geodaten-Informationsdienstes Bayern genannt werden. Online abrufbar unter: http://geoportal.bayern.de/GeoportalBayern/anwendungen/Suche/q=grabungsatlas/

[150] Vgl. Bundesnetzagentur: Bericht des NGA-Forums. 8. November 2011. S. 7 f. Online abrufbar unter: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/NGAForum/16teSitzung/Endbericht_NGAForum_111108.pdf?__blob=publicationFile. Die einzelnen Spezifikationen sind zusammengestellt und verlinkt auf der Webseite der Bundesnetzagentur. Online abrufbar unter: http://www.bundesnetzagentur.de/cln_1932/DE/Sachgebiete/Telekommunikation/ RegulierungTelekommunikation/NGAForum/NGAForum_Basepage.html

Geschäftsprozessen zwangsläufige Voraussetzung ist, um zu wirtschaftlich darstellbaren Konditionen Vorleistungskooperationen in diesem Markt zu realisieren.

I.3.3.3 Investitionszuschüsse

Ein wirtschaftlicher Ausbau ist nicht immer möglich, weil etwa die Topographie eine Erschließung massiv verteuert. Infolgedessen können den Kunden keine ausreichenden Zugänge angeboten werden. In diesen Regionen können im Einzelfall auch Investitionszuschüsse der öffentlichen Hand beziehungsweise gezielte Investitionsanreize helfen.[151] Neben der direkten Zahlung sind hier beispielsweise auch steuerliche Vergünstigungen denkbar. Daneben kann dies auch durch Verbindung von Ausbaupflichten mit der Gewährung sonstiger Rechte, etwa im Rahmen von Frequenzzuteilungsverfahren, einhergehen. Die erforderliche Wettbewerbsneutralität von solchen Vorteilsgewährungen an einzelne ausbauende Unternehmen kann durch zusätzliche Verpflichtungen der Begünstigten erreicht werden, etwa zu einer Zugangsgewährung nach den bereits beschriebenen Open Access-Regeln.

Die *Breitbandstrategie der Bundesregierung* weist auf die Bedeutung wettbewerbsneutraler staatlicher Förderprogramme für die Erschließung ländlicher Regionen mit breitbandiger Infrastruktur hin.[152] Gefördert wurde bislang beispielsweise im Rahmen der Gemeinschaftsaufgabe zur Verbesserung der Agrarstruktur und des Küstenschutzes (GAK).[153]

Daneben treten Fördermöglichkeiten der KfW-Bankengruppe. Im Rahmen des Vermittlungsverfahrens zum Telekommunikationsgesetz wurde verabredet, dass die Bundesregierung gemeinsam mit den Bundesländern und der KfW Vorschläge erarbeitet, um den Breitbandausbau in Deutschland noch gezielter zu fördern. Dabei sollen bestehende KfW-Programme sowohl für Kommunen als auch für Unternehmen präziser beschrieben und Maßnahmen zur Verbesserung des Bekanntheitsgrades ergriffen werden. Darüber hinaus soll eine erhöhte Transparenz der Programme zur Verbesserung der Antragsquote führen. Gleichzeitig wurde eine Evaluation der Nutzung von Bundes- und Länderprogrammen

---

[151] Vgl. Bundesministerium für Wirtschaft und Technologie: Breitbandstrategie der Bundesregierung. Februar 2009. S. 15 f. Online abrufbar unter: http://www.bmwi.de/Dateien/BBA/PDF/breitbandstrategie-der-bundesregierung,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf

[152] Vgl. ebd.

[153] Vgl. Bundesministerium für Wirtschaft und Technologie: Möglichkeiten der Breitbandförderung. Februar 2010, S. 6 f. Online abrufbar unter: http://www.bmelv.de/SharedDocs/Downloads/Broschueren/Breitbandfoerderung.pdf;jsessionid =2A79AAE87457D59D50F704686ECCC1A8.2_cid154?__blob=publicationFile

beziehungsweise möglicher Nutzungshemmnisse für den Breitbandausbau verabredet. Diese Evaluation soll gegebenenfalls Grundlage für eine Veränderung der Programme sein.

I.3.3.4 Universaldienstverpflichtung

Nach Artikel 32 der EU-Universaldienstrichtlinie[154] können die Mitgliedstaaten eine beliebige Bandbreite als Universaldienst festlegen, sofern die dadurch entstehenden Kosten nicht auf die Telekommunikationsunternehmen umgelegt werden. Eine Umlage ist nur zulässig, wenn hieraus keine Marktverzerrung entsteht. Gemäß Artikel 4 Absatz 2 der Richtlinie ist eine Umlage nur dann möglich, wenn die als Universaldienst vorgegebene Bandbreite nicht größer als die von der Mehrzahl der Teilnehmer verwendeten Bandbreiten ist. Die EU-Kommission erarbeitet derzeit eine Empfehlung über die Auslegung der Richtline im Hinblick auf die Implementierung eines Breitband-Universaldienstes. Klar ist, dass eine Universal-dienstverpflichtung aufgrund der europäischen Vorgaben technologieneutral ausgestaltet werden muss.

Die Befürworter einer Universaldienstverpflichtung weisen darauf hin, dass es in Deutschland trotz der Aktivitäten der Telekommunikationsunternehmen, der Fördergelder der Europäischen Union (EU), des Bundes und der Länder sowie lokaler Initiativen noch immer unterversorgte Gebiete geben könnte.

Daher argumentieren die Befürworter einer Universaldienstverpflichtung, dass die Telekommunikationsunternehmen, die nach Marktmechanismen investieren, nicht alle „weißen Flecken“ erschließen könnten und dass sich der Universaldienst ausschließlich auf die letzten, trotz bestehender Fördermaßnahmen weiterhin aus betriebswirtschaftlicher Sicht unrentablen „weißen Flecken“ sowie die bisher unterversorgten Regionen vor allem im ländlichen Raum auswirken würde. Mit einer Universaldienstverpflichtung würde man auf das Versagen des Marktes reagieren und die unter Kapitel I.2 dargestellte

[154] Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie) (ABl. L 108 vom 24.4.2002, S. 51–77). Online abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0051:0077:DE:PDF, zuletzt geändert durch: Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (ABl. L 337 vom 18. Dezember 2009, S. 11–36). Online abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:DE:PDF

verfassungsrechtliche Verpflichtung des Bundes erfüllen. Somit wäre der Universaldienst eine Ultima-Ratio-Maßnahme zur Sicherstellung eines bestimmten Grundversorgungsniveaus.

Die Kritiker einer Universaldienstverpflichtung befürchten, dass die Festlegung auf ein europarechtlich zulässiges Grundversorgungsniveau die Gefahr beinhalten würde, den Antrieb und die Anreize für eine zukunftsgerichtete Technologieausstattung durch die Privatwirtschaft zu mindern und die weitere Marktentwicklung zu verfälschen. Demzufolge würde die Schaffung eines Universaldienstes die Kräfte des Wettbewerbs, die wesentliche Treiber des Breitbandausbaus seien, außer Kraft setzen. Anreize für aus eigener Kraft finanzierte Ausbauinvestitionen kämen unmittelbar zum Erliegen, da es mit einer Universaldienstverpflichtung wirtschaftlicher wäre, auf die Anordnung eines durch Umlage finanzierten Ausbaus zu warten.

Die Netzbetreiber und die Aktivitäten der Politik u. a. durch Fördermittel der EU, des Bundes und der Länder haben in Deutschland in den vergangenen Jahren die Breitbandversorgung bei immer geringeren Endkundenpreisen erheblich verbessert. Nach Angaben der Bundesnetzagentur wurden zwischen 1998 und 2010 über 93 Milliarden Euro in moderne IT-Infrastrukturen investiert.[155] Breitbandanschlüsse von 1 Mbit/s sind heute nahezu flächendeckend verfügbar.

Die Nutzung der digitalen Dividende (LTE-Technik) wird die Breitbandversorgung kurzfristig weiter verbessern. Aufgrund der in Kapitel I.3.1.2.1 beschriebenen Einschränkungen kann LTE den Festnetzausbau allerdings nicht vollständig ersetzen.

[155] Ausweislich des Tätigkeitsberichts Telekommunikation 2010/ 2011 der Bundesnetzagentur beliefen sich die Investionen von 1998 bis 2010 auf insgesamt 93,3 Milliarden Euro. Der Anteil der alternativen Anbieter von dieser Summe betrug 48,5 Milliarden Euro (52 Prozent); 44,8 Millarden Euro (48 Prozent) entfielen auf die Deutsche Telekom AG. Vgl. hierzu Bundesnetzagentur: Tätigkeitsbericht Telekommunikation 2010/ 2011. 2011. S. 28. Online abrufbar unter: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/TaetigkeitsberichtTK20102011pdf.pdf?__blob=publicationFile

II. Sicherheit im Internet

II.1. Schutz Kritischer Infrastrukturen im Internet

II.1.1 Einleitung

Ein Leben ohne Informationstechnologie (IT) ist heutzutage kaum vorstellbar. Moderne Gesellschaften sind auf funktionierende Informationsinfrastrukturen genauso angewiesen wie auf eine zuverlässige Strom- und Wasserversorgung sowie auf gut ausgebaute Verkehrsnetze.

IT findet Anwendung in nahezu allen Lebensbereichen und hat sich damit zu einer Kritischen Infrastruktur entwickelt. Der Einsatz von IT in den klassischen Kritischen Infrastrukturen, wie zum Beispiel dem Energie- oder Transport- und Verkehrssektor, hat zu komplexen IT-abhängigen Systemen und hohen Interdependenzen zwischen verschiedenen Sektoren geführt. Fallen diese IT-abhängigen Systeme aus, kann dies zum Teil schwerwiegende Folgen haben wie folgende Beispiele belegen: Bei DENIC, der zentralen Registrierungsstelle für .de-Domains, fielen im Mai 2010 mehrere Server aus, wodurch viele deutsche Webseiten zeitweise nicht erreichbar waren.[156] Infolge eines Systemausfalls bei der Deutschen Flugsicherung (DSF) in München kam es im Juli 2012 zu Verspätungen und Ausfällen von Flügen.[157] An der New Yorker Börse führten im August 2012 Probleme mit den IT-Systemen zu einer zeitweisen Unterbrechung des Handels.[158]

Viele Prozesse in Unternehmen und Behörden sind auf das reibungslose Funktionieren der IT-Infrastrukturen angewiesen. Immer mehr Daten – seien es Unternehmensdaten oder private Daten – werden mit IT-Systemen erstellt und verarbeitet, über Netzwerke wie das Internet transportiert und lokal oder in der Cloud gespeichert. Der Schaden, der mit dem Verlust von Vertraulichkeit, Integrität und Verfügbarkeit von Daten einhergeht, kann für Behörden, Unternehmen und Private enorm sein. Ein Schutz der IT-Infrastruktur ist zugleich auch ein Schutz der Daten beziehungsweise der aus ihnen gewonnenen Informationen.

---

[156] Vgl. beispielsweise Spiegel Online: Ausfall der Adresszentrale – Server-Crash blockiert viele deutsche Webseiten. 12.05.2010. Online abrufbar unter: http://www.spiegel.de/netzwelt/web/ausfall-der-adresszentrale-server-crash-blockiert-viele-deutsche-webseiten-a-694551.html

[157] Vgl. beispielsweise Sueddeutsche.de: Systemausfall bei der Flugsicherung – Chaos am Münchener Flughafen. 06.07.2012. Online abrufbar unter: http://www.sueddeutsche.de/muenchen/erding/systemausfall-bei-der-flugsicherung-chaos-am-muenchner-flughafen-1.1404698

[158] Vgl. beispielsweise Financial Times Deutschland: Wall Street – Technikpanne verursacht Börsenchaos. 02.08.2012. Online abrufbar unter: http://www.ftd.de/finanzen/maerkte/:wall-street-technikpanne-verursacht-boersenchaos/70071350.html

Die Bedrohungen, denen IT-Systeme ausgesetzt sind, sind vielfältig. Sie können durch Naturgefahren, technische Defekte, menschliches Versagen sowie gezielte Angriffe verursacht sein. Durch die Anbindung an das Internet werden IT-Systeme anfällig für Angriffe. Obwohl das Internet nicht an sich als kriminell zu bertrachten ist, werdensowohl die Infrastruktur des Internets als auch die neu angebotenen Dienste als Tatmittel für kriminelle Handlungen, Sabotage- und Spionageakte missbraucht.[159] Gefährdet sind allerdings auch IT-Systeme, die nicht mit dem Internet verbunden sind. Der Fall des Computerwurms Stuxnet hat dies offenbart. Hier wurde die Schadsoftware mittels eines USB-Sticks durch Innentäter in das System eingeschleust. [160]

Die Vernetzung der Kritischen Infrastrukturen kann als die „Achillesferse moderner Gesellschaften“[161] bezeichnet werden. Neue Herausforderungen an die IT-Sicherheit ergeben sich aus der Komplexität der IT-Infrastruktur selbst, aus der weiter zunehmenden Vernetzung, welche „die Menge der systemübergreifenden Verwundbarkeiten erhöht“[162] und aus der Geschwindigkeit, mit der neue Bedrohungen entstehen.

Dabei wird es durch die weltweite Vernetzung „immer schwieriger, zwischen kriminellen und militärischen Bedrohungspotentialen, öffentlichen und privaten Interessen, politischen und geographischen Grenzen, innerer und äusserer Sicherheit von Staat und Gesellschaft zu unterscheiden.“[163]

Der Schutz Kritischer Infrastrukturen ist eine gesamtgesellschaftliche Aufgabe. Die Verbesserung der IT-Sicherheit und damit der möglichst weitgehende Schutz Kritischer Infrastrukturen kann nur durch gemeinsames Handeln von Staat, Wirtschaft und Gesellschaft erfolgen. Gleichzeitig handelt es sich nicht nur um eine nationale Aufgabe (siehe Kapitel II.1.3.3). Kritische Infrastrukturen werden über die Grenzen eines Staates hinweg betrieben. Daher ist auch eine europäische (siehe Kapitel II.1.3.2) und internationale (siehe Kapitel II.1.3.1) Zusammenarbeit unentbehrlich.

---

[159] Siehe hierzu auch die Ausführungen zur Verwendung des Schlagwortes „Internet als Tatmittel“ der Polizeilichen Kriminalstatistik in Kapitel II.2.1.1.

[160] Siehe um Beispiel: http://www.gulli.com/news/15859-sandro-gaycken-der-cyberwar-ist-realitaet-2011-04-16

[161] Spiegel-Online (Hrsg.): Cyberwar – USA und Russland wollen virtuellen Rüstungswettlauf verhindern. 14.12.2009. Online abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/cyberwar-usa-und-russland-wollen-virtuellen-ruestungswettlauf-verhindern-a-666880.html

[162] Gaycken, Sandro: Cyberwar: Das Internet als Kriegsschauplatz. 2010, S. 70.

[163] Geiger, Gebhard: „Information Warfare“ – Bedrohung und Schutz IT-abhängiger gesellschaftliche Infrastrukturen. DuD 24 (2000). S. 129.

II.1.1.1 Kritische Informationsinfrastrukturen als Teil Kritischer Infrastrukuren

Definitorisch ist zwischen Kritischen Infrastrukturen und Kritischen Informationsinfrastrukturen zu unterscheiden: Informationsinfrastrukturen werden dem Bereich der Informationstechnik zugeordnet. Sie bilden eine Teilmenge der Kritischen Infrastrukturen. Sowohl der Sektor der Informationstechnik und Telekommunikation als auch die IT-basierten Systeme – welche Hardware, Software sowie Computernetzwerke umfassen – anderer Sektoren der Kritischen Infrastrukturen werden dem Begriff der Informationsinfrastrukturen zugeordnet.[164]

Mit dem Schutz Kritischer Infrastrukturen befasst sich die vom Bundesministerium des Innern (BMI) herausgegebene *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*[165]. Die Sicherstellung des Schutzes Kritischer Informationsinfrastrukturen wird seit 2011 durch die *Cyber-Sicherheitsstrategie für Deutschland*[166] adressiert, welche den bis dahin geltenden *Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI)*[167] abgelöst hat. Um den Schutz der Informationsinfrastrukturen in den KRITIS-Branchen weiter zu fördern, hat das BMI in Zusammenarbeit mit den Betreibern Kritischer Infrastrukturen und deren Interessenverbänden den *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen (UP KRITIS)*[168] entwickelt. Für den Schutz der Informationsinfrastrukturen in der Bundesverwaltung hat die Bundesregierung den *Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung (UP Bund)* beschlossen.[169]

---

[164] Vgl. die Ausführungen des Bundesamtes für Sicherheit in der Informationstechnik: Schutz Kritischer Infrastrukturen. Online abrufbar unter: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/Kritis/Kritis_node.html sowie die Definition im Grünbuch über ein europäisches Programm für den Schutz kritischer Infrastrukturen. KOM(2005) 576 endgültig. Online abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0576:DE:NOT

[165] Bundesministerium des Innern (Hrsg.): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Juni 2009. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?__blob=publicationFile

[166] Bundesministerium des Innern (Hrsg.): Cyber-Sicherheitsstrategie für Deutschland. Februar 2011. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile

[167] Bundesministerium des Innern (Hrsg.): Nationaler Plan zum Schutz der Informationsinfrastrukturen. Juli 2005. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf?__blob=publicationFile

[168] Bundesministerium des Innern (Hrsg.): Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen (UP KRITIS). September 2007. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2007/Kritis.pdf?__blob=publicationFile

[169] Bundesministerium des Innern (Hrsg.): Nationaler Plan zum Schutz der Informationsinfrastrukturen. Juli 2005, S. 7. Online abrufbar unter:

Der Schwerpunkt des vorliegenden Kapitels liegt auf der Betrachtung Kritischer Informationsinfrastrukturen. Dennoch ist es zunächst notwendig, auf die Kritischen Infrastrukturen im Allgemeinen einzugehen. Anschließend werden Beispiele für die wachsende IT-Durchdringung der Kritischen Infrastrukturen aufgezeigt.

II.1.1.1.1 Definition – Kritische Infrastrukturen

Als Kritische Infrastrukturen sind allgemein Versorgungs- und Dienstleistungseinrichtungen zu verstehen, die für das Gemeinwohl wichtig sind und deren Ausfall starke bis katastrophale Auswirkungen auf Staat, Wirtschaft und Gesellschaft zur Folge hätte.

Kritische Infrastrukturen wurden erstmals vom Gesetzgeber in § 17 Absatz 1 Satz 2 Nummer 3 des Zivilschutz- und Katastrophenhilfegesetzes (ZSKG) definiert. Dieses ist durch das Zivilschutzgesetzänderungsgesetz (ZSGÄndG) am 9. April 2009 in Kraft getreten. Als Kritische Infrastrukturen werden demzufolge „Infrastrukturen, bei deren Ausfall die Versorgung der Bevölkerung erheblich beeinträchtigt wird“ bezeichnet.[170]

Das Bundesministerium des Innern definiert Kritische Infrastrukturen als „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“[171] Es ist dabei unerheblich, ob sich die Kritischen Infrastrukturen in privatwirtschaftlicher[172] oder staatlicher Hand befinden.

Ob eine Infrastruktur als „kritisch“ einzustufen ist, hängt vor allem von ihrer Bedeutung für die Gesellschaft sowie den Folgen, die mit ihrer Störung oder ihrem Ausfall verbunden sind, ab. Ein dafür relevantes Kriterium ist die Kritikalität. Diese wird definiert als „relatives Maß für die Bedeutsamkeit einer Infrastruktur in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Versorgungssicherheit der Gesellschaft mit wichtigen

---

http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf?__blob=publicationFile

[170] Greve, Holger: Kritische Infrastrukturen. DuD 12/2009. S. 757.

[171] Bundesministerium des Innern (Hrsg.): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Juni 2009, S. 3. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?__blob=publicationFile

[172] Es wird davon ausgegangen, dass circa 80 Prozent der Kritischen Infrastrukturen privatwirtschaftlich betrieben werden. Siehe dazu: John-Koch, Monika: Strategische Meilensteine – Kritische Infrastrukturen im Blick. Magazin Bevölkerungsschutz des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe. 3. Quartal 2010. S. 2. Online abrufbar unter: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Publ_magazin/bsmag_3_10.pdf?__blob=publicationFile

Gütern und Dienstleistungen hat".[173] Kritikalität kann systemischer und/oder symbolischer Art sein: Sofern eine Infrastruktur „aufgrund ihrer strukturellen, funktionellen und technischen Positionierung im Gesamtsystem der Infrastrukturbereiche von besonders hoher interdependenter Relevanz ist" – zum Beispiel im Bereich der Elektrizitäts- sowie Informations- und Telekommunikationsinfrastrukturen – liegt systemische Kritikalität vor.[174] Eine symbolische Kritikalität besitzt hingegen eine Infrastruktur, deren Zerstörung „aufgrund ihrer kulturellen oder identitätsstiftenden Bedeutung […] eine Gesellschaft emotional erschüttern und psychologisch nachhaltig aus dem Gleichgewicht bringen kann".[175]

Eine Aufteilung der Kritischen Infrastrukturen in Sektoren erfolgte erstmals 1997 durch die Presidential Commission on Critical Infrastructure Protection (PCCIP) in den USA.[176] Auf dieser Grundlage entwickelten sich abhängig von soziopolitischen Faktoren sowie geografischen und historischen Voraussetzungen länderspezifisch unterschiedliche Auffassungen davon, ob ein Sektor als „kritisch" einzustufen ist.[177]

Die seit 2003 in Deutschland auf Bundesebene bestehende Sektoren- und Brancheneinteilung der Kritischen Infrastrukturen wurde im Jahr 2011 von einer Bund-Länder-Arbeitsgruppe überarbeitet. Bund und Länder haben sich erstmals auf eine gemeinsame Sektoreneinteilung festgelegt; die Bundesressorts verständigten sich auf eine einheitliche Untergliederung in Branchen. Die Kritischen Infrastrukturen werden in Deutschland demnach in neun Sektoren und 29 Branchen unterteilt (siehe Tabelle 1).[178] Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) führt im Zeitraum 2009 bis 2012 das Projekt KritisKAT durch, welches „ein allgemein anwendbares Kriterien-Set zur Identifizierung und Bewertung von kritischen Infrastrukturen" zum Ziel hat, wodurch Entscheidungsträgern „eine Priorisierung von Aktivitäten und Maßnahmen im Risikomanagement ermöglicht werden" soll.[179]

---

[173] Ebd., S. 5.

[174] Ebd.

[175] Ebd.

[176] Vgl. Brunner, Elgin/ Suter, Manuel: International CIIP Handbook 2008/2009. 2008, S. 36.

[177] Vgl. ebd., S. 36, S. 529.

[178] Vgl. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe/Bundesamt für Sicherheit in der Informationstechnik: Sektoren und Branchen Kritischer Infrastrukturen. 2011. Online abrufbar unter: http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html

[179] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: Projekt KritisKAT. Online abrufbar unter: http://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/Projekte/KritisKat/kritiskat_node.html

Sektoren	Branchen
Energie	– Elektrizität – Gas – Mineralöl
Informationstechnik und Telekommunikation	– Telekommunikation – Informationstechnik
Transport und Verkehr	– Luftfahrt – Seeschifffahrt – Binnenschifffahrt – Schienenverkehr – Straßenverkehr – Logistik
Gesundheit	– Medizinische Versorgung – Arzneimittel und Impfstoffe – Labore
Wasser	– Öffentliche Wasserversorung – Öffentliche Abwasserbeseitigung
Ernährung	– Ernährungswirtschaft – Lebensmittelhandel
Finanz- und Versicherungswesen	– Banken – Börsen – Versicherungen – Finanzdienstleister
Staat und Verwaltung	– Regierung und Verwaltung – Parlament – Justizeinrichtungen – Notfall-/ Rettungswesen einschließlich Katastrophenschutz
Medien und Kultur	– Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse – Kulturgut – symbolträchtige Bauwerke

Tabelle 1: Sektoren- und Brancheneinteilung Kritischer Infrastrukturen[180]

Vergleich Kritischer Infrastrukturen Deutschland – USA

Basierend auf der amerikanischen Definition Kritischer Infrastrukturen als „systems and assets, whether physical or virtual, so vital to the United States that the incapacity or

[180] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe/Bundesamt für Sicherheit in der Informationstechnik: Sektoren und Branchen Kritischer Infrastrukturen. 2011. Online abrufbar unter: http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html

destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"[181], zählen die USA insgesamt 18 Sektoren zu den Kritischen Infrastrukturen. Diese stimmen größtenteils mit den in Deutschland identifizierten Sektoren überein. Es werden aber auch die Rüstungsindustrie sowie Teile des produzierenden Gewerbes, beispielsweise die Kraftfahrzeugindustrie und die Metall verarbeitende Industrie, genannt.[182] Zusätzlich zu den inländischen Kritischen Infrastrukturen betrachten die USA auch solche, die sich außerhalb ihrer Landesgrenzen befinden, da deren Ausfall trotz der geografischen Entfernung Auswirkungen auf die amerikanische Sicherheit oder Wirtschaft haben könnte. So werden in einem von Wikileaks veröffentlichten internen Dokument diverse internationale Einrichtungen und Infrastrukturen aufgelistet, beispielsweise internationale Seekabel für die Internet- und Telekommunikation, Häfen, Staudämme, besondere Produktionsstätten, Hersteller von Chemie- und Pharmaprodukten aber auch Ressourcen wie seltene Erden.[183]

II.1.1.1.2 Beispiele für die wachsende IT-Durchdringung der Kritischen Infrastrukturen

Kritische Infrastrukturen sind zunehmend mehr von IT-Infrastrukturen abhängig.

Vor allem zur Überwachung, Steuerung und Automatisierung von Prozessen im industriellen Bereich werden industrielle Kontrollsysteme (Industrial Control Systems, ICS) – insbesondere Supervisory Control And Data Acquisition(SCADA)-Systeme – eingesetzt. Diese „enthalten heute immer mehr Bestandteile, die auf ‚Standardinformationstechnik' basieren" und werden „immer häufiger mit gängiger Netzwerktechnik und unter Verwendung standardisierter Kommunikationsprotokolle wie Ethernet und TCP/IP" vernetzt.[184] Damit

---

[181] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Public Law 107-56, Section 1016(e). 26. Oktober 2001.

[182] Vgl. die Einteilung auf der Website des Department of Homeland Security: Critical Infrastructure. Online abrufbar unter: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

[183] Vgl. beispielsweise Lister, Tim: WikiLeaks lists sites key to U.S. security. 7. Dezember 2010. Online abrufbar unter: http://edition.cnn.com/2010/US/12/06/wikileaks/index.html und Zetter, Kim: Wikileaks releases secret list of critical infrastructure sites. 6. Dezember 2010. Online abrufbar unter: http://www.wired.com/threatlevel/2010/12/critical-infrastructures-cable/ sowie Schulzki-Haddouti, Christiane: Eierlauf – Kritische Infrastrukturen neu betrachtet. In: c't. Heft 4, 2011, S. 68 ff.

[184] Bundesamt für Sicherheit in der Informationstechnik: Informationstechnik in der Prozessüberwachung und -steuerung. 2008, S. 3. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/IT_in_der_Prozesssteuerung_pdf.pdf?__blob=publicationFile

solche IT-Systeme zum Beispiel aus der Ferne gewartet werden können, werden sie mit dem Internet vernetzt.

Beispielsweise erfolgt in der Energieversorgung die Steuerung und Regelung von Energieanlagen über IT-Systeme. Die Wasserversorgung und -entsorgung läuft computergestützt ab. In der Nahrungsmittelindustrie setzen Lebensmittelhersteller IT-Lösungen zur Steuerung ihrer Produktionsprozesse ein.

Aber auch im Dienstleistungssektor spielt der IT-Einsatz eine wesentliche Rolle. Im Finanzwesen werden IT-Infrastrukturen zur Abwicklung des bargeldlosen Zahlungsverkehrs benötigt. Im Transport- und Verkehrswesen werden IT-Systeme zur Automatisierung des Straßen- und Schienenverkehrs genutzt. In Krankenhäusern finden IT-Lösungen beim Patientenmanagement mit der elektronischen Patientenakte Anwendung.

Dies sind nur einige von vielen Einsatzgebieten, die die Bedeutung der IT-Infrastrukturen für die Kritischen Infrastrukturen aufzeigen. Es wird deutlich, dass der Ausfall der IT-Infrastrukturen aufgrund der bestehenden Interdependenzen, das heißt der Abhängigkeiten zwischen Sektoren, einen Dominoeffekt auslösen kann: Störungen der IT-Systeme können zu Problemen in einem anderen Bereich führen.[185] Dabei können die daraus resultierenden Folgen weitaus größer sein als der ursprüngliche Ausfall (so genannter Kaskadeneffekt).[186]

Die weltweit voranschreitende Einführung des Internetprotokolls in der Version 6 (IPv6)[187] sowie Entwicklungen wie das Internet der Dinge oder intelligente Stromnetze (englisch: Smart Grid) zeigen, dass die Vernetzung weiter zunehmen wird. Mit dieser wachsenden IT-Abhängigkeit geht die „steigende Notwendigkeit, Kritische Infrastrukturen vor Cyberangriffen zu schützen“, einher.[188]

---

[185] Vgl. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe/Bundesamt für Sicherheit in der Informationstechnik: Sektoren und Branchen Kritischer Infrastrukturen. 2011. Online abrufbar unter: http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Gefahren/Gefahren_node.html

[186] Vgl. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe/Bundesamt für Sicherheit in der Informationstechnik: Sektoren und Branchen Kritischer Infrastrukturen. 2011. Online abrufbar unter: http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Gefahren/Gefahren_node.html

[187] Siehe zum Thema Sicherheitsaspekte bei der Einführung des neuen Internetprotokolls Version 6 den Exkurs in Kapitel I.2.2.2.

[188] Helmbrecht, Udo: Die aktuelle Bedrohungslage durch Ausfall von IT-Infrastruktur.2010, S. 42.

II.1.2 Bedrohungen Kritischer Infrastrukturen/Informationsinfrastrukturen

Kritische Infrastrukturen/Informationsinfrastrukturen sind vielfältigen Bedrohungen ausgesetzt, wobei eine Bedrohung allgemein definiert wird als „ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen.“[189]

Vor dem Hintergrund der Themenstellung der Enquete-Kommission Internet und digitale Gesellschaft konzentrieren sich die folgenden Ausführungen auf den Bereich der vorsätzlichen Handlungen, speziell der so genannten IT-Angriffe.[190]

Ein IT-Angriff richtet sich gegen einen oder mehrere andere IT-Systeme und zielt darauf ab, die IT-Sicherheit ganz oder teilweise hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit zu überwinden.[191]

Im Rahmen der *Cyber-Sicherheitsstrategie für Deutschland*[192] wird der Cyber-Raum definiert als „der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab. Dem Cyber-Raum liegt als universelles und öffentlich zugängliches Verbindungs- und Transportnetz das Internet zugrunde, welches durch beliebige andere Datennetze ergänzt und erweitert werden kann.“ [193] Dieser kann dabei „als primärer Angriffsweg benutzt [werden]

---

[189] BSI: Glossar – IT-Grundschutz-Kataloge. Online abrufbar unter: https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

[190] Sonstige Gefährdungspotenziale wurden bereits an anderer Stelle durch den Deutschen Bundestag eingehend betrachtet. Siehe beispielsweise: http://www.bundestag.de/bundestag/ausschuesse17/a18/anhoerungen/Stromausfall/41-1105251.pdf

[191] BMI: Cyber-Sicherheitsstrategie für Deutschland. S. 14. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile

[192] Siehe Kapitel II.2.3.3.2.

[193] BMI: Cyber-Sicherheitsstrategie für Deutschland. Februar 2011. S. 14. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile

oder selbst das Ziel eines Angriffs [sein].“[194] Informationsinfrastrukturen kommt somit eine Besonderheit zuteil: sie sind einerseits Begehungsmittel, andererseits Angriffsobjekt.

IT-Angriffe können sowohl gezielt, dass heißt auf ein zuvor bestimmtes Objekt, als auch ungezielt erfolgen. Bei gezielten Angriffen besteht die Gefahr von Irrläufern. Welche Angriffsart ein Täter wählt, hängt vom Motiv[195] des Angriffs ab.[196] Angriffsziele können Daten beziehungsweise Informationen, IT-Systeme oder IT-Dienste sein.[197] Einen Überblick über konkrete Bedrohungen und Angriffsmittel, die dem Bereich der IT-Angriffe zuzuordnen sind, liefern die Kapitel II.3.1.5, II.4.4 sowie II.5.4.

Laut IT-Lagezentrums des BSI zeigt sich die aktuelle Bedrohungslage im Oktober 2012 wie folgt:

- „Etwa alle zwei Sekunden erscheint ein neues Schadprogramm oder eine neue Variante.
- Pro Minute werden etwa zwei digitale Identitäten in Deutschland gestohlen.
- Pro Tag werden etwa vier bis fünf gezielte Trojaner-E-Mails im Regierungsnetz detektiert.
- Pro Monat werden etwa 40.000 Zugriffsversuche aus dem Regierungsnetz auf schädliche Webseiten blockiert.“[198]

Studien weisen darauf hin, dass die Bedrohung durch IT-Angriffe auf Kritische Infrastrukturen beziehungsweise deren Informationsinfrastrukturen in den nächsten Jahren weltweit zunehmen wird: Dies zeigt u. a. die 2010 gemeinsam vom Center for Strategic and International Studies (CSIS) und dem Unternehmen McAfee veröffentlichte Studie *In the Crossfire*[199], an der 600 IT-Führungskräfte von Unternehmen Kritischer Infrastrukturen aus

---

[194] BSI: Sensibilisierung: Cyber-Bedrohung – ein Einstieg. Häufig gestellte Fragen und Antworten. 15.10.2012. S. 1. Online abrufbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/sensibilisierung/BSI-CS_012.pdf?__blob=publicationFile

[195] Zu den möglichen Motiven siehe Kapitel II.3.1.4.

[196] Vgl. BSI: Grundlagen: Register aktueller Cyber-Gefährdungen und –Angriffsformen. Anhang B – Angriffsinitiierung. S. 6. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/BSI-A-CS_001.pdf?__blob=publicationFile

[197] Diese können weiter unterteilt werden. Siehe: BSI: Grundlagen: Register aktueller Cyber-Gefährdungen und –Angriffsformen. Anhang B – Angriffsinitiierung. S. 1ff. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/BSI-A-CS_001.pdf?__blob=publicationFile

[198] BSI: Sensibilisierung: Cyber-Bedrohung – ein Einstieg. Häufig gestellte Fragen und Antworten. 15.10.2012. S. 5. Online abrufbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/sensibilisierung/BSI-CS_012.pdf?__blob=publicationFile

[199] Vgl. CSIS/McAfee: In the Crossfire. Critical Infrastructure in the Age of Cyber War.2009. Online abrufbar unter: http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf

14 Staaten teilgenommen haben. Die Folgestudie *In the Dark*[200] aus dem Jahr 2011 – herausgegeben nach dem Bekanntwerden des Computerwurms Stuxnet – bestätigt einen Anstieg an Bedrohungen. Auch die *Symantec 2010 Critical Infrastructure Protection Study*[201] kommt zu diesem Ergebnis. Eine Vielzahl der Befragten vermutet, dass die IT-Attacken auf ihre Infrastrukturen von anderen Staaten ausgingen beziehungsweise politisch motiviert waren.[202]

Die Studien zeigen, dass sich die Unternehmen der Gefahr eines IT-Angriffes bewusst sind. Dennoch fühlten sich 2010 nur ein Drittel der Betreiber Kritischer Infrastrukturen äußerst vorbereitet („extremely prepared"), ein weiteres Drittel der Befragten fühlte sich dagegen weniger als einigermaßen vorbereitet („less then somewhat prepared").[203] Hinsichtlich des Schutzes vor IT-Angriffen gibt es folglich noch Raum für die Verbesserung („room for readiness improvement").[204] Dies legt auch die erste CSIS/McAfee-Studie nahe.[205] Die Folgestudie zeigt, dass es innerhalb eines Jahres nur mäßige sicherheitsbezogene Verbesserungen („only modest improvements in security") gegeben hat[206].

Der ENISA-Bericht *Protecting Industrial Control Systems. Recommendations for Europe and Member States*[207] von 2011 stellt fest, dass Kritische Infrastrukturen noch immer nicht ausreichend auf IT-Angriffe wie DuQu vorbereitet seien. Insbesondere fehle es in Europa an spezifischen Initiativen und Richtlinien um die IT-Sicherheit von Industrial-Control-Systems

---

[200] Vgl. CSIS/McAfee: In the Dark. 2011. Online abrufbar unter: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf Siehe hierzu auch: Computerworld: Timeline: Critical infrastructure attacks increase steadily in past decade. 5. November 2012. Online abrufbar unter: http://www.computerworld.com/s/article/9233173/Timeline_Critical_infrastructure_attacks_increase_steadily_in_past_decade

[201] Vgl. Symantec 2010 Critical Infrastructure Protection Study. Oktober 2010. Online abrufbar unter: http://www.symantec.com/content/en/us/about/presskits/Symantec_2010_CIP_Study_Global_Data.pdf

[202] Vgl. CSIS/McAfee: In the Crossfire. Critical Infrastructure in the Age of Cyber War.2009. S. 4. Online abrufbar unter: http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf; Symantec 2010 Critical Infrastructure Protection Study. Oktober 2010. S. 5. Online abrufbar unter: http://www.symantec.com/content/en/us/about/presskits/Symantec_2010_CIP_Study_Global_Data.pdf; Vgl. CSIS/McAfee: In the Dark. 2011. S. 20. Online abrufbar unter: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf

[203] Symantec 2010 Critical Infrastructure Protection Study. Oktober 2010. S. 7. Online abrufbar unter: http://www.symantec.com/content/en/us/about/presskits/Symantec_2010_CIP_Study_Global_Data.pdf

[204] Symantec 2010 Critical Infrastructure Protection Study. Oktober 2010. S. 7. Online abrufbar unter: http://www.symantec.com/content/en/us/about/presskits/Symantec_2010_CIP_Study_Global_Data.pdf

[205] CSIS/McAfee: In the Crossfire. Critical Infrastructure in the Age of Cyber War.2009. S. 32ff. Online abrufbar unter: http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf

[206] CSIS/McAfee: In the Dark. 2011. S. 1. Online abrufbar unter: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf

[207] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states/at_download/fullReport

(ICS) zu adressieren. Es gebe keine allgemein angewandten Sicherheitsstandards, Leitlinien oder Regelungen für derartige Systeme, die Unternehmensleitung sei nicht ausreichend involviert und es gebe zahlreiche technische Schwachstellen.[208]

In einem Interview zum Thema Schutz Kritischer Infrastrukturen teilte ein Mitarbeiter des BSI mit, dass „gerade die letztjährige Lükex-Übung zum Schutz vor Cyberangriffen […] gezeigt [hat], dass Deutschland grundsätzlich gut aufgestellt ist". Jedoch sind „einige Branchen innerhalb der kritischen Infrastrukturen besser aufgestellt […] als andere. Dort, wo es noch nicht so funktioniert, fehlt es an branchenweiten Standards oder an der Zusammenarbeit zwischen den Unternehmen, was den Austausch aktueller Informationen angeht. Innerhalb des Umsetzungsplanes KRITIS können verschiedene Branchen durchaus noch voneinander lernen."[209]

Einer repräsentativen Umfrage unter 800 Unternehmen unterschiedlicher Branchen und Unternehmensgrößen zufolge, hat „fast jedes zweite Unternehmen (45 Prozent) […] nicht einmal einen Notfallplan für IT-Sicherheitsvorfälle."[210]

Das BSI hat eine *Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen*[211] mit dem Ziel „den Ist-Zustand des IT-Sicherheits- und Krisenmanagements sowie der Sicherheit kritischer IT-Infrastrukturen im Bereich der kleinen und mittleren Unternehmen zu ermitteln"[212], durchgeführt. Demnach „sind die KMU bei Wertung der umgesetzten IT-Sicherheitsmaßnahmen grundsätzlich geeignet aufgestellt", durchschnittlich werden „rund zwei Drittel der in Anlehnung an den IT-Grundschutz abgefragten IT-Sicherheitsmaßnahmen in den Unternehmen umgesetzt".[213] Verbesserungsbedarf gibt es „vor allem noch im Bereich

---

[208] Der englische Originaltext lautet „Critical infrastructures are still not sufficiently prepared for attacks like DuQu. In particular, Europe lacks specific initiatives and policies to address ICS security. There are no commonly adopted ICS security standards, guidelines or regulations, corporate management is not sufficiently involved, and there are numerous technical vulnerabilities." https://www.enisa.europa.eu/media/news-items/duqu-analysis

[209] http://www.computerwoche.de/a/deutschland-nimmt-eine-vorreiterrolle-ein,2528104

[210] BITKOM: Presseinformation. Jede zweite Firma hat keinen Notfallplan für IT-Sicherheitsvorfälle. 7. März 2012.

[211] BSI: Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. Grad der Sensibilisierung des Mittelstandes in Deutschland. 2011. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile

[212] https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.html

[213] BSI: Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. Grad der Sensibilisierung des Mittelstandes in Deutschland. 2011. S. 98, 8. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile

der *geschäftskritischen IT-Sicherheitsprozesse*, das heißt, dem Umgang mit *Sicherheitsvorfällen*, dem *Notfallmanagement* und der *Bewertung der Gefahrenbereiche*“.[214]

Neben Unternehmen sind auch Behörden, welche auch zu den Kritischen Infrastrukturen zählen, Ziel von IT-Angriffen: „Nach Erkenntnissen des Bundesamtes für Sicherheit in der Informationstechnik werden durchschnittlich fünf gezielte Angriffe täglich auf Personen als Nutzer des Regierungsnetzes detektiert und abgewehrt.“[215] Das BSI ist laut § 3 des Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSIG) zuständig für die „Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes“.

Auch der Deutsche Bundestag sieht sich IT-Angriffen (insbesondere aus dem Internet) unterschiedlicher Intensität ausgesetzt. Dank umfangreicher technischer und organisatorischer IT-Sicherheitsmaßnahmen (zum Beispiel der Umsetzung des IT-Grundschutzes), sowie engem Kontakt zum Bundesamt für Sicherheit in der Informationstechnik haben die Auswirkungen eines Angriffes auf den Deutschen Bundestag weder zu größeren Ausfällen von IT-Systemen, noch zum ungewollten Abfluss von Daten geführt.

Die Europäischen Kommission fasst die unterschiedlichen Bedrohungen, denen Informationsinfrastrukturen ausgesetzt sind, in drei Kategorien zusammen:[216]

Kriminelle Ausnutzung

Die kriminelle Ausnutzung des Internets erfolgt u. a. durch gezielte, komplexe und anhaltende IT-Angriffe durch hoch qualifizierte Täter zur Begehung wirtschaftlicher- oder politischer Spionage. Diese so genannten Advanced Persistent Threats (APT) können zum Beispiel durch eine gezielt an eine Person gerichtete E-Mail (so genanntes Spear Phishing, siehe auch Kapitel II.3.1.7.2) oder durch Sicherheitslücken in Software (siehe auch Kapitel II.3.1.7.1) ausgelöst werden. Ziel ist, einen Rechner mit einer Schadsoftware zu infizieren, um Zugang

---

[214] BSI: Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. Grad der Sensibilisierung des Mittelstandes in Deutschland. 2011. S. 99. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile

[215] BT-Drucksache 17/5677. 29.04.2011. S. 4. Online abrufbar unter: http://dipbt.bundestag.de/dip21/btd/17/056/1705677.pdf. Siehe auch BSI: Die Lage der IT-Sicherheit in Deutschland 2011. S. 26. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile

[216] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen „Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit”. KOM(2011) 163 endgültig. 31. März 2011. Online abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:DE:PDF

zu einem Netzwerk zu erlangen. Bei einer Infiltration durch ein APT kann ein Angreifer über einen langen Zeitraum unbemerkt Informationen ausspionieren. Es kann davon ausgegangen werden, dass nur wenige solcher Angriffe bekannt werden, um Wirtschaft und Staat zu schützen.

Beispiele:

a) Das staatliche IT-System des französischen Finanzministeriums ist von Dezember 2010 bis März 2011 Opfer eines APTs gewesen. Die Angreifer infizierten bei der Attacke circa 150 Computer des Ministeriums mit Trojanern (siehe Kapitel II.3.1.6.1.3), die es erlauben, auf fremde Rechner zuzugreifen beziehungsweise diese auszuspionieren. Bei dem Angriff wurden zahlreiche Daten ausgespäht, Informationen über einzelne Personen waren aber nicht betroffen. Die Angreifer hatten es auf Dokumente abgesehen, die im Zusammenhang mit der G20 stehen, der Frankreich zu dem Zeitpunkt vorsaß.[217]

b) Die EU-Kommission musste Anfang 2011 nach Angriffen auf mehreren nationale Emissionshandelsstellen den Handel mit Emissionsrechten unterbrechen.[218] Bei diesen Vorfällen war es den Angreifern u. a. gelungen, europäische Emissionsrechte im Wert von etwa 6,7 Millionen Euro aus dem Handelsregister in Tschechien auszuspähen.[219] Schon Anfang 2010 haben Angreifer Verschmutzungsrechte entwendet. Davon allein in Deutschland in Höhe von drei Millionen Euro.[220]

Die Kapitel II.3 sowie II.4 befassen sich ausführlich mit den Themen Kriminalität im Internet und Spionage.

Störung/Sabotage

Seit mehreren Jahren ist ein Trend festzustellen, dass mit Schadsoftware infizierte Computer zu einem so genannten Botnetz zusammengeschlossen werden (siehe auch Kapitel II.3.1.5.1).[221] Rechner, die Teil eines Botnetzes sind, können unbemerkt von den Betreibern des Botnetzes ferngesteuert werden. So können sie von kriminell agierenden Gruppen

---

[217] Vgl. http://www.spiegel.de/netzwelt/web/frankreich-hacker-attackierten-finanzministerium-a-749421.html

[218] Vgl. http://europa.eu/rapid/press-release_MEMO-11-34_en.htm?locale=fr

[219] Vgl. http://www.euractiv.de/222/artikel/eu-emissionshandel-nach-hacker-angriff-gestoppt-004245

[220] Vgl. http://www.euractiv.de/energie-und-klimaschutz/artikel/datendiebstahl-bei-emissionshandlern-002683

[221] Vgl. BSI: Die Lage der IT-Sicherheit in Deutschland 2011. S. 7. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile

beispielsweise zum Versenden von Spam oder zum Ausführen eines Distributed Denial of Service-Angriffes (DDoS-Angriffs) missbraucht werden. Ein Denial of Service-Angriff (DoS-Angriff) führt zur Überlastung einer IT-Infrastruktur durch einen Angriff auf einen Server. Geht ein solcher Angriff koordiniert von mehreren Systemen aus, spricht man von einem Distributed Denial of Service-Angriffe (DDoS-Angriff).

Botnetze stellen eine zentrale Bedrohung dar, wie die folgenden Beispiele zeigen:

a) Im Frühjahr 2009 verursachte die Schadsoftware Conficker erhebliche Beeinträchtigungen bei Banken, Krankenhäusern und Streitkräften verschiedener Länder.[222] Conficker baut ein Botnetz auf. Die infizierten Rechner sollen durch einen oder mehrere Command-and-Control-Server zu koordiniertem Handeln gebracht werden, um so gespeicherte Daten und insbesondere Passwörter auszuspähen und über das Internet zu transferieren.[223] Anfang des Jahres 2009 legte Conficker beispielsweise circa 3 000 Computer des Amtes der Kärntner Landesregierung in Österreich lahm.[224] Heute gibt es immer noch Millionen Computer die mit Conficker infiziert sind. Laut einer Studie von Microsoft ist Conficker noch immer eine der größten Bedrohungen für Unternehmensnetzwerke.[225]

b) Im Juli 2010 wurde der Computerwurm[226] Stuxnet entdeckt. Stuxnet ist ein qualitativer Wendepunkt in der IT-Sicherheitsgeschichte. Laut BSI muss seitdem das Risiko für Kritische Infrastrukturen und ihre Prozesssteuerungssysteme neu bewertet werden.[227] Stuxnet wurde für gezielte Angriffe auf SCADA-Systeme[228] mit dem Ziel der Sabotage von Industrieanlagen entwickelt.[229] Angriffe wie der durch Stuxnet zeigen eine veränderte Angriffsqualität, da die Entwicklung von Stuxnet nur mit erheblichem Know-how und finanziellem Aufwand möglich gewesen sein soll.[230] Laut Studien werden 80 Prozent der bekannt gewordenen Angriffe durch eigene Mitarbeiter

---

[222] Vgl. den Abschnitt Auswirkungen bei http://de.wikipedia.org/wiki/Conficker

[223] Vgl. Prof. Dr. Peter Martini, RFW Universität Bonn am 15.11.2011 auf dem Forum „Cyber Defence“ in Bonn.

[224] Vgl. http://www.heise.de/security/meldung/Conficker-schlaegt-bei-Kaerntner-Regierung-zu-195496.html

[225] Vgl. http://www.microsoft.com/germany/newsroom/pressemitteilung.mspx?id=533537

[226] Siehe hierzu auch Kapitel II.3.1.6.1.2.

[227] Vgl. BSI: Die Lage der IT-Sicherheit in Deutschland 2011. S. 29. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile Siehe auch Kapitel II.5.4.1.

[228] Siehe hierzu auch Kapitel II.2.1.1.2.

[229] Vgl. Bevölkerungsschutz. Cyber-Sicherheit, 4/2011. Hg: BBK, S.4.

[230] Vgl. beispielsweise http://www.symantec.com/de/de/theme.jsp?themeid=stuxnet

von Unternehmen und Behörden durchgeführt.[231] Stuxnet zeigt die Bedeutung des Faktors Mensch beziehungsweise die Gefahr von Innentätern deutlich auf, da die Schadsoftware mittels USB-Stick eingeschleust wurde.

c) Im Oktober 2011 wurde der Computerwurm Duqu entdeckt, der als Nachfolger von Stuxnet gilt und einen Teil dessen Quellcode enthält. DuQu ist ein Trojaner, der gezielt eingesetzt wird, um Daten von Unternehmen, die an der Entwicklung von Software für Industrieanlagen beteiligt sind, zu erhalten.[232]

Durch das immer weiter ansteigende Technologieniveau wird sich die Steuerung der Botnetze in der Zukunft verstärkt über Peer-to-Peer-Netzwerke, wie beispielsweise im Falle des Miner-Botnetzes, abspielen und nicht mehr durch wenige zentrale Command-and-Control-Server. Werden diese vom Netz genommen, kann das Botnetz nicht mehr gesteuert werden. Durch die dezentralisierte Struktur wird die Auflösung eines Botznetzes jedoch erschwert.[233]

Das Kapitel II.5 befasst sich ausführlich mit dem Thema Sabotage.

Zerstörung

Eine Zerstörung stellt eine realistische Gefahr dar, wenngleich sie bisher selten verwirklicht wurde. Der Stuxnet-Computerwurm hat die Zerstörung von Uran-Zentrifugen verursacht.[234] Auch im Labor wurde die Zerstörung von Kritischer Infrastruktur unter realistischen Bedingungen bereits verwirklicht.[235] Durch die immer stärkere Durchdringung Kritischer Infrastrukturen mit IT ist die Gefahr einer Zerstörung möglich, insbesondere für Systeme wie intelligente Netze (Smart Grids).

Aufgrund der steigenden Komplexität von IT-Systemen, werden diese auch immer anfälliger für die oben genannten Bedrohungen. Der amerikanische Sicherheitsexperte Bruce Schneier

---

[231] „IT-Sicherheit: Konzepte - Verfahren – Protokolle“, Claudia Eckert, 2009, Seite XX

[232] Vgl. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf ; http://www.zeit.de/digital/internet/2011-10/computerwurm-duqu-stuxnet

[233] Vgl. Computerwoche: Im Kampf gegen Botnetze. 9. November 2011. Online abrufbar unter: http://www.computerwoche.de/a/im-kampf-gege-botnetze,2368581,5;

[234] Vgl. http://isis-online.org/upload/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf ; http://www.spiegel.de/netzwelt/netzpolitik/angriff-auf-irans-atomprogramm-stuxnet-virus-koennte-tausend-uran-zentrifugen-zerstoert-habe-a-736604-html

[235] Das Department of Homeland Security hat im Rahmen eines Versuchs unter dem Codenamen „Aurora“ im Idaho National Laboratory einen Stromgenerator dazu gebracht, sich selbst zu zerstören, in dem über die Maschinensteuerung ein Notabschaltungsmodul manipuliert wurde.

erklärte bereits 2003, dass komplexe Systeme u. a. mehr Codezeilen hätten und dadurch auch mehr Sicherheitslücken enthielten. Zudem seien komplexe Systeme mühsamer zu testen und enthielten daher eher ungetestete Programmteile. In Bezug auf Sicherheit sei es komplizierter solche Systeme zu modellieren, zu implementieren, zu konfigurieren und zu nutzen. Darüber hinaus seien sie für den Anwender schwerer zu verstehen. Komplexität führe zu schwächerer Sicherheit. Er fasst dies damit zusammen, dass mit der steigenden Komplexität von Computern und Netzwerken automatisch eine sinkende Sicherheit einhergehe.[236] In einem Interview aus dem Jahr 2012 betonte Bruce Schneier erneut, dass Komplexität der größte Feind der Sicherheit sei („Complexity is the worst enemy of security“).[237]

II.1.3 Vorhandene Regelungen und Maßnahmen zum Schutz kritischer Infrastrukturen beziehungsweise Informationsinfrastrukturen

Aufgezeigt werden im Folgenden die Aktivitäten zum Schutz Kritischer Infrastrukturen und Kritischer Informationsinfrastrukturen auf internationaler, europäischer und nationaler Ebene, wobei es sich nur um eine exemplarische Übersicht ohne den Anspruch auf Vollständigkeit handeln kann.

II.1.3.1 Aktivitäten auf internationaler Ebene

In der heutigen immer stärker vernetzten Welt muss jeder Staat den Schutz seiner Infrastrukturen beständig überprüfen und verbessern. Die Vernetzung ist dabei nicht national begrenzt, sondern länderübergreifend. Auch Katastrophen sind oft länderübergreifend, so dass internationale Kooperationen beim Schutz Kritischer Infrastrukturen und Kritischer Informationsinfrastrukturen erforderlich sind.

Man kann die bisherigen nationalen Ansätze der Staaten in zwei Kategorien einteilen:

---

[236] Siehe hierzu die Ausführungen von Bruce Schneier , S. 11. 22. Juni 2003. http://www.gpo.gov/fdsys/pkg/CHRG-108hhrg98312/pdf/CHRG-108hhrg98312.pdf ; http://www.gpo.gov/fdsys/search/pagedetails.action?st=Crypto&granuleId=CHRG-108hhrg98312&packageId=CHRG-108hhrg98312&bread=true
Die englische Originalfassung lautet: „Complex systems have more lines of code and therefore more security bugs. Complex systems have more interactions and therefore more potential for insecurities. Compley systems are harder to test and therefore more likely to have untestetd portions. Complex systems are harder to design securely, implement seucrely, configure securely, and use securely. Compley systems are harder for users to understand. Everything about complexity leads towards lower security. As our computers and networks become more complex, they inherently become less secure.“.

[237] www.computerworld.com/s/article/9234815/Complexity_the_worst_enemy_of_security

1. Critical Information Infrastructure Protection (CIIP): Dieser Ansatz bezieht sich ausschließlich auf die Sicherheit und die Sicherung von IT-Verbindungen und IT-Lösungen innerhalb und zwischen den einzelnen Infrastruktursektoren, wobei der Schutz der physischen Komponenten separat sichergestellt wird. Dieser Ansatz lässt sich mit dem Terminus IT-KRITIS umschreiben.
2. All-hazards-Ansatz: Auch die physischen Komponenten sind Teil des nationalen Zivilschutzmodells. Deshalb umfasst der zweite Ansatz sowohl den Schutz der IT-KRITIS als auch den physischen Schutz. Die zentralen Koordinations- und Strategieorgane sind zugleich Kompetenzzentren für IT-Sicherheit, Zivil- und Katastrophenschutz.[238]

Auf europäischer Ebene ist das *Europäische Programm für den Schutz der Kritischen Infrastrukturen (EPSKI)*[239] Grundlage der derzeitigen Aktivitäten.[240] Zu benennen ist beispielsweise der Aktionsplan zum Schutz Kritischer Informationsinfrastrukturen (CIIP-Aktionsplan), der im Rahmen einer Mitteilung der Kommission mit dem Titel *Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität* am 30. März 2009 veröffentlicht wurde.[241] Im Rahmen des CIIP-Aktionsplans gibt es „eine beginnende Kooperation zwischen Behörden der EU-Mitgliedstaaten, die sich um den Schutz von kritischen Informationsinfrastrukturen kümmern, und privatwirtschaftlichen Unternehmen, die kritische Informationsinfrastrukturen betreiben oder unterstützen“.[242]

Im Rahmen der internationalen Zusammenarbeit unterstützt Deutschland alle Bemühungen und Maßnahmen, grenzüberschreitende Kritische Infrastrukturen zu erkennen und deren Verletzlichkeit zu minimieren. Es werden auch bilaterale Kooperationen zum Informationsaustausch gefördert und Maßnahmen zum Schutz Kritischer Infrastrukturen aufeinander abgestimmt. Wichtige internationale Partner und Kooperationen sind

---

[238] Vgl. zu IT-KRITIS und zum All-hazards-Ansatz ausführlich Bundesamt für Sicherheit in der Informationstechnik: Internationale Aktivitäten zum Schutz Kritischer Infrastrukturen, S. 2f.; In einem dritten "Sonderfall" gibt es "keine Kooperationen zwischen öffentlichem und privatem Sektor" ("chinesisches Modell") (ebda.). Online abrufbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/476704/publicationFile/30898/Artikel_Internationales_2004_2008_pdf.pdf (Stand: 21.08.2012)

[239] Abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:DE:PDF

[240] Abrufbar unter: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_de.htm (Stand: 21.08.2012)

[241] Abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:DE:PDF (Stand: 21.08.2012)

[242] http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Internationales/internationales_node.html (Stand: 21.08.2012)

insbesondere die unmittelbar angrenzenden Nachbarstaaten, die Europäische Union, die G8-Staaten, die G20-Staaten und die NATO.[243]

Seit den Anschlägen des 11. September 2001 hat die NATO ihre Bemühungen zur Terrorismusbekämpfung verstärkt, da auch Terrorakte zu den Gefahren für die Sicherheit des Bündnisses gehören. Wichtig ist in diesem Zusammenhang das 2004 gegründete Programm *Defence against Terrorism Program of Work*[244] *(DAT POW)*. Mit diesem Programm werden Projekte in zehn Bereichen unterstützt, in denen mittels neuartiger und innovativer Technologien terroristische Aktivitäten bekämpft oder zumindest die Folgen von terroristischen Anschlägen gemildert werden können. Dazu zählt auch der Schutz Kritischer Infrastrukturen.[245] Mit der *NATO Policy on Cyber Defence* hat sich die NATO durch die Beschlüsse des Lissabon-Gipfels ein Programm zur Sicherstellung der eigenen Netzwerke und der der Mitgliedsstaaten in Zusammenarbeit mit allen Akteuren auferlegt.[246]

Das 2006 gegründete UN Internet Governance Forum (IGF)[247] bietet die Möglichkeit das Thema auf internationaler Ebene und in einer Multi-Stakeholder-Umgebung zu besprechen. Aufgabe des IGF ist u. a. „to discuss public policy issues related to key elements of Internet Governance in order to foster the sustainability, robustness, security, stability an development of the Internet“ und „to discuss, inter alia, issues relating to critical Internet resources“.[248]

---

[243] Vgl. BMI, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), S. 18, abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?__blob=publicationFile (Stand: 21.08.2012)

[244] Vgl. http://www.nato.int/cps/en/natolive/topics_50313.htm (Stand: 21.08.2012)

[245] Vgl. http://www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/TerrorismusOK/TerrorismusbekaempfungNATO_node.htm l (Stand: 26.08.2012)

[246] Vgl. http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf
Siehe hierzu auch die Ausführungen auf: http://www.nato.int/cps/en/natolive/topics_78170.htm. Siehe auch die beiden UN Resolutionen 57/239 (2002): Creation of a global culture of cybersecurity, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf und 58/199 (2004): Creation of a global culture of cybersecurity and the protection of critical information infrastructures, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf. Auch die OECD setzt sich mit dem Thema Schutz Kritischer Informationsinfrastrukturen auseinander, siehe OECD Recommendation on the Council on the Protection of Critical Information Infrastructure, http://www.oecd.org/sti/40825404.pdf.

[247] Siehe unter: http://www.intgovforum.org

[248] http://www.itu.int/wsis/docs2/tunis/off/6rev1.html, Nr. 72. Siehe hierzu ausführlich den Bericht der Projektgruppe Internationales und Internet Governance.

II.1.3.2 Aktivitäten auf europäischer Ebene

II.1.3.2.1 Initiativen der Europäischen Union (EU)

Im Jahr 2004 hat der Europäische Rat die EU-Kommission beauftragt eine Gesamtstrategie zur Verstärkung des Schutzes Kritischer Infrastrukturen zu erarbeiten.[249] Vorgeschlagen werden Maßnahmen zur verstärkten Prävention, Abwehrbereitschaft und Reaktionsfähigkeit der Europäischen Union bei terroristischen Angriffen auf Kritische Infrastrukturen. Die EU-Kommission legte am 20. Oktober 2004 die Mitteilung *Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung*[250] vor. Diese gibt einen Überblick über die Maßnahmen auf europäische Ebene zum Schutz Kritischer Infrastrukturen und enthält Vorschläge für zusätzliche Maßnahmen zur Stärkung der bestehenden Instrumente.

2006 wurde das *Europäische Programm für den Schutz kritischer Infrastrukturen (EPSKI)*[251] ausgearbeitet. Das EPSKI schlägt konkrete gesetzgeberische Maßnahmen vor, beispielsweise die Etablierung eines Verfahrens zur Ermittlung und Ausweisung Kritischer europäischer Infrastrukturen und eines gemeinsamen Konzeptes für die Bewertung der Notwendigkeit des Schutzes derartiger Infrastrukturen. Daneben werden die Errichtung eines Warn- und Informationsnetzes für Kritische Infrastrukturen (WINKI), die Einsetzung einer EU-Sachverständigengruppen zu Fragen des Schutzes Kritischer Infrastrukturen und der regelmäßige Informationsaustausch vorgeschlagen. Ziel des EPSKI ist die Verbesserung des Schutzes Kritischer Infrastrukturen in der EU. Dies soll durch die Einführung einer europäischen Gesetzgebung zum Schutzes Kritischer Infrastrukturen sichergestellt werden. Das EPSKI wird durch das Gemeinschaftsprogramm „Prävention, Abwehrbereitschaft und Folgenbewältigung im Zusammenhang mit Terrorakten und anderen Sicherheitsrisiken“, welches im Februar 2007 angenommen wurde, von 2007 bis 2013 kofinanziert.[252] Am 17. November 2005 nahm die Kommission das Grünbuch über ein Europäisches Programm

---

[249] Informationen hierzu sind abrufbar unter: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_de.htm (Stand: 21.08.2012)

[250] Mitteilung der Kommission an den Rat und das Europäische Parlament vom 20. Oktober 2004 „Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung" (KOM(2004) 702 endg., abrufbar unter: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=de&type_doc=COMfinal&an_doc=2004&nu_doc=702 (Stand: 21.08.2012)

[251] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:DE:PDF (Stand: 21.08.2012)

[252] Vgl. dazu ausführlich: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_de.htm (Stand: 21.08.2012)

für den Schutz Kitischer Infrastrukturen[253] an. 2006 erfolgte der Beschluss über die Finanzierung des EPSKI-Pilotprojekts. Zudem legte die Kommission einen Vorschlag für eine *Richtlinie über die Ermittlung und Ausweisung kritischer europäischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern*[254] vor. Die Richtlinie wurde zwischenzeitlich erlassen und in Deutschland durch die *Verordnung zum Schutz von Übertragungsnetzen* umgesetzt.[255]

2009 stellte die EU-Kommission einen Aktionsplan für den Schutz Kritischer Informationsinfrastrukturen im Rahmen einer Mitteilung vor.[256] Im Gegensatz zu EPSKI konzentriert sich dieser auf den IKT-Sektor. Das weitere Vorgehen wurde 2011 in der Veröffentlichung der Europäischen Kommission *Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit*[257] vorgeschlagen und im März 2012 mit der Mitteilung der Kommission *Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität* fortgeschrieben.[258]

Am 13. Dezember 2011 kündigte Neelie Kroes, EU-Kommissarin für die Digitale Agenda, eine „große europäische Strategie für die Sicherheit der europäischen Netze“ an.[259] Die EU-Kommission hat am 28. März 2012 die Einrichtung eines europäischen Cybercrime Centre

---

[253] Grünbuch vom 17. November 2005 über ein Europäisches Programm für den Schutz kritischer Infrastrukturen (KOM(2005) 576 endg.). (Stand: 21.08.2012)

[254] Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern. Online abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:DE:PDF (Stand: 21.08.2012)

[255] Abrufbar unter: http://www.gesetze-im-internet.de/_nschutzv/BJNR006900012.html (Stand: 21.08.2012)

[256] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen - „Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität“ (KOM(2009) 0149 endg.), abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:DE:PDF (Stand: 21.08.2012)

[257] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen - „Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit” (KOM(2011) 163endg.), abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:DE:PDF

[258] Mitteilung der Kommission „Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität“ KOM/2012/0140, abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0140:DE:NOT . (Stand: 21.08.2012)

[259] http://www.heise.de/newsticker/meldung/Neue-EU-Strategie-fuer-Sicherheit-in-den-Netzen-angekuendigt-1394814.html (Stand: 21.08.2012)

(E3C) vorgeschlagen, welches Europol angeschlossen werden soll. Es ist geplant, dass das E3C seine Arbeit Anfang 2013 aufnimmt.[260]

Europäische Agentur für Netz- und Informationssicherheit (ENISA)

Die Europäische Agentur für Netz- und Informationssicherheit (European Network and Information Security Agency, ENISA)[261] ist, zusammen mit anderen EU-Institutionen und nationalen Behörden, zuständig für die Entwicklung einer Sicherheitskultur für EU-weite Informationsnetze.[262] Rechtsgrundlage von ENISA ist die *Verordnung des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit*.[263] Ihre Aufgabe ist es, hochgradige Netz- und Informationssicherheit zu gewährleisten, indem sie EU-Institutionen und staatlichen Behörden fachkundigen Rat zur Netz- und Informationssicherheit erteilt, ein Forum für den Austausch bewährter Verfahren bietet und Kontakte zwischen EU-Institutionen, staatlichen Behörden und Unternehmen vermittelt und erleichtert.[264] Die Kapazitäten der Europäischen Union, der EU-Mitgliedstaaten und der Unternehmen im Bereich der Netz- und Informationssicherheit sollen durch ENISA verstärkt werden. Zudem unterstützt ENISA die Europäische Kommission bei den technischen Vorarbeiten für die Aktualisierung und Weiterentwicklung der EU-Rechtsvorschriften sowie bei den Bemühungen eine Zusammenarbeit mit Drittländern zur Förderung eines Gesamtkonzepts in IT-Sicherheitsfragen sowie eigene Schlussfolgerungen, Leitlinien und Ratschläge zu formulieren.[265]

ENISA setzt sich aus einem Verwaltungsrat, einem Direktor und einer Ständigen Gruppe der Interessenvertreter zusammen. In den Verwaltungsrat werden von jedem EU-Mitgliedstaat je ein und von der Kommission drei Vertreter entsandt. Darüber hinaus gehören dem Verwaltungsrat je ein Vertreter der IKT-Industrie, von Verbrauchergruppen sowie ein

---

[260] Vgl. Mitteilung der Kommission an den Rat und das Europäische Parlament Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität /* COM/2012/0140 final */ Online abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:DE:PDF sowie https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417 (Stand: 21.08.2012)

[261] Offizielle Webseite: http://www.enisa.europa.eu (Stand: 21.08.2012)

[262] Vgl. http://europa.eu/agencies/regulatory_agencies_bodies/policy_agencies/enisa/index_de.htm (Stand: 21.08.2012)

[263] Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (Text von Bedeutung für den EWR), abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:DE:NOT. (Stand: 21.08.2012)

[264] Vgl. http://europa.eu/agencies/regulatory_agencies_bodies/policy_agencies/enisa/index_de.htm (Stand: 21.08.2012)

[265] Die Aufgaben von ENISA werden in der Verordnung zur Errichtung von ENISA beschrieben. Online abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:077:0001:0011:DE:PDF Abschnitt 1 Artikel 3
Vgl. http://europa.eu/legislation_summaries/information_society/internet/l24153_de.htm (Stand: 21.08.2012)

wissenschaftlicher Sachverständiger für die Netz- und Informationssicherheit an, welche jedoch kein Stimmrecht besitzen. Der Direktor wird vom Verwaltungsrat aus einer von der EU-Kommission vorgelegten Bewerberliste ausgewählt und ernannt. Die Ständige Gruppe der Interessenvertreter besteht aus Vertretern der IKT-Branche, Verbrauchervertretern und wissenschaftlichen Sachverständigen.[266]

Das Mandat für ENISA soll erweitert werden – über das Nachfolgemandat wird derzeit verhandelt.[267] Zudem hat Neelie Kroes, EU-Kommissarin für die Digitale Agenda, eine verstärke Rolle für ENISA in der europäischen IT-Sicherheit angekündigt.[268] Ursprünglich wurde ENISA bis zum Jahr 2004 eingerichtet. Im Juni 2011 wurde die Einsetzungsdauer bereits zum zweiten Mal bis zum 13. September 2013 verlängert.[269]

Am 4. November 2011 wurde die erste europäische Cybersicherheitsübung *Cyber Europe 2010* mit Unterstützung der ENISA und der Gemeinsamen Forschungsstelle der Europäischen Kommission (Joint Research Centre, JRC) durchgeführt.[270] Im Abschlussbericht über die Cybersicherheitsübung wird die Übung als „useful 'cyber stress test'" bewertet. Ein wichtiges Ergebnis der Übung war auch, dass hierdurch die Klärung der Kompetenzen in den jeweiligen europäischen Ländern und, dass es jetzt in jedem Land einen Ansprechpartner gibt.[271] Die Mitgliedstaaten wollen weitere nationale und europäische Cybersicherheitsübungen durchführen und bei diesen den privaten Sektor mit einbeziehen.[272]

---

[266] Die Organisationsstruktur ist in der Verordnung zur Errichtung von ENISA geregelt. Online abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:077:0001:0011:DE:PDF Abschnitt 2 Artikel 5 bis 8. Vgl. auch http://europa.eu/legislation_summaries/information_society/internet/l24153_de.htm (Stand: 21.08.2012)

[267] S. die Pressemitteilung des Rates 10494/11 vom 27. Mai 2011, abrufbar unter: http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/11/145&format=HTML&aged=1&language=DE&guiLanguage=en, sowie den zugehörigen Sachstandsbericht 10296/11, abrufbar unter: http://register.consilium.europa.eu/pdf/de/11/st10/st10296.de11.pdf

[268] Meldung auf Heise online vom 13.12.2011, abrufbar unter: http://www.heise.de/newsticker/meldung/Neue-EU-Strategie-fuer-Sicherheit-in-den-Netzen-angekuendigt-1394814.html (Stand: 21.08.2012)

[269] Verordnung (EU) Nr. 580/2011 des Europäischen Paralaments und des Rates vom 8. Juni 2011 zur Änderung der Verordnung (EG) Nr. 460/2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer, S. 3. Online abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:165:0003:0004:DE:PDF. (Stand: 21.08.2012)

[270] Digitale Agenda: Experten für Netzsicherheit erproben Abwehrfähigkeit bei erster gesamteuropäischer Simulation, Pressemitteilung vom 4. November 2010, abrufbar unter: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1459&format=HTML&aged=1&language=DE&guiLanguage=en (Stand: 21.08.2012)

[271] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report/at_download/fullReport, Seite 8.

[272] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report/at_download/fullReport, Seite 6.

Aufbauend auf den Erkenntnissen der ersten europäischen Cybersicherheitsübung fand am 4. Oktober 2012 die zweite Cybersicherheitsübung *Cyber Europe 2012* statt.[273]

II.1.3.2.2 Initiativen des Europarates

Am 8. November 2001 wurde das Übereinkommen über Computerkriminalität[274] (englisch: Convention on Cybercrime, CC) durch das Ministerkomitee des Europarats in Budapest verabschiedet (siehe hierzu ausführlich Kapitel II.2.3.1.1).

II.1.3.3 Aktiviäten auf Bundesebene

Die Gewährleistung des Schutzes Kritischer Infrastrukturen ist eine „Kernaufgabe staatlicher und unternehmerischer Sicherheitsvorsorge und zentrales Thema der Sicherheitspolitik“ in Deutschland.[275] Auf Bundesebene wird diese komplexe und vielschichtige Aufgabe durch mehrere Akteure wahrgenommen. Es wurden verschiedene Strategie und Maßnahmen entwickelt. Im Folgenden werden, ohne den Anspruch auf Vollständigkeit, die Akteure und Maßnahmen vorgestellt.

II.1.3.3.1 Akteure

Bundesministerium des Innern (BMI)

Die ressortübergreifende Koordinierung des Schutzes Kritischer Infrastrukturen aller bundesstaatlichen Maßnahmen obliegt dem BMI. Bereits 2005 hat das BMI als die in Deutschland für die Innere Sicherheit zuständige Behörde gemeinsam mit Sicherheitsexperten des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe **(**BBK), des Bundeskriminalamtes (BKA) und aus der Wirtschaft ein Basisschutzkonzept[276] erarbeitet, das potenzielle Gefährdungen analysiert und Maßnahmen für Schutzvorkehrungen baulicher, organisatorischer, personeller und technischer Art empfiehlt.[277] Auf dieser Grundlage baut der

---

[273] Vgl. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report/at_download/fullReport

[274] Convention on Cybercrime, Online abrufbar unter: http://conventions.coe.int/treaty/ger/treaties/html/185.htm (Stand: 21.08.2012)

[275] Vgl. dazu ausführlich KRITIS-Strategie, Seite 3, online abrufbar unter: http://www.bmi.bund.de/cae/servlet/contentblob/598730/publicationFile/34416/kritis.pdf

[276] Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2005/Basisschutzkonzept_kritische_Infrastrukturen.html?nn=106228 (Stand: 26.08.2012)

[277] Vgl. http://www.bmi.bund.de/DE/Themen/Sicherheit/BevoelkerungKrisen/Kritis/kritis_node.html (Stand: 26.08.2012) i.V.m. http://www.bmi.bund.de/cae/servlet/contentblob/598730/publicationFile/34416/kritis.pdf (Stand: 26.08.2012)

2008 veröffentlichte und 2011 aktualisierte Leitfaden „Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement“[278] für die Betreiber Kritischer Infrastrukturen auf.

Die Zuständigkeit des BMI erstreckt sich auch auf die Sicherheit im Cyber-Raum und den Schutz der Kritischen Informationsstrukturen.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik, eine nationale Sicherheitsbehörde im Geschäftsbereich des BMI, versteht sich als zentraler IT-Sicherheitsdienstleister des Bundes mit dem Ziel, die IT-Sicherheit in Deutschland voranzubringen. Es wurde am 1. Januar 1991 als unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft gegründet.[279] Zu seinen Aufgaben zählen die vier Kernbereiche Information und Beratung zur IT-Sicherheit, Entwicklung von IT-Sicherheitsanwendungen und -produkten sowie Zertifizierung von IT-Systemen.[280] Diese sind ausführlich im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG), Artikel 3, beschrieben.

In der Stellungnahme des BSI, die der Projektgruppe im Rahmen des öffentlichen Expertengespräches „Sicherheit im Netz“ vom 28. November 2011 zugegangen ist, wurde darauf hingewiesen, dass „staatliche Eingriffsbefugnisse […] für das BSI in Bezug auf IKT-Sicherheit Kritischer Infrastrukturen in der Regel weder allgemein noch konkret [bestehen]. Daher kann das BSI den unmittelbaren Schutz Kritischer Infrastrukturen durch Anwendung eigener Mittel nur begrenzt gewährleisten. Dennoch besteht natürlich ein erhebliches staatliches Interesse, den notwendigen Schutz Kritischer Infrastrukturen sicherzustellen. Im Rahmen seines Auftrags trägt des BSI hierzu in verschiedensten Bereichen umfangreich bei. Beispielhaft sollen hier folgende Punkte genannt werden:

– Besondere Berücksichtigung des Schutzes Kritischer Infrastrukturen bei der Umsetzung der Cybersicherheitsstrategie des Bundes

---

[278] Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen.html?nn=106228 (Stand: 26.08.2012)

[279] Vgl. https://www.bsi.bund.de/DE/DasBSI/Aufgaben/aufgaben_node.html (Stand: 26.08.2012)

[280] Vgl. https://www.bsi.bund.de/DE/DasBSI/Leitbild/leitbild_node.html (Stand: 26.08.2012) Zu den

– Kooperation mit Betreibern Kritischer Infrastrukturen bei der strategischen Umsetzung des IKT-spezifischen Schutzes Kritischer Infrastrukturen (Kontext: Cybersicherheitsstrategie des Bundes, Umsetzungsplan KRITIS)
– Einbindung von Betreibern Kritischer Infrastrukturen in die Warn- und Krisenkommunikation des IT-Lagezentrums und des IT-Krisenreaktionszentrums des Bundes, das im BSI betrieben wird
– Spezifische Berücksichtigung von Aspekten des Schutzes Kritischer Infrastrukturen bei der täglichen Beobachtung der IKT-Lage
– Besondere Behandlung von IKT-Vorfällen mit Relevanz für Kritische Infrastrukturen (z.B. Stuxnet)

Darüber hinaus sind die allgemeinen Tätigkeiten des BSI eine gerade für den Schutz Kritischer Infrastrukturen unverzichtbare Grundlage. Dies sind beispielsweise:

– Bereitstellung allgemeiner Empfehlungen zum Schutz von IKT-Systemen. Diese enthalten auch wesentliche Hinweise für den Schutz Kritischer Infrastrukturen enthalten (IT-Grundschutz nach BSI, ISi-Reihe et al.)
– Bereitstellung von Studien und Sicherheitsanalysen zu spezifischen IKT-Themen und IKT-gestützten Basistechnologien
– Verbesserung des Schutzes von IKT-Systemen allgemein. Dies trägt auch zur Verringerung der allgemeine Bedrohung für Kritische Infrastrukturen bei.“[281]

Innerhalb des BSI: CERT-Bund

Die Betreiber Kritischer Infrastrukturen sind in die Warn- und Krisenkommunikation des IT-Lagezentrums und des IT-Krisenreaktionszentrums des Bundes (CERT-Bund, kurz für Computer Emergency Response Team der Bundesverwaltung) eingebunden, das im BSI betrieben wird. Die IKT-Lage wird unter Berücksichtigung des Schutzes von IKT täglich beobachtet. Das BSI stellt zudem allgemeine Empfehlungen zum Schutz von IKT-Systemen,

[281] Stellungnahme zum Expertengespräch der Projektgruppe Zugang, Struktur und Sicherheit im Netz am 28. November 2011 von Andreas Könen (BSI), S. 2, abrufbar unter http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZustrSi_2011-11-28_oeffentliches_Expertengespraech/PGZuStSi_2011-11-28_Expertengespraech_Stellungnahme_Koenen.pdf ; nach § 7 BSIG besteht die Befugnis, Warnungen vor Sicherheitslücken in informationstechnischen Produkten und vor Schadprogrammen an die betroffenen Kreise oder die Öffentlichkeit weiterzugeben oder Sicherheitsmaßnahmen zu empfehlen. Vgl. dazu Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG), abrufbar unter: http://www.gesetze-im-internet.de/bundesrecht/bsig_2009/gesamt.pdf

Studien und Sicherheitsanalysen zu spezifischen IKT-Themen und IKT-gestützten Basistechnologie zur Verfügung.[282] CERT-Bund wurde am 1. September 2001 gegründet und übernimmt Aufgaben im Bereich der Computersicherheit in den verschiedenen Institutionen der Bundesrepublik Deutschland. Das BSI bietet auch einen kostenfreien Dienst für Privatpersonen an, das so genannte Bürger-CERT, der vor Sicherheitslücken in Computerprogrammen warnt.[283]

Das BSI sieht bei elektronischen Automatisierungs-, Steuerungs- und Kontrollsystemen ein steigendes Risiko für IT-Angriffe, und zwar insbesondere hinsichtlich der Systeme, die für die Steuerung kritischer Infrastrukturen eingesetzt werden. Solche SCADA-Systeme sind mittlerweile beinahe Standard in der Verkehrssteuerung sowie in der Energie- und Wasserversorgung. Im Finanzwesen stützt man sich hauptsächlich auf IT-Verfahren, insbesondere im Hinblick auf Finanztransaktionen. Auch Krankenhäuser setzen, sowohl was den Umgang mit Patientendaten angeht als auch sogar in der Intensivmedizin, zunehmend auf IT. Notfall- und Rettungsdienste nutzen im Einsatz Smartphones und andere Mobilkommunikationssysteme und werden damit potenzielle Opfer von IT-Angriffen.[284]

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

Beim BBK werden alle einschlägigen Aufgaben zur Sicherung der zivilen Sicherheit an einer Stelle gebündelt. Es ist Fachbehörde des BMI, kann aber fachübergreifend alle Bereiche der zivilen Sicherheitsvorsorge berücksichtigen und andere Bundes- und Landesbehörde beraten und unterstützen. Das BBK koordiniert den Schutz Kritischer Infrastrukturen und insbesondere die Kommunikationen des Bundes mit den Ländern und Gemeinden, der Privatwirtschaft und der Bevölkerung über Vorsorgeplanung und aktuelle Bedrohungen. Es sammelt die verschiedenen Informationsquellen zu Gefahren, fasst diese zusammen und bewertet sie. Außerdem unterstützt es das Management von Einsatzkräften des Bundes und anderer öffentlicher und privater Ressourcen bei großflächigen Gefahrenlagen. Es ist zuständig für die bedrohungsgerechte Ausbildung von Führungskräften aller Verwaltungsebenen im Bevölkerungsschutz. Zudem ist es zuständig für die Koordinierung

---

[282] Vgl. Stellungnahme Expertengespräch PG ZStrSi von Andreas Könen (BSI) 28. November 2011, http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZustrSi_2011-11-28_oeffentliches_Expertengespraech/PGZuStSi_2011-11-28_Expertengespraech_Stellungnahme_Koenen.pdf

[283] www.bsi.bund.de, www.buerger-cert.de (Stand: 24.08.2012)

[284] Vgl. dazu ausführlich Bevölkerungsschutz, Cyber-Sicherheit 4/2011, Herausgeber BBK, S. 5

von Bund, Ländern, Feuerwehren und privaten Hilfsorganisationen bei der Wahrnehmung internationaler humanitärer Aufgaben und in der zivil-militärischen Zusammenarbeit.[285]

Das BBK nahm im Jahr 2004 seine Arbeit auf. Nach den Anschlägen auf das World Trade Center in New York am 11. September 2001 und nach der Flutkatastrophe in Deutschland im Jahr 2002 stand die bisherige Zweiteilung des deutschen Katastrophenvorsorgesystems, das zwischen der Bundeszuständigkeit für den Bevölkerungsschutz im Verteidigungsfall und der alleinigen Zuständigkeit der Länder auch bei länderübergreifenden Katastrophenfällen unterscheidet, in Frage. Die Einrichtung des BBK trägt dem Bedürfnis nach einem gemeinsamen Krisenmanagement durch Bund und Länder bei außergewöhnlichen, national bedeutsamen Gefahren- und Schadenslagen Rechnung, bei dem alle Ebenen zusammen arbeiten müssen. [286]

Das BSI und das BBK betreiben eine gemeinsame „Internetplattform zum Schutz kritischer Infrastrukturen“.[287]

Bundesanstalt Technisches Hilfswerk (THW)

Gemäß § 1 Absatz 2 des Gesetzes über das Technische Hilfswerk (THW-Helferrechtsgesetz, THW-Gesetz) leistet die Bundesanstalt Technisches Hilfswerk technische Hilfe: „1. nach dem Zivilschutz- und Katastrophenhilfegesetz, 2. im Ausland im Auftrag der Bundesregierung, 3. bei der Bekämpfung von Katastrophen, öffentlichen Notständen und Unglücksfällen größeren Ausmaßes auf Anforderung der für die Gefahrenabwehr zuständigen Stellen sowie 4. bei der Erfüllung öffentlicher Aufgaben im Sinne der Nummer 1 bis 3, soweit es diese durch Vereinbarung übernommen hat“.[288] Sie ist bundesweit aufgestellt und dabei örtlich, national und weltweit einsatzfähig.

Bundeskriminalamt (BKA)

Das BKA hilft bei der Aufklärung von Verbrechen gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland und unterstützt dabei den Generalbundesanwalt und die Staatsanwaltschaften. Gemäß § 4 Absatz 1 Nummer 5 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in

---

[285] Vgl. dazu ausführlich http://www.bbk.bund.de/DE/DasBBK/UeberdasBBK/ueberdasbbk_node.html (Stand: 26.08.2012)

[286] Vgl dazu: http://www.bbk.bund.de/DE/DasBBK/UeberdasBBK/ueberdasbbk_node.html (Stand: 26.08.2012)

[287] Abrufbar unter: http://www.kritis.bund.de/SubSites/Kritis/DE/Home/home_node.html. (Stand: 21.08.2012)

[288] THW-Gesetz § 1 Abs. 2, Gesetz über das Technische Hilfswerk (THW-Helferrechtsgesetz - THW-Gesetz), abrufbar unter: http://www.gesetze-im-internet.de/thw-helfrg/BJNR001180990.html

kriminalpolizeilichen Angelegenheiten (BKAG)[289] ermittelt das BKA zum Beispiel auch in besonders schweren Fällen der Computersabotage (§ 303b Strafgesetzbuch), wenn dadurch etwa sicherheitsempfindliche Stellen lebenswichtiger Einrichtungen, bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen zu befürchten ist, betroffen sind, oder die innere oder äußere Sicherheit der Bundesrepublik Deutschland beeinträchtigt wird.[290] Das BKA unterstützt auch die Behörden der Länder bei Strafverfolgungsmaßnahmen, wenn dies erforderlich ist oder die Landesbehörde darum ersucht.[291] Zudem ermittelt es im Rahmen der Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) im Internet nach strafbaren Inhalten[292]

Bundesnetzagentur (BNetzA)

Die Bundesnetzagentur ist insbesondere dafür zuständig, die Umsetzung von Regulierungsvorhaben voranzutreiben und zu kontrollieren. Sie stellt die Zuverlässigkeit und Sicherheit von Telekommunikationsnetzwerken sicher.

Bundesministerium der Verteidigung (BMVg)

Das Bundesministerium der Verteidigung ist für die Landesverteidigung und die Aufrechterhaltung der Einsatzbereitschaft und Leistungsfähigkeit der Streitkräfte zuständig und unterstützt den Schutz Kritischer Infrastrukturen in diesem Rahmen seiner Zuständigkeit.[293]

II.1.3.3.2 Maßnahmen

Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)[294]

---

[289] BKAG: Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, online abrufbar unter: http://www.gesetze-im-internet.de/bkag_1997/BJNR165010997.html (Stand: 24.08.2012)

[290] Vgl. http://www.bka.de/nn_206342/DE/DasBKA/Aufgaben/Ermittlungen/ermittlungen__node.html?__nnn=true (Stand: 24.08.2012)

[291] Vgl. § 17Abs. 1 BKAG (Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, online abrufbar unter: http://www.gesetze-im-internet.de/bkag_1997/BJNR165010997.html

[292] Vgl. http://www.bka.de/nn_204456/DE/DasBKA/Aufgaben/Zentralstellen/ZaRD/zard__node.html?__nnn=true#doc204436bodyText1 (Stand: 24.08.2012)

[293] Vgl. http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYuxDsIwDET_yE62lo2qQmIFCQhb2kaRUeNUxikLH08ycCe94Z4On1jLfqfolTL7FR_oZjpMH5jSHuGVi9QVEjG9NQiVhPf2WQLMmYM2amClyihes8CWRddmikg1QAs6Y8fBWPOP_XZX159une3H83DBLaXjD6EEIfY!/ S. 13, 29 (Stand: 26.08.2012)

[294] Bundesministerium des Innern (Hrsg.) : Nationaler Plan zum Schutz der Informationsinfrastrukturen. Juli 2005. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf?__blob=publicationFile

Der NPSI wurde 2005 als deutsche Dachstrategie für den Schutz der Informationsinfrastrukturen durch das Bundeskabinett beschlossen. Ziele waren Prävention, Reaktion und Nachhaltigkeit. Informationsinfrastrukturen sollten angemessen geschützt, bei IT-Sicherheitsvorfällen sollte sinnvoll gehandelt und deutsche IT-Sicherheitskompetenz sollte gestärkt werden. Eine Maßnahme aus dem NPSI ist der Aufbau eines IT-Lagezentrums, das für Bundesbehörden und Betreiber Kritischer Infrastrukturen 24 Stunden erreichbar ist.[295] Der NPSI wurde im Februar 2011durch die *Cyber-Sicherheitsstrategie für Deutschland* abgelöst.

Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen (UP KRITIS)[296]

Der UP KRITIS wurde 2007 gleichzeitig mit dem *Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung (UP Bund)* entwickelt. Beim UP KRITIS haben etwa 30 große Betreiber Kritischer Infrastrukturen in Deutschland beziehungsweise deren Interessenverbände mit Vertretern des Bundes zusammengearbeitet, um die dort beschriebenen IT-Sicherheitsmaßnahmen zu ihrem eigenen Standard zu erklären und dieses Niveau dauerhaft sicherzustellen.[297] Der Schwerpunkt der Zusammenarbeit liegt in der Kommunikation zwischen den einzelnen Sektoren sowie zwischen Staat und Unternehmen. Es soll sowohl die Kommunikation verbessert als auch die Bewältigung von IT-Krisen geplant und frühzeitig geübt werden, da gerade eine funktionierende Kommunikation und belastbare Beziehungsstrukturen unabdingbar für die Bewältigung einer IT-Krise sind.[298] Im Mittelpunkt der Krisenkommunikation stehen SPOCs (Single Points of Contact). Der Kommunikationsaufwand eines jeden Beteiligten soll minimiert und die Kommunikationswege sollen strukturiert werden. Die SPOCs fungieren als Melde- und Verteilerstellen sowohl zum BSI-Lagezentrum als auch zu den Kontaktstellen der Unternehmen der jeweiligen Branche.[299]

---

[295] Vgl.dazu https://www.bsi.bund.de/DE/Themen/IT-Krisenmanagement/IT-Lagezentrum/itlagezentrum_node.html (Stand: 26.08.2012)

[296] Bundesministerium des Innern (Hrsg.): Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen (UP KRITIS). September 2007. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2007/Kritis.pdf?__blob=publicationFile

[297] Vgl. Pressemmitteilung des Bundesministerium des Innern „Bundeskabinett verabschiedet Pläne zur Erhöhung der IT-Sicherheit in Deutschland, online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2007/09/it_sicherheit.html?nn=109632 (Stand: 24.08.2012)

[298] Vgl. Bevölkerungsschutz, Cyber-Sicherheit, 4/2011, Herausgeber: BBK, S. 12f

[299] Vgl. ebd., S. 13

Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)[300]

Die *KRITIS-Strategie* aus dem Jahr 2009 fasst die Zielvorstellungen und den politisch-strategischen Ansatz des Bundes zusammen und ist Ausgangspunkt dafür, das bisher Erlangte fortzusetzen und mit Blick auf neue Herausforderungen weiterzuentwickeln.[301]

Cyber-Sicherheitsstrategie für Deutschland[302]

Am 23. Februar 2011 beschloss die Bundesregierung die *Cyber-Sicherheitsstrategie für Deutschland*.[303] Kernpunkt der Strategie sind „der verstärkte Schutz Kritischer Infrastrukturen von IT-Angriffen, der Schutz der IT-Systeme in Deutschland, der Aufbau eines Nationalen Cyber-Abwehrzentrums sowie die Einrichtung eines Nationalen Cyber-Sicherheitsrates.“[304] Das Nationale Cyber-Abwehrzentrum nahm am 1. April 2011 seine Arbeit mit der Aufgabe auf, „IT-Sicherheitsvorfälle schnell und umfassend zu bewerten und abgestimmte Handlungsempfehlungen zu erarbeiten.“[305] Federführend ist das BSI. Direkt beteiligt sind das Bundesamt für Verfassungsschutz (BfV) und das BBK, als assoziierte Behörden wirken das BKA, die Bundespolizei (BPol), das Zollkriminalamt (ZKA), der Bundesnachrichtendienst (BND) und die Bundeswehr mit.[306]

IKT-Strategie der Bundesregierung „Deutschland Digital 2015“[307]

Die *IKT-Strategie* aus dem Jahr 2010 verweist auf die Aktivitäten der Bundesregierung zum Schutz Kritischer Infrastrukturen. In ihrem Rahmen planen das federführende Bundesministerium für Wirtschaft und Technologie (BMWi) und die verschiedenen Ressorts

---

[300] Bundesministerium des Innern (Hrsg.): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Juni 2009. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?__blob=publicationFile

[301] Vgl. Bundesministerium des Innern: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), S. 2, online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.html?nn=106228 (Stand: 21.08.2012)

[302] Bundesministerium des Innern (Hrsg.): Cyber-Sicherheitsstrategie für Deutschland. Februar 2011. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile

[303] Vgl. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile (Stand: 24.08.2012)

[304] http://www.bmi.bund.de/DE/Themen/OeffentlDienstVerwaltung/Informationsgesellschaft/SicherheitInDerIT/CSS/css_node.html (Stand: 26.08.2012)

[305] https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Cyber-Abwehrzentrum_01042011.html (Stand: 26.08.2012)

[306] Vgl. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile, S. 6. (Stand: 24.08.2012)

[307] http://www.bmwi.de/Dateien/BBA/PDF/ikt-strategie-der-bundesregierung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

ihre Aktivitäten und setzen diese um. Ziel der Strategie *Deutschland Digital 2015* ist es, das enorme Potenzial von IKT für Wachstum und Beschäftigung in Deutschland zu nutzen. Entstanden ist die IKT-Strategie im Zusammenspiel von Politik, Wirtschaft und Wissenschaft. Der nationale IT-Gipfel ist dabei zentrale Plattform.[308]

Mithilfe der Strategie sollen Unternehmen in ihrer Wettbewerbsfähigkeit gestärkt, Infrastrukturen ausgebaut, Schutz- und Individualrechte der Nutzer ausgebaut sowie Entwicklung und Forschung in diesem Bereich ausgebaut werden. Zudem soll IKT bei der Lösung gesellschaftlicher Probleme im Bereich Klimaschutz, Gesundheit und Mobilität genutzt werden.

Task Force IT-Sicherheit in der Wirtschaft[309]

Im März 2011 wurde zudem die Task Force IT-Sicherheit in der Wirtschaft vom BMWi eingesetzt. Damit sollen insbesondere die kleinen und mittelständischen Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützt werden. Durch eine enge Zusammenarbeit mit der Wirtschaft sollen sie für ein digitales Zeitalter gerüstet werden.[310]

Allianz für Cyber-Sicherheit[311]

Die Allianz für Cyber-Sicherheit ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) gegründet wurde. Sie hat das Ziel, die Cyber-Sicherheit in Deutschland zu erhöhen und die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Sie baut hierfür eine umfangreiche Wissensbasis auf und unterstützt den gegenseitigen Informations- und Erfahrungsaustausch aus.

Hightech-Strategie 2020 für Deutschland[312]

Auch das Bundesministerium für Bildung und Forschung (BMBF) beschäftigt sich mit IT-Sicherheit. IKT ist einer von fünf Bereichen, auf die sich die Bundesregierung mit der

---

[308] Vgl. dazu ausführlich: BMWi „IKT-Strategie der Bundesregierung „Deutschland Digital 2015“, S. 3, online abrufbar: http://www.bmwi.de/Dateien/BBA/PDF/ikt-strategie-der-bundesregierung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (Stand: 21.08.2012)

[309] http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/task-force.html

[310] Vgl. http://www.bmwi.de/BMWi/Navigation/Service/veranstaltungen,did=382160.html (Stand: 26.08.2012)

[311] http://www.allianz-fuer-cybersicherheit.de

[312] http://www.bmbf.de/pub/hts_2020.pdf

Hightech-Strategie 2020 konzentriert.[313] Die Förderung der Forschung im Bereich IT-Sicherheit soll mit der Fortführung beziehungsweise Neuauflage des IT-Sicherheitsforschungsprogramms ausgebaut werden. IKT gehört zu den Schlüsseltechnologien und ist deshalb Voraussetzung für neue Verfahren und Dienstleistungen, um neue gesellschaftliche Herausforderungen zu meistern.[314] In der letzten Auswahlrunde des aktuellen Spitzencluster-Wettbewerbs fand das Thema IT-Sicherheit im Gegensatz zu Themen wie Elektromobilität keine Berücksichtigung. Um die bereits in Deutschland aufgebaute Kompetenzen zur IT-Sicherheit zu erhalten und auszubauen, ist eine intensive politische und wirtschaftliche Flankierung nötig.

Für dieses Programm werden neue Instrumente eingesetzt. Geplant sind Innovationsallianzen und Technologieverbünde. Kleinere und mittlere Unternehmen sollen unter anderem durch vereinfachte Förderverfahren unterstützt werden. Es soll eine zentrale Anlaufstelle geben sowie einen kürzeren Zeitraum zwischen Antragstellung und Antragsbescheidung sowie Bereitstellung bewilligter Mittel. Anwendungsbereiche sind insbesondere die Automobilindustrie und Maschinenbau sowie Gesundheit, Medizintechnik, Logistik und Dienstleistungen.[315]

Die Übungsserie LÜKEX[316]

Seit 2004 wird in Deutschland LÜKEX (Länderübergreifende Krisenmanagement Exercise) als Übungsserie im Bereich des nationalen Krisenmanagements durchgeführt. Das federführende BMI hat für die Planung, Vorbereitung und Durchführung in Abstimmung mit den Ländern eine Bund-Länder-Projektorganisation eingerichtet.[317] An der Übung sind Bund, Länder und Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber) beteiligt. Bisher fanden fünf LÜKEX-Übungen für den Krisenstab der Bundesregierung sowie die Krisenstäbe der Landesregierungen statt. Die letzte LÜKEX-Übung fand am 30. November und 1. Dezember 2011 zum Thema Sicherheit in der Informationstechnologie statt, wobei die Übungsvorbereitungen schon Mitte 2010 begonnen haben.[318]

---

[313] Vgl. http://www.bmbf.de/pub/hts_2020.pdf (Stand: 26.08.2012)

[314] Vgl. http://www.bmbf.de/de/9069.php (Stand: 26.08.2012)

[315] Vgl. http://www.bmbf.de/de/9069.php (Stand: 26.08.2012)

[316] https://www.denis.bund.de/luekex/

[317] Vgl. Bevölkerungsschutz. Cyber-Sicherheit, 4/2011. Hg: BBK, S.9.

[318] Vgl. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Sonstiges/Infos_ueber_Luekex.pdf?__blob=publicationFile (Stand: 26.08.2012)

Seit dieser Zeit wurde beim BBK gemeinsam mit dem BSI das Szenario eines Angriffs auf die IT-Infrastruktur entwickelt. Insgesamt probten ungefähr 2 500 Beteiligte aus zwölf Bundesländern, unter ihnen auch IT-Spezialisten, wie ein länderübergreifendes Krisenmanagement anläuft, wenn ein IT-Notfall festgestellt wird, der dann eskaliert. Zum ersten Mal waren an einer LÜKEX-Übung auch das nationale Cyber-Abwehrzentrum und die Bundesnetzagentur beteiligt.

Das Übungsszenario ging von IT-Störungen durch zielgerichtete Angriffe aus, die IT-Schwachstellen ausnutzen. Simuliert wurde wie erhebliche Beeinträchtigungen bei kritischen Infrastrukturen und Versorgungsengpässe im gesellschaftlichen Umfeld eintraten, etwa im Verkehr, in den Bereichen Finanzwesen und Kommunikation, aber auch in der öffentlichen Verwaltungen von Bund und Ländern. Die von der IT-Übung hauptsächlich betroffenen Bundesressorts sowie zwölf Bundesländer übten zusammen mit ausgewählten Unternehmen der kritischen Infrastrukturen. Darüber hinaus waren auch Verbände und Hilfsorganisationen an der Übung beteiligt.[319] Inwieweit die Übung als Erfolg gewertet werden wird, wird eine Analyse nach der Durchführung ergeben.

II.2. Kriminalität im Internet

Die intensive Nutzung des Internets und der teilweise hohe Grad der Vernetzung wurden in anderen Berichten der Enquete-Kommission bereits dargestellt. Neuere Trends wie das Cloud Computing oder die Nutzung mobiler Endgeräte verstärken die Vernetzung.[320] Auch Straftäter benutzen das Netz und seine Möglichkeiten für ihre Aktivitäten. Nicht nur herkömmliche Formen von Kriminalität, die sich lediglich der neuen technischen Mittel bedienen, sind zu beobachten, sondern auch gänzlich neue Kriminalitätsformen, die ohne das Internet nicht denkbar wären. Die Politik sieht sich der Herausforderung gegenüber, zum einen für den Schutz der Betroffenen und der gesamten Gesellschaft zu sorgen, gleichzeitig aber die Offenheit des Netzes zu bewahren.

---

[319] Vgl. http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2011/ohneMarginalspalte/11/luekex2011.html (Stand: 26.08.2012)

[320] S. dazu BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 6, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile

II.2.1 Grundlagen

II.2.1.1 Überblick und Eingrenzung des Themenfeldes „Kriminalität im Internet“

Für das Jahr 2011 weist die Polizeiliche Kriminalstatistik (PKS) 222 267 über das Internet begangene Straftaten aus.[321] Hervorzuheben sind hier vor allem die Betrugsdelikte – insbesondere der Warenbetrug[322] – die mit insgesamt 75,5 Prozent den größten Anteil ausmachen.[323] Eine steigende Tendenz ist im Bereich des Ausspähens und Abfangens von Daten zu erkennen.[324] Die Aufklärungsquote bei Straftaten unter Einsatz des Tatmittels Internet lag 2011 bei 65,1 Prozent.[325]

Eine allgemeine Definition des Begriffs „Kriminalität im Internet“ ist aufgrund der Uferlosigkeit möglicher Erscheinungsformen schwierig.[326] Denn oftmals ist das Internet nur (ein weiteres) Mittel zum Zweck, etwa beim Betrug gemäß § 263 des Strafgesetzbuches (StGB)[327]. Daher ist die genannte Zahl der PKS unter dem dort gewählten Schlagwort „Internet als Tatmittel“ mit der gebotenen Vorsicht zu betrachten.[328]

Zur Eingrenzung des Diskussionsgegenstandes bedarf es einer Konkretisierung des Themenfeldes. Hier kommt insbesondere die von der PKS gesondert erfasste „IuK-Kriminalität im engeren Sinne“ als Teil der genannten Straftaten in Betracht. Dieser Begriff erfasst Computerbetrug, Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten,

---

[321] BMI, Polizeiliche Kriminalstatistik 2011, S. 7, abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2012/PKS2011.pdf?__blob=publicationFile

[322] 28,3 %, s. BMI, Polizeiliche Kriminalstatistik 2011, S. 7, abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2012/PKS2011.pdf?__blob=publicationFile

[323] BMI, Polizeiliche Kriminalstatistik 2011, S. 7, abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2012/PKS2011.pdf?__blob=publicationFile

[324] BMI, Polizeiliche Kriminalstatistik 2011, S. 7, abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2012/PKS2011.pdf?__blob=publicationFile

[325] http://www.polizei-beratung.de/datenbanken/infografiken/download/KP_2012_export_Internet.jpg und siehe hierzu auch das Bundeslagebild Cybercrime des BKA vom 17. September 2012 http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2011,templateId=raw,property=publicationFile.pdf/cybercrime2011.pdf

[326] Gercke, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 73; Kshetri, The Global Cybercrime Industry, 2010, S. 3 f.

[327] Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 25. Juni 2012 (BGBl. I S. 1374).

[328] S. Franosch, Schriftliche Stellungnahme zu Expertengespräch „Internetkriminalität“, S. 11, der darauf hinweist, dass aus diesem Grund für das Jahr 2010 auch 31 Fälle des „Diebstahls von Fahrrädern unter erschwerenden Umständen“ unter dem genannten Punkt erfasst wurden. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

Datenfälschung, Täuschung im Rechtsverkehr bei Datenverarbeitungen, Datenveränderung/Computersabotage sowie das Ausspähen beziehungsweise Abfangen von Daten. In diesem Bereich wurden für das Jahr 2011 insgesamt 59 494 Fälle verzeichnet.[329] Laut dem „Cybercrime Bundeslagebild 2010“, in welchem die gleichen Straftaten unter dem Begriff „Cybercrime“ erfasst werden, nennt das Bundeskriminalamt (BKA) einen registrierten Gesamtschaden von 61,5 Millionen Euro, was einem Anstieg von 24,6 Millionen Euro oder 66,9 Prozent im Vergleich zum Jahr 2009 entspricht.[330] Zusätzlich ist aber von einer hohen Dunkelziffer auszugehen.[331]

II.2.1.2 Arbeitsdefinition

Für diesen Bericht wird im Weiteren folgende Definition zugrunde gelegt:

„Kriminalität im Internet“ im Rahmen dieses Berichts meint die Begehung von Straftaten, welche nicht der Spionage oder Sabotage zuzuordnen sind, und die entweder ausschließlich im Internet möglich sind oder aber bei denen der Einsatz von Internettechnik zumindest wesentlich für die Tatausführung ist.

II.2.1.3 IT-Sicherheit

Mit dem Begriff der Internetkriminalität einher geht der davon zu unterscheidende Begriff der IT-Sicherheit. Der Ausgangspunkt jeder Überlegung und Planung eines sicheren IT-Systems

---

[329] BMI, Polizeiliche Kriminalstatistik 2011, S. 7 f., abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2012/PKS2011.pdf?__blob=publicationFile

[330] BKA, Cybercrime Bundeslagebild 2010, S. 6, abrufbar unter: http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf; die Schadenssumme wird allerdings nur bei den Delikten Computerbetrug und Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten erfasst, s. Franosch, Schriftliche Stellungnahme zu Expertengespräch „Sicherheit im Netz“, S. 13. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf. Im Bereich der Polizeibehörden wird von „IuK-Kriminalität“ gesprochen, die nicht deckungsgleich sein muss mit dem Begriff Internetkriminalität, wie er im Bereich der Strafrechtswissenschaft gebraucht wird; vgl. Förster, Internetkriminalität, S.178; s. weiter Walter, Internetkriminalität, 2008, S. 19.

[331] BKA, Cybercrime Bundeslagebild 2010, S. 7, abrufbar unter: http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf; s. auch Walter, Internetkriminalität, 2008, S. 12.

ist die Definition von Schutzzielen. Die folgende Einteilung hat sich durchgesetzt und ist bereits seit vielen Jahren anerkannt:[332]

- **Integrität** ist gegeben, wenn Daten hinsichtlich Korrektheit und Vollständigkeit vor unberechtigter und unbemerkter Manipulation geschützt sind.[333]
- Der Begriff der **Vertraulichkeit** ist eng mit dem Begriff der Integrität verbunden. Er ist komplementär zum Schutz vor Veränderung von Daten als Schutz vor Zugriff auf Daten durch nicht autorisierte Personen zu verstehen.[334]
- **Verfügbarkeit** bedeutet, dass ein IT-System zum erwarteten Zeitpunkt mit den erforderlichen Daten und Funktionen dem berechtigten Anwender zur Verfügung steht.[335]
- Die Eigenschaft der **Authentizität** liegt vor, wenn die Identität eines Nutzers eindeutig und zweifelsfrei bestätigt werden kann. Dies kann beispielsweise durch die Eingabe eines Benutzernamens und des dazugehörigen Passworts erfolgen.[336]

II.2.1.4 Motivation der Täter

Im Bereich der Internetkriminalität handeln die Täter oft aus reiner Freude an der Beschäftigung mit der Technik, um ein als sicher geltendes System zu überwinden.[337] So ist es möglich, dass „these hackers often don't have any malicious intent and are unaware that their actions violate security policy or criminal codes".[338] Aber auch Anerkennung in einer

---

[332] Hierzu Tanenbaum, Moderne Betriebssysteme, 2009, S. 712; Tipton/Krause, Information Security Management Handbook, 2007, S. 2409; Sonntag, IT-Sicherheit kritischer Infrastrukturen, 2005, S. 53 f.; oftmalswerden auch nur Integrität, Vertraulichkeit und Verfügbarkeit genannt, s. Gercke/Brunst, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, S. 2; Gaycken, Cyberwar, 2011, S. 124 (Fn. 1) m.w.N.; Blattner-Zimmermann, in: Holznagel/Hanßmann/Sonntag, IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen, 2001, S. 8, 16; die genannten Kriterien sind auch in zahlreichen IT-Sicherheitsstandards verankert, so beispielsweise in den Common Criteria for Information Technology Security Evaluation (inzwischen zum ISO-Standard 15408 erhoben); ebenso im ISO-Standard 27001 zu den Anforderungen an Informationssicherheits-Managementsysteme sowie im BSI-Standard 100-1 zum IT-Grundschutz; dementsprechend auch § 2 Absatz 2 BSIG: „[...] Verfügbarkeit, Unversehrtheit oder Vertraulichkeit [...]"; auch die Cybercrime Convention des Europarates basiert ausweislich ihrer Präambel auf den Sicherheitszielen „Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computersystemen".

[333] Vgl. Eckert, IT-Sicherheit: Konzepte – Verfahren – Protokolle, 2009, S. 9.

[334] Vgl. ebd., S. 10.

[335] Vgl. Brenner, Michael et al.: Praxisbuch ISO/IEC 27001. 2011, S. 4.

[336] Vgl. ebd., S. 4.

[337] S. nur Chin-Wan Chung et. al., Web Communication Technologies and Internet-Related Social Issues – HSI 2003: Second International Conference on Human Societey@Internet Band 2, 2003, S. 178 f.

[338] http://technet.microsoft.com/en-us/library/cc505924.aspx

Hacker-Community[339] ist ein gängiges Motiv. Dabei sei aber bereits an dieser Stelle betont, dass Hacker häufig auch rein legale Ziele verfolgen und nicht grundsätzlich mit Internetkriminellen gleichzustellen sind.[340]

Keine Besonderheit der Internetkriminalität, sondern vielmehr ein Charakteristikum von Kriminalität an sich, ist vorrangig die vom Motiv der finanziellen Bereicherung geleitete Tatbegehung. Gerade das Streben nach finanziellen Vorteilen ist unabhängig von technologischen Weiterentwicklungen beziehungsweise Veränderungen und bleibt vorherrschender Antrieb im Bereich der Internetkriminalität. Die Statistiken weisen darauf hin, dass die Zahl der Angriffe, die in Zusammenhang mit der Verfolgung eines monetären Ziels stehen, stetig zunimmt und sich die Vorgehensweisen der Täter weiter professionalisieren.[341] Daneben spielen aber auch ideologische oder politische Motive eine Rolle.

II.2.1.5 Bedrohungen

Die beiden oben dargelegten Motivationslinien spiegeln sich auch in den Bedrohungsarten wider, denen IT-Systeme durch kriminelle Handlungen im Wesentlichen ausgesetzt sind. Für die Täter stellt sich je nach dem Motiv ihrer Handlung die Frage nach dem wirkungsvollsten Weg zur Erreichung ihres Ziels. Die so entstehenden Bedrohungen sind äußerst vielfältig.

Folgende Bedrohungen werden dabei von Sicherheitsexperten sowohl aus der Privatwirtschaft[342] als auch seitens des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als besonders relevant angesehen[343]:

II.2.1.5.1 Botnetze

Ein Botnetz besteht aus einer großen Anzahl von miteinander vernetzten Computern, die mit einer Schadsoftware (englisch: Malware) infiziert wurden.[344] Diese Schadsoftware ermöglicht

---

[339] Taylor, Hackers – Crime in the digital sublime, 1999, S. 45 ff.

[340] S. dazu unten Abschnitt II.3.3.1; s. außerdem die beispielsweise vom Chaos Computer Club (CCC) bereitgestellte Hackerethik, abrufbar unter: http://www.ccc.de/hackerethics

[341] Kshetri, The Glocal Cybercrime Industry, 2010, S. 23 m.w.N.

[342] Hier werden insbesondere verschiedene Studien, unter anderem von IBM, dem Antivirenhersteller McAfee, der Wirtschaftsberatungsfirma KPMG und anderen, herangezogen. Alle diese Studien entsprechen nicht den Anforderungen an eine wissenschaftliche Aufarbeitung des Themas. Sie bieten jedoch einen guten Überblick.

[343] Siehe hierzu den BSI-Lagebericht „Die Lage der IT-Sicherheit in Deutschland 2011“. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile

es einem Täter, die Computer fernzusteuern und für einen Distributed Denial of Service-Angriff (DDoS-Angriff)[345] oder auch nur für den Versand von Spam zu nutzen.[346] Der Aufbau eines Botnetzes findet zumeist ungerichtet statt. Ziel der Täter ist es, eine möglichst große Anzahl an Rechnern in das Botnetz einzubinden.[347] Hierbei bedienen sie sich verschiedenster Methoden, um die Rechner mit Schadsoftware zu infizieren.[348] Wer der Besitzer des kompromittierten Systems ist, ist für den Täter nicht weiter von Bedeutung.

Die Kontrolle über ein ausreichend großes Botnetz eröffnet dem Täter vielfältige Möglichkeiten: So wurden Botnetze beispielsweise als Drohungsmittel für Erpressungen[349] genutzt, um Vergeltung auszuüben oder um Wettbewerbsvorteile zu erlangen[350]. Angesichts der massiven Schäden, die ein DDoS-Angriff für ein Unternehmen bedeuten kann, genügt in der Regel schon die Androhung eines entsprechenden Angriffs, um ein Unternehmen zur Zahlung eine Schutzgeldes zu bewegen.[351] Botnetze können auch stunden- oder tageweise[352] an Dritte vermietet werden, die diese ohne eigene technische Kenntnisse zum Spamversand oder für die genannten DDoS-Angriffe nutzen. Hieraus hat sich inzwischen ein eigenes Geschäftsmodell entwickelt.[353] Der Kunde benötigt so kaum noch eigenes vertieftes Wissen über die technischen Zusammenhänge.

Ein drittes Geschäftsmodell beim Betrieb eines Botnetzes ist der sogenannte Click Fraud. Die ferngesteuerten Computer (die Bots) werden genutzt, um massenhaft und andauernd

---

[344] S. dazu auch Walter, Internetkriminalität, 2008, S. 21, der auf eine Zahl aus dem Jahr 2007 verweist, wonach angeblich 11 % aller mit dem Internet verbundenen Computer mit Botnetz-Malware infiziert sein sollen.

[345] Ein Angriff, bei dem mittels einer Vielzahl von einzelnen Computern, die oft in ein Botnetz eingebunden sind, ein einzelnes Computersystem, in der Regel ein Server im Internet, so lange mit Anfrage überhäuft wird, bis dieser neue Anfragen nicht mehr beantworten kann. Tipton/Krause, Information Security Handbook, 2007, S. 2253; s. weiter Walter, Internetkriminalität, 2008, S. 20; näher zu dem Thema unten Abschnitt II.2.1.5.4.

[346] Pfleeger/Pfleeger, Analyzing Computer Security: A Threat / Vulnerability / Countermeasure Approach, 2011, S. 638 f.

[347] S. dazu auch Kshetri, The Global Cybercrime Industry, 2010, S. 2, der auf eine Schätzung hinweist, nach der etwa 10 Millionen Computer täglich übernommen und zu einem Bestandteil eines Botnetzes gemacht werden.

[348] Zu diesen sogleich Abschnitte II.2.1.6 und II.2.1.7.

[349] Vacca, Computer and Information Security Handbook, 2009, S. 124.

[350] Vgl. BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 15, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile

[351] S. das Beispiel bei Brauch, Geld oder Netz!, c't 14/04 sowie http://www.heise.de/security/meldung/DDoS-Angriff-vermiest-Conrad-die-Weihnachtsstimmung-1400117.html

[352] BKA, Cybercrime Bundeslagebild 2010, S. 7, abrufbar unter: http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf

[353] Walter, Internetkriminalität, 2008, S. 21.

Werbebanner anzuklicken, an deren Umsätzen der Angreifer verdient.[354] Auch die Übernahme, das so genannte „Hijacking“, eines Botnetzes ist möglich.[355]

Ein bereits angesprochener, weiterer Einsatzzweck im Bereich der Botnetze ist der Spamversand.[356] Hierbei ist der Versand von Spam zum einen das Geschäftsmodell selbst, da sich trotz der niedrigen Conversion Rate[357] durch Umsatzbeteiligung an den so verkauften Produkten weiterhin erhebliche Gewinne erzielen lassen.[358] Zum anderen dienen die versandten E-Mails auch dazu, weitere Rechner zu infizieren und dadurch zu einem Bestandteil des Botnetzes zu machen.

Der BSI-Lagebericht 2011 stellt zudem fest, dass „im Jahr 2010 zunehmend ein weiterer Trend auftrat: Beim so genannten ‘Hacktivismus‘, einer Mischform von Hacking und Aktivismus, stellen Internet-Nutzer ihre PCs freiwillig zur Verfügung, um Angriffe, beispielweise DDoS-Angriffe, auf Unternehmen durchzuführen. Auf diese Weise kann sich ebenfalls ein Botnetz bilden“.[359]

II.2.1.5.2 Identitätsdiebstahl und -missbrauch

Angriffe auf eine fremde Identität versetzen Angreifer in die Lage, sich im Internet oder innerhalb eines IT-Systems als die Person auszugeben, deren Identität sie übernehmen konnten. Die Identität lässt sich auf verschiedene Weise für den Täter nutzen. Eine der direktesten Formen ist etwa der Zugriff auf das Onlinebanking der Nutzer. Die Täter finden dabei trotz sicherheitstechnologischer Weiterentwicklungen immer wieder neue Wege zur Umgehung der Sicherheitsmechanismen. Zur Weiterleitung der unrechtmäßig erlangten Gelder ins Ausland werden so genannte Finanzagenten eingesetzt. Diese Personen werden wiederum durch Spam angeworben.[360] Auch im Bereich des Warenbetrugs spielt der

---

[354] Vacca, Computer and Information Security Handbook, 2009, S. 124.

[355] 2009 wurde beispielsweise das Torping-Botnetz für mehrere Tage von Forschern übernommen und in dieser Zeit beobachtet, vgl. Brett Stone-Gross u.a.; Your Botnet is My Botnet: Analysis of a Botnet Takeover, 2009, abrufbar unter: http://www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf

[356] Vacca, Computer and Information Security Handbook, 2009, S. 124; http://www.shadowserver.org/wiki/uploads/Information/RBN-AS40989.pdf, S. 4.

[357] Die Studie Kranich/Kreibich/Levchenko et al., Spamalytics, Proceedings of the 15th ACM conference on Computer and communications security - CCS '08, 2008 legt nahe, dass eine "conversion rate of well under 0.00001%" (S. 11) vorliegt, also mehr als einhunderttausend Spam-Mails für einen aus Sicht der Spammer erfolgreichen Abschluss nötig sind.

[358] Eingehend: Ebd.

[359] BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 15, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile

[360] Beschrieben etwa hier: BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 23, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile.

Identitätsdiebstahl eine zentrale Rolle. Zur Abholung und Weiterleitung der unter falscher Identität bestellten Waren werden wiederum so genannte „Warenagenten“ eingesetzt.[361]

Ein weiteres Feld im Bereich des Identitätsmissbrauchs ist der Missbrauch von Zahlungskarten. Nach Einschätzung des BKA hat sich hier mit dem Carding in den letzten Jahren eine neue Methode etabliert, bei der Waren unter fremder Identität gekauft und sodann von den Tätern wieder verkauft werden.[362] Auch hier kommen oftmals „Agenten“ zum Einsatz, die für die Täter die Ware abholen oder weiterversenden.

II.2.1.5.3 Spam

Von den sonstigen Bedrohungengrundsätzlich zu unterscheiden sind solche Handlungen, die zwar als sozialschädlich betrachtet werden, aber mangels des dafür erforderlichen besonderen Unrechtsgehaltes nicht ohne Weiteres als Straftaten im juristischen Sinne und damit als Internetkriminalität charakterisiert werden können. Dies sind namentlich Ordnungswidrigkeiten und bloße Belästigungen, wie beispielsweise unerwünschte Werbung im Internet und bestimmte Formen unverlangt zugestellter E-Mails. Das damit angesprochene Versenden von Spam ist zwar nicht ohne Weiteres unmittelbar als Straftat anzusehen, stellt aber etwa mit werblichem Inhalt eine Ordnungswidrigkeit nach §§ 6 Absatz 2, 16 Absatz 1 des Telemediengesetzes (TMG)[363] dar, wenn der kommerzielle Charakter oder der Absender verschleiert oder verheimlicht wird.

Daneben stellt Spam auch eine unzumutbare Belästigung nach § 7 Absatz 3 Nummer 3 und 4 des Gesetzes gegen den unlauteren Wettbewerb (UWG)[364] dar und kann damit zu einem wettbewerbsrechtlichen Unterlassungsanspruch führen. Ein solcher Unterlassungsanspruch

---

[361] S. etwa die Warnung des BSI hier: FD-StrafR 2008, 271131; weitere Beispiele: BKA, Cybercrime Bundeslagebild 2010, S. 10 ff., abrufbar unter: http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf

[362] Der Begriff Carding wird im betreffenden Bericht für eine Methode verwendet, nach der mithilfe ausgespähter oder gestohlener Kreditkarten zunächst online Waren gekauft werden, die dann von den Tätern über andere Online-Shops oder Plattformen wie eBay weiterverkauft werden, s. BKA, Cybercrime Bundeslagebild 2010, S. 12, abrufbar unter: http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf; der Begriff wird teilweise aber auch so verstanden, dass „Carding“ den Vorgang beschreibt, wenn der Dieb einer Kreditkarte durch die Abbuchung kleinerer und damit unauffälliger Beträge kontrolliert, ob die entwendete Karte bereits gesperrt oder noch nutzbar ist.

[363] Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692).

[364] Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung vom 3. März 2010 (BGBl. I S. 254).

nach §§ 823, 1004 des Bürgerlichen Gesetzbuches (BGB)[365] analog kann sich aus einer Verletzung des allgemeinen Persönlichkeitsrechts[366] oder dem Eingriff in das Recht am eingerichteten und ausgeübten Gewebetrieb[367] ergeben. Parallel können Schadensersatzansprüche nach § 823 Absatz 1 BGB entstehen. Der Durchsetzung derartiger zivilrechtlicher Ansprüche stehen aber oft praktische Gründe entgegen, da die Verfolgung langwierig, teuer und oft erfolglos ist.[368]

Größere Bedeutung hat Spam allerdings als Vorbereitungshandlung für andere Formen der Internetkriminalität. Spam wird genutzt, um Phishing einzuleiten, um Personen für den Warenbetrug anzuwerben[369] oder um weitere PC-Infektionen herbeizuführen.[370] In diesen Fällen nimmt Spam also eine vorbereitende Funktion für andere Angriffsformen ein und entfaltet damit eine mittelbare Bedrohungswirkung.[371]

Insofern war und ist Spam weiterhin die zahlenmäßig häufigste Angriffsform.[372] Durch die enorme Rechen- und Sendeleistung, die den Versendern mittlerweile zur Verfügung steht, sind Spamwellen erheblichen Ausmaßes zu beobachten.[373]

II.2.1.5.4 Professionalisierung/Organisierte Internetkriminalität

Zudem ist eine Tendenz zur Professionalisierung bei der Begehung von Straftaten aus dem Bereich der Internetkriminalität zu beobachten.

Diese Entwicklung zeigt sich am Beispiel der groß angelegten DDoS-Angriffe auf die Websites von bedeutenden Wirtschaftsunternehmen. Derartige Angriffe werden regelmäßig

---

[365] Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Artikel 1 des Gesetzes vom 10. Mai 2012 (BGBl. I S. 1084).

[366] LG Berlin NJW 1998, 3208.

[367] LG Berlin NJW 2002, 2569, 2570.

[368] Conrad, in: Auer-Reinsdorff/Conrad, Beck'sches Mandatshandbuch IT-Recht, § 25 Rn. 250.

[369] BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 20, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile Siehe auch die Ausführungen in Kaputel II.2.1.5.2.

[370] Viren können mittels Dateianhängen über E-Mails verteilt werden. Hierzu werden die selben Techniken wie beim Spamversand genutzt. Viren können so in großer Zahl verteilt werden. Zum Ganzen: Kurose/Ross, Computernetzwerke: Der Top-Down-Ansatz, 2008, S. 78.

[371] BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 20, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile

[372] S. dazu Kshetri, The Global Cybercrime Industry, 2010, S. 5, wo auf eine Schätzung von 200 Milliarden Spammails täglich und auf einen Spananteil von 87 bis 90 % bei allen E-Mails für das Jahr 2009 hingewiesen wird.

[373] S. die aufschlussreiche Grafik bei: BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 20, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile; weiter dazu Walter, Internetkriminalität, 2008, S. 20.

mit Hilfe großer Botnetze durchgeführt.[374] Zudem „sind Cyberkriminelle auf Server-Standorte angewiesen, die vor dem Zugriff der [hiesigen] Polizei geschützt sind“[375]. Eine der bekanntesten Adressen war das zwischenzeitlich inaktive Russian Business Network (RBN).[376] Dem russischen Internet-Service-Provider (ISP) und Webhoster wird von verschiedenen Seiten vorgeworfen,[377] Betreiber eines der weltweit größten Botnetze gewesen zu sein und zudem andere Formen der Internetkriminalität selbst zu betreiben oder zu ermöglichen.[378]

Die zunehmend konzertierte Art von Angriffen deutet darauf hin, dass es eine Reihe von gut organisierten Gruppen gibt, die kriminelle Handlungen vornehmen und auch entsprechende „Dienstleistungen“ anbieten.[379] Wie weit diese „Underground Economy“[380], gerade auch die Strukturen der organisierten Internetkriminalität, aber genau gediehen ist, ist bislang nicht eindeutig empirisch geklärt.

Organisierte Kriminalität wird definiert als „die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig

a) unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,

b) unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder

---

[374] Kurose/Ross, Computernetzwerke: Der Top-Down-Ansatz, 2008, S. 78; Tipton/Krause, Information Security Handbook, 2007, S. 952.

[375] BSI, Quartalslagebericht 4/2010, S. 20.

[376] Zum RBN und deren Methoden s. auch Kshetri, The Global Cybercrime Industry, 2010, S. 13.

[377] So erhob etwa VeriSign entsprechende Anschuldigungen: http://www.economist.com/node/9723768?story_id=9723768

[378] S. etwa die Berichte: http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html; http://www.shadowserver.org/wiki/uploads/Information/RBN-AS40989.pdf

[379] BKA, Cybercrime Bundeslagebild 2010, S. 7, abrufbar unter: http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf; s. auch Kshetri, The Global Cybercrime Industry, 2010, S. 1, 14.

[380] Das heißt ein globaler, virtueller Marktplatz, über den kriminelle Anbieter und Nachfrager ihre Geschäfte abwickeln, die sich um die digitale Welt drehen, zum Beispiel den Verkauf gestohlener digitaler Identitäten oder auch kompletter krimineller Infrastrukturen, s. Franosch, Schriftliche Stellungnahme zu Expertengespräch „Internetkriminalität“, S. 6. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

c) unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken".[381]

Für die Qualifizierung kriminellen Verhaltens als organisierte Kriminalität müssen alle generellen und zusätzlich mindestens eines der speziellen Merkmale der Alternativen a) bis c) vorliegen. Formen organisierter Kriminalität im Internet reichen vom gemeinschaftlich geplanten und begangenen Warenbetrug über den Missbrauch von Bankdaten bis hin zu Erpressungen. Die Täter passen sich dabei laufend an technische Entwicklungen und auch gestiegene Sicherheitsvorkehrungen gegen kriminelles Handeln an. Darüber hinaus „agieren nicht mehr wenige hochspezialisierte Straftäter, sondern überwiegend Kriminelle, die zumeist auf internationaler Ebene arbeitsteilig zusammenwirken".[382]

Neben den soeben beschriebenen Formen organisierter Kriminalität, bei denen es lediglich zu einer Verbindung der jeweils gewachsenen Strukturen der bisherigen organisierten Kriminalität und des Internets kommt, sind in den letzten Jahren auch „internetspezifische" Formen der organisierten Kriminalität entstanden.[383] Deren wesentliches Merkmal ist, dass die Defizite, die Einzeltäter in puncto Wissen oder Infrastruktur aufweisen, durch Vernetzung ausgeglichen werden. Inzwischen hat sich insofern ein Parallelmarkt entwickelt, auf dem Daten, Waren, Geschäftsmodelle und Infrastrukturen gehandelt werden. Dieser Markt orientiert sich dabei vor allem an der Nachfragesituation. Wissen und Ressourcen werden teilweise mit elektronischen Zahlungsmitteln wie Bitcoins, UKash oder Webmoney bezahlt und durch Umsatz- und Gewinnbeteiligungen abgegolten. Die Schwierigkeit für die Strafverfolgungsbehörden besteht dabei nicht zuletzt darin, dass sich innerhalb dieser

---

[381] BKA, Organisierte Kriminalität Bundeslagebild 2010, S. 9; http://www.bka.de/nn_193314/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/OrganisierteKriminalitaet/organisierteKriminalitaetBundeslagebild2010,templateId=raw,property=publicationFile.pdf/organisierteKriminalitaetBundeslagebild2010.pdf

[382] BKA, Cybercrime Bundeslagebild 2010, S. 14, abrufbar unter: http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf; so auch Franosch, Schriftliche Stellungnahme zu Expertengespräch „Sicherheit im Netz", S. 7: „Die im Phänomenbereich aktiven Täter haben heute nach den bisherigen Erfahrungen in einer Vielzahl der Fälle als Einzelpersonen oder in Kleingruppen weder das vollständige zur Tatbegehung technische und soziale Wissen / Erfahrung, noch die zur Tatbegehung notwendige (technische und finanzielle) Infrastruktur". Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

[383] Franosch, Schriftliche Stellungnahme zu Expertengespräch „Internetkriminalität", S. 7. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

dezentral organisierten Strukturen die Beteiligten in aller Regel nicht kennen, sondern auch untereinander anonym bleiben.[384]

Fallbeispiel für Professionalisierung – Aufbau eines Botnetzes:

Ein großes Botnetz bringt demjenigen, der es kontrolliert, Skalenvorteile. Ist die Anfangsinvestition (der Aufbau des Botnetzes) getätigt und hat das Netz eine kritische Masse überschritten, sinken die Kosten für jede Neuinfektion, da die bereits infizierten Computer als Mittel der Infektion genutzt werden können. Der Aufbau eines solchen Netzes verlangt indes erhebliche Investitionen. Es muss eine Sicherheitslücke gefunden werden, die im Idealfall noch nicht bekannt oder zumindest noch nicht geschlossen ist (zum so genannten „Zero-Day-Exploit“, siehe Abschnitt II.2.2.2.2), es muss eine entsprechende „Backdoor“-Software (siehe Abschnitt II.2.1.6.1, dort Abschnitt: Backdoors) geschrieben oder angepasst werden und es muss ein Infektionsweg gefunden werden. Das Ziel desjenigen, der ein solches Botnetz kontrolliert, wird es sein, die versunkenen Kosten, die der Aufbau des Botnetzes erfordert, wieder zu amortisieren.

II.2.1.6 Angriffsmittel

Im Folgenden soll ein Überblick über die wesentlichen technischen Angriffsmittel gegeben werden, die IT-Systeme gefährden können:

II.2.1.6.1 Schadsoftware

Schadsoftware (englisch: Malware) umfasst jede Art von Code, der auf einem fremden Computer das Ausführen schädlicher Funktionen durch einen Angreifer ermöglicht.[385] Innerhalb dieser sehr weiten Definition gibt es eine Reihe von Unterscheidungen:

II.2.1.6.1.1 Viren

Unter Viren werden sich selbst vermehrende Computerprogramme verstanden, deren Ziel in erster Linie die Verbreitung des eigenen Codes, also die Vermehrung und die Ausführung von Schadcode ist.[386] Das namensgebende Charakteristikum eines Virus ist, dass er sich stets eines Wirtes in Form eines anderen Programmes bedient, in dessen Programmcode er sich

[384] Ebd.

[385] Malware = Malicious Software = Bösartige Software; s. zu der Thematik auch Walter, Internetkriminalität, 2008, S. 19.

[386] Eckert, IT-Sicherheit: Konzepte – Verfahren – Protokolle, 2009, S. 45 f.

hineinkopiert und dann mit ausgeführt wird, sobald das Wirtsprogramm gestartet wird.[387] Als Wirt können alle ausführbaren Teile eines IT-Systems dienen. Hierzu gehören Programmdateien, Skripte, Makros in Dokumenten, aber auch weniger offensichtlich einsehbare Bereiche, wie Programmbibliotheken oder Bootsektoren, die für den Anwender nur schwer als ausführbarer Teil eines Programms erkennbar sind.[388]

Wird das Wirtsprogramm gestartet, laufen in aller Regel zwei Routinen ab: Zum einen die Schadroutine, die den Schadcode ausführt, und zum anderen die Verbreitungsroutine, bei der der Virus sich selbst in weitere, noch nicht infizierte Programme hineinkopiert.[389]

Die Verbreitungsmethoden von Viren hängen von der Verbreitung der Wirtsprogramme ab. Insofern ist der Weg, auf dem Viren verbreitet werden können, beliebig und korreliert regelmäßig mit der typischen Art, wie Programmcode weitergegeben wird.[390] So hat sich die Art der Verbreitung von Viren ebenso gewandelt wie die Art der Verbreitung von Programmcode. Während in der Vergangenheit noch die Weitergabe mittels Diskette oder CD-ROM üblich war, steht heute, im Internetzeitalter, die Verbreitung über E-Mails, FTP-Server, Web-Server und Filesharing-Netzwerke im Vordergrund. Viren spielen nach wie vor insbesondere in speziellen Bereichen – wie etwa bei eingebetteten Systemen oder Betriebssystemen mobiler Endgeräte – eine erhebliche Rolle.[391]

II.2.1.6.1.2 Würmer

Während Viren auf eine Verbreitung der von ihnen infizierten Dateien angewiesen sind, haben Computerwürmer die Möglichkeit, die , bereitgestellte Netzinfrastruktur des Systems, auf dem sie sich befinden, zu nutzen, um sich eigenständig über ein Netzwerk zu verbreiten.[392] So erklärt sich auch die gänzlich andere Angriffsstrategie eines Computerwurms gegenüber der eines Virus. Während der Virus zum Ziel hat, möglichst viele andere Dateien

---

[387] Slade, in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S. 256.

[388] S. zu den verschiedenen Typen von Viren: Slade, in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S. 258 f.

[389] Tipton/Krause, Information Security Management Handbook, 2007, S. 100.

[390] So lässt sich sagen, dass die Weitergabe eines Virus noch immer der Interaktion eines Menschen bedarf. Vacca, Computer and Information Security Handbook, 2009, S. 56.

[391] Auch das Überspringen eines Virus vom PC auf ein mobiles Endgerät stellt technisch kein Problem dar, auch wenn derartige Fälle in der Praxis, soweit ersichtlich, noch nicht beobachtet wurden, s. BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 25, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile; zumindest für den Bereich der Privatanwender gilt, dass Virenscanner einen durchaus effektiven Schutz bieten, sofern sie den Vorgaben entsprechend eingesetzt werden. S. hierzu Pfleeger/Pfleeger, Analyzing Computer Security: A Threat / Vulnerability / Countermeasure Approach, 2011, S. 159 f.

[392] Slade, in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S. 256, S. 255.

zu infizieren, da so die Wahrscheinlichkeit steigt, auf ein anderes, noch nicht infiziertes System übertragen zu werden, nisten sich Würmer in den meisten Fällen unauffällig im System ein. Je länger der Wurm unbemerkt bleibt, umso größer ist der Erfolg, der in der Ausführung des Schadcodes und in der Weiterverbreitung des Wurms liegt.[393] Das Gefahrenpotenzial von Würmern steigt noch immer. Dies ist zum einen auf die immer ausgefeiltere Technik, mit der diese zur Umgehung von Sicherheitsmechansimen programmiert werden, zurückzuführen; zum anderen auf die immer weitere Verbreitung von Internetanschlüssen und damit auch von Würmern.

II.2.1.6.1.3 Trojaner

Ein Trojaner, auch Trojanisches Pferd genannt, ist eine Software, welche vom Benutzer im Glauben ausgeführt wird dass es sich um ein nützliches Programm handele.[394] Auf diese Weise implementiert sich ungewollt ein Schadprogramm. Heutige Varianten sind häufig sehr flexibel. Teilweise bieten sie die Möglichkeit, Schadcode nachzuladen und damit durch zusätzliche Funktionen mehr Schaden anzurichten; sie können sich nicht selbst verbreiten.[395] Die Grenzziehung zwischen Viren und Trojanern ist nicht trennscharf, aber auch nicht erforderlich. Zu den häufigsten Funktionen gehören das Ausspionieren von Daten sowie das Überwachen von Benutzereingaben wie Passwörtern. Oftmals enthalten Trojaner auch Backdoor-Funktionalitäten.[396]

II.2.1.6.1.4 Backdoors

Eine Backdoor ermöglicht den alternativen, unüblichen Zugang zu einem IT-System,[397] den ein Hersteller setzen oder ein feindlicher Angreifer hinzufügen kann. Mittels einer solchen Hintertür erhält ein Angreifer Zugriff auf das fremde System und kann mit ihm umgehen, als sei er ein berechtigter Benutzer.[398] Zu den typischen Schadroutinen gehört hier das Nachladen weiterer schädlicher Software sowie das Löschen oder Verändern bestehender Dateien. Darüber hinaus dienen Backdoors auch dem Ausspähen von Benutzereingaben wie

---

[393] Pfleeger/Pfleeger, Analyzing Computer Security: A Threat / Vulnerability / Countermeasure Approach, 2011, S. 136 f.

[394] Der Begriff Trojaner wird nicht einheitlich gebraucht. Oftmals werden auch Schadprogramme mit der Funktion einer Backdoor auch dann als Trojaner bezeichnet, wenn sie sich gerade nicht den Anschein von sinnvoller Software geben. Dies ist jedoch angesichts der mythologischen Herleitung ungenau. Indes enthalten Trojaner regelmäßig Backdoorfunktionalität, und Backdoorsoftware kommt als Trojaner auf den Computer. So wie hier etwa auch Newman, Computer Security, 2010, S. 40.

[395] Vgl. https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/g/g05/g05021.html

[396] Tanenbaum, Moderne Betriebssysteme, 2009, S. 772 ff.; s. weiter im Anschluss.

[397] Whitman/Mattord, Principles of Information Security, 2009, S. 58 f.

[398] Vacca, Computer and Information Security Handbook, 2009, S. 295.

Passwörtern, dem Versenden von Spam oder auch dem Ausführen eines DDoS-Angriffs. Backdoors sind im Zusammenspiel mit anderen Techniken von erheblichem Gefährdungspotenzial. So können mittels eines auf dem Computer installierten Backdoorprogramms in Verbindung mit einem gezielten Phishing-Angriff Schutzmechanismen des Onlinebanking, wie etwa das indizierte Transaktionsnummern(iTAN)-Verfahren, außer Kraft gesetzt werden.[399]

Im Bereich Backdoors ist ebenfalls relevant, dass ein Großteil der IT-Produkte inzwischen in Ländern hergestellt und/oder entwickelt wird, in denen die politische Lage nicht ausschließen lässt, dass Hintertüren bereits bei der Entwicklung und Produktion in die Hard- oder Software implementiert werden. Das betrifft nicht nur Produkte für einzelne IT-Systeme, sondern auch Netzwerkkomponenten wie beispielsweise die in Unternehmensnetzwerken oder in den Backbone-Netzen des Internets eingesetzten Router.

Zur Verdeutlichung kann darauf verwiesen werden, dass in den vergangenen Jahren eine Reihe von Fällen „verborgener Hintertüren“ sowohl im Hardware- als auch im Software-Bereich öffentlich geworden ist.

Dass typischerweise in größeren Stückzahlen bestellte Technologie wie Computerchips nicht mehr einzeln getestet werden können, begünstigt den Einbau von Hintertüren. 2011 wurde etwa bekannt, dass 59 000 Mikrochips aus China, die von der US-Armee gekauft worden waren, eine Hintertür enthielten. Diese hätte das Abschalten der Chips aus der Ferne ermöglicht.[400] Wie man solche Hintertüren auffindet, ist daher seit Jahren Teil wissenschaftlicher Forschung.[401]

Im Januar 2012 wurde bekannt, dass die Hersteller RIM, Nokia und Apple den indischen Behörden über eine Hintertür Zugang zu Inhalten von Mobilkommunikation verschafft haben. Die Hersteller räumten die Zusammenarbeit mit den staatlichen Behörden und Militärs ein.[402]

---

[399] BKA, Cybercrime Bundeslagebild 2010, S. 10, abrufbar unter: http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf

[400] S. Johnson, „The Navy Bought Fake Chinese Microchips That Could Have Disarmed U.S. Missiles“, abrufbar unter: http://www.businessinsider.com/navy-chinese-microchips-weapons-could-have-been-shut-off-2011-6

[401] S. Adee, „The Hunt for the Kill Switch”, abrufbar unter: http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0

[402] S. „Nokia and Apple have provided the Indian Military with backdoor access to cellular surveillance”, abrufbar unter: http://www.terminalx.org/2012/01/blackberry-nokia-and-apple-have.html

Zudem werden heute neben den Backdoors auch sogenannte Bugdoors verwendet, da die Ausnutzung einer absichtlich nicht geschlossenen Sicherheitslücke weniger riskant ist als das direkte Hinterlassen einer Hintertür. Bugdoors werden ebenfalls von den Herstellern implementiert und können wie „verborgene Hintertüren“ benutzt werden. Vergleichbares gilt für von Herstellern vergebene Passwörter, die eine ähnliche Wirkung wie eine Hintertür entfalten können.

II.2.1.6.1.5 Rootkits

Mit den Backdoors verbunden ist die Funktion der Rootkits, die in erster Linie dazu dienen, nach dem Kompromittieren des Systems die Entdeckung des Angriffs zu verhindern.[403] Hierzu können unberechtigte Anmeldevorgänge verborgen sowie Prozesse und Dateien vor dem Benutzer, aber auch vor Virenscannern versteckt werden. Merkmal von Rootkits ist, dass sie im Vergleich zu anderer Schadsoftware wesentlich tiefer in das System eingreifen, was ein Entdecken und Löschen schwierig bis fast unmöglich macht.[404]

II.2.1.6.1.6 Spyware

Der Begriff Spyware umfasst Schadsoftware, die darauf ausgelegt ist das Nutzerverhalten aufzuzeichnen und diese Daten an den Angreifer oder Dritte zu senden, regelmäßig um personalisierte Werbung zu ermöglichen oder Marktforschung zu betreiben.[405] Oft werden diese Informationen in Datenbanken gesammelt und genutzt, um gezielt Benutzerprofile zu erstellen.[406]

Spyware wird in den meisten Fällen als Trojanisches Pferd zusammen mit einer (vermeintlich) nützlichen Software installiert. Außerdem wird Spyware auch mittels Drive-by-Download unter Ausnutzung einer Sicherheitslücke im Browser oder eines Plug-Ins installiert.[407]

II.2.1.6.2 Andere Angriffsmethoden

Es gibt noch eine Reihe weiterer Angriffsmethoden. Einen Schwerpunkt bilden Vorgänge zur Erlangung von Passwörtern oder ähnlichen Daten, um so die spätere Kompromittierung des Systems erst zu ermöglichen.

---

[403] Sehr ausführlich: Tanenbaum, Moderne Betriebssysteme, 2009, S. 795 ff.

[404] Sehr ausführlich: Ebd.

[405] Tipton/Krause, Information Security Management Handbook, 2007, S. 663.

[406] Erbschloe, Trojans, Worms, and Spyware; A Computer Security Professionals Guide to Malicious Code, 2005, S. 26 f.

[407] Zu dieser Problematik näher unten Abschnitt II.2.1.7.1.

So kann etwa mittels Packet Sniffing der gesamte Verkehr eines Netzwerks „mitgehört“ werden. Dies ist für Angreifer besonders dann von Interesse, wenn Übertragungsprotokolle im Einsatz sind, bei denen der Datenverkehr – und insbesondere auch die Passwörter – unverschlüsselt übertragen werden.[408] Ein offenes oder nicht mit einem ausreichend starken Passwort verschlüsseltes WLAN stellt so ein erhebliches Sicherheitsrisiko dar. Während offene WLANs im Unternehmens- und Privatbereich[409] inzwischen eher die Ausnahme sein dürften, finden sich öffentliche HotSpots etwa in Cafés oder Hotels. Der Angriff auf die Datenströme von Computern eines solchen öffentlichen HotSpots ist, sofern bei der Nutzung des HotSpots keine Verschlüsselungstechniken genutzt werden, auch für technisch weniger versierte Angreifer mittels im Internet angebotener Tools leicht möglich. Hier steht zu erwarten, dass die Angriffe noch vielfältiger werden. Immer öfter werden auch wichtige Geschäftsdaten unterwegs bearbeitet und versendet und werden so zum möglichen Ziel von Sniffing.[410]

Ebenfalls zu den nutzbaren Mitteln technisch wenig versierter Angreifer gehören so genannte Vulnerability Scanner. Diese Programme dienen dem Zweck, ein Zielsystem auf das Vorhandensein von bekannten Sicherheitslücken zu untersuchen. Gedacht sind sie in erster Linie zur Absicherung des eigenen Systems. In dieser Funktion haben sie in der IT-Sicherheit auch erhebliche Bedeutung.[411] Ein Missbrauch lässt sich jedoch nicht ausschließen.

II.2.1.7 Infektions- und Angriffspunkte

Die Täter von Internetkriminalität machen sich sicherheitstechnische Schwachstellen zunutze. In diesem Zusammenhang sind vor allem folgende Punkte zu nennen:

---

[408] Erickson, Hacking: The Art of Exploitation, 2008, S. 226 ff.

[409] Dies ist wohl auch darauf zurückzuführen, dass praktisch alle Router heute mit einer Anwendersoftware ausgeliefert werden, die bei der ersten Einrichtung des Routers automatisch ein sicheres Passwort wählt.

[410] S. auch BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 34, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile Hiernach wissen lediglich rund 60 % der vom BSI befragten Nutzer, dass ihre mobilen Endgeräte die gleichen Sicherheitsanforderungen haben wie ein PC. Einer Studie im Auftrag der Wirtschaftsberatungsfirma KPMG zufolge (The e-Crime Report 2011), werden geschäftliche Mobiltelefone wesentlich häufiger verloren als private (http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/Advisory/ecrime-report-2011-accessible-2.pdf, S. 15). Dies alles mag als Hinweis darauf verstanden werden, wie sorglos Nutzer immer noch dem Trend zu mehr Mobilität gegenüberstehen.

[411] So bietet auch das BSI eine Live CD mit der Sicherheitssoftware OpenVAS, zu deren Bestandteilen auch ein Vulnerability Scanner gehört.

II.2.1.7.1 Sicherheitslücken von Software

Das wohl am ehesten mit Internetkriminalität assoziierte und auch bislang das häufigste Verfahren des Einbruchs in ein System ist das Ausnutzen einer Sicherheitslücke (englisch: exploit), die aufgrund von Programmierfehlern in einem Programm enthalten ist.[412] Trotz der wohl recht hohen Dunkelziffer weisen Statistiken des BSI darauf hin, dass die Zahl der veröffentlichten Sicherheitslücken in Software nach wie vor als hoch einzustufen ist und die Zahl der vom Bürger-CERT[413] gemeldeten Sicherheitslücken zumindest zwischen 2008 und 2010 eine ansteigende Tendenz aufweist.[414] Besonders relevant im Bereich dieser Sicherheitslücken, wenn auch mit abnehmender Tendenz, sind Drittanbieter-Web-Anwendungen.[415] Mit dem zunehmenden Bedürfnis eines interaktiven Internets müssen Techniken jenseits der reinen Auszeichnungssprache HTML verwendet werden. Bereits frühzeitig wurden verschiedene Techniken für aktive Inhalte entwickelt, die Erweiterungen des Browsers darstellen und es erlauben, dynamisch auf Benutzeraktionen zu reagieren. Dieser eingebettete Code wird lokal auf dem Rechner des Nutzers ausgeführt. Browser-Plug-Ins[416], sind daher bei Virenautoren beliebte Ziele und werden besonders oft angegriffen. Insbesondere ist ein Anstieg an neu bekannt werdenden Sicherheitslücken bei Rich Media-Anwendungen[417] zu beobachten. So gehört derzeit etwa der Adobe Flash Player zu den Programmen, in denen besonders viele Sicherheitslücken bekannt wurden.[418] Zusammen mit den ohnehin bereits in den Browsern und Betriebssystemen vorhandenen Sicherheitslücken[419] kumulieren sich damit die Schwachstellen beim Einsatz der Software.

---

[412] Gaycken, Cyberwar, 2011, S. 54.

[413] Das Bürger-CERT (Computer Emergency Response Team) ist eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) betriebene Plattform und dient der Warnung von Bürgerinnen und Bürgern sowie kleinen Unternehmen vor Viren, Würmern und Sicherheitslücken in Software. Das Bürger-CERT ist online erreichbar unter: https://www.buerger-cert.de/

[414] BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 6, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile

[415] BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 6, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile

[416] Ein Browser-Plug-In ist eine Software eines Drittanbieters, die dazu dient, die ursprüngliche vom Hersteller eines Browser vorgegebene Funktionalität zu erweitern.

[417] Unter Rich Media werden multimediale und interaktive Inhalte wie beispielweise Videos und Animationen verstanden.

[418] BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 6, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile; IBM X-Force 2011 Mid-Year Trend and Risk Report, S. 67, abrufbar unter: http://www-935.ibm.com/services/us/iss/xforce/trendreports

[419] Beispielsweise wurden für Mozilla Firefox 2011 60 Schwachstellen entdeckt, welche die Ausführung von Schadcode ermöglichen, s. dazu BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 6, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile

Eine weitere Form des Ausnutzens von Sicherheitslücken ist der Drive-by-Exploit. Hierbei werden insbesondere auch Sicherheitslücken in Software wie etwa Browsern, in Adobe Flash sowie in der Java-Laufzeitumgebung ausgenutzt. Die besondere Gefahr von Drive-by-Exploits liegt darin, dass die Infektion des Computers herbeigeführt werden kann, ohne dass eine willentliche Interaktion des Benutzers mit der Quelle der Schadsoftware vorliegt. Eine Infektionsquelle kann beispielsweise eine manipulierte Website sein, auf die der Benutzer mittels Spam gelockt wird. Aber auch über eine dem Anwender bereits bekannte Website kann eine Infektion erfolgen, falls diese als Folge eines Angriffs auf den hostenden Webserver manipulierte wurde.

II.2.1.7.2 Social Engineering und Phishing

Social Engineering unterscheidet sich fundamental von den anderen beschriebenen Techniken und ist gleichzeitig integraler Bestandteil zahlreicher Angriffe. Social Engineering bezeichnet einen Angriff auf ein IT-System, welcher nicht vorrangig auf technischen Mitteln, sondern vielmehr auf der Beeinflussung eines Anwenders beruht.[420] Dabei stehen neben zunehmend raffinierteren technischen Kenntnissen vor allem auch psychologische und sprachliche Fähigkeiten der Angreifer im Mittelpunkt, um etwa bei einem Opfer falsches Vertrauen zu erzeugen und so die gewünschten Informationen zu erhalten.[421] Analysten gehen davon aus, dass Social Engineering mit der weiterhin zunehmenden Popularität von sozialen Netzwerken noch weiter an Bedeutung gewinnen wird.[422] Die Gefahr, die von Social Engineering ausgeht, ist insbesondere deshalb als relevant anzusehen, weil es kaum technische Schutzmittel gegen diese Form des Angriffs gibt. Bei sowohl technisch als auch psychologisch hinreichend ausgeklügelten Social-Engineering-Angriffen stellt sich die Erkennung eines Angriffs selbst für versierte und computeraffine Nutzer als Herausforderung dar.

Im Bereich des Social Engineering ist auch das Phishing anzusiedeln. Ein Phishing-Angriff funktioniert üblicherweise so, dass der Angreifer eine bekannte Website möglichst detailgetreu nachbaut. Hierbei versucht er, die Website unter einer Domain abzulegen, die der Domain der Originalwebsite ähnelt, beispielsweise durch das Vertauschen eines Buchstabens. Nun sendet er eine große Anzahl an E-Mails an beliebige Empfänger. Hierfür werden regelmäßig Botnetze oder ähnliche Spamstrukturen benutzt. In diesen E-Mails, die durch ihr

---

[420] Vacca, Computer and Information Security Handbook, 2009, S. 55; s. dazu auch Kshetri, The Global Cybercrime Industry, 2010, S. 10.

[421] Kshetri, The Global Cybercrime Industry, 2010, S. 10.

[422] The e-Crime Report 2011, S. 13, abrufbar unter: http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/Advisory/ecrime-report-2011-accessible-2.pdf

Design und ihre Absenderkennung den Anschein erwecken sollen, sie kämen von dem Betreiber der eigentliche, echten Website,[423] wird der Benutzer aufgefordert, aus einem wichtigen Grund einem Link in der E-Mail zu folgen und auf der so besuchten Seite seine Daten einzugeben. Folgt der Benutzer dieser Aufforderung, werden seine Daten vom Täter abgefangen. Dies kann vom vergleichsweise harmlosen Identitätsdiebstahl in sozialen Netzwerken bis hin zu erheblichen Vermögensschäden reichen, wenn etwa das Onlinebanking eines Benutzers betroffen ist. Hierbei hat allerdings nach Informationen des BSI diese einfache Form des Phishing zumindest im Bereich des Onlinebanking fast vollständig an Bedeutung verloren.[424] Einige Studien legen nahe, dass sich das Phishing von der E-Mail-Kommunikation auf soziale Netzwerke und Instant-Messaging ausgebreitet hat.[425]

Phishing in seiner klassischen Form eines sehr breit angelegten Angriffs, bei dem aufgrund der schieren Anzahl an versuchten Angriffen irgendwann ein Erfolg erzielt wird, ähnelt praktisch nur dem Namen nach dem neueren Spear Phishing. So werden die nach Einschätzung von Sicherheitsexperten zunehmend auftretenden, sehr gezielten und oftmals sehr gut vorbereiteten Angriffe genannt, welche auf ein bestimmtes Opfer zugeschnitten sind.[426]

Ein weiteres Beispiel für Social Engineering ist die so genannte Scareware. Dabei handelt es sich um Software, die dem Benutzer eine Bedrohung seines Computers vorgaukelt, wie beispielsweise einen Virenbefall. Auf diese Weise will man den Benutzer zu einer bestimmten Aktion bewegen, wie dem kostenpflichten Download eines Antivirenprogramms zur Bereinigung des Computers. Bei diesen Programmen handelt es sich oftmals um Trojaner mit Backdoor-Funktionalität[427]. Grundsätzlich gehören auch solche Trojaner in den Bereich des Social Engineering.

---

[423] Der Absender einer E-Mail ist einfach zu fälschen. Für den Laien sind solche Fälschungen kaum auszumachen. Hierzu und zum Ganzen: Jahankhani/Watson/Me, Handbook of Electronic Security and Digital Forensics, S. 401.

[424] BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 23, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile

[425] IBM X-Force 2011 Mid-Year Trend and Risk Report, S. 18, abrufbar unter: http://www-935.ibm.com/services/us/iss/xforce/trendreports/

[426] Ebd., S. 22. Sowie: The e-Crime Report 2011, S. 13, abrufbar unter: http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/Advisory/ecrime-report-2011-accessible-2.pdf

[427] Vgl. zum Beispiel Heise News: BKA hilft bei Zerschlagung von Scareware-Bande. 23. Juni 2011. Online abrufbar unter: http://www.heise.de/newsticker/meldung/BKA-hilft-bei-Zerschlagung-von-Scareware-Bande-1266523.html

II.2.1.7.3 Ausnutzen des Anwenderverhaltens/Fehlendes Sicherheitsbewusstsein

Große Sicherheitsrisiken bei IT-Systemen basieren darüber hinaus regelmäßig auf dem Verhalten der Anwender. Diese sorgen in vielen Fällen unbewusst dafür, dass auch die am besten ausgearbeitete Sicherheitsstrategie scheitert.[428]

Dabei spielt häufig auch unachtsames und von fehlendem Risikobewusstsein geprägtes Verhalten eine Rolle (siehe dazu das Fallbeispiel zu manipulierter Hardware). Dazu zählt auch das Nichtdurchführen von Systemupdates trotz bereits erfolgter Bereitstellung von Seiten der Hersteller/Produzenten,[429] sowie das unachtsame Installieren von Drittanbietersoftware, beziehungsweise die unachtsame Rechtezuweisung an diese und die Ignorierung von Warnhinweisen.[430]

Fallbeispiel – manipulierte Hardware:

Mittels manipulierter Computermäuse, die im Rahmen eines Tests als vermeintliches Geschenk an die Mitarbeiter einer Firma geschickt wurden, konnte ein Angriff auf Firmennetzwerke erfolgreich vorgetragen werden. Die Mäuse enthielten einen Mikrocontroller, der bei Anschluss an die USB-Schnittstelle des Computers einen Trojaner auf den Rechner schleuste. Erfolgreich war der Angriff auch deshalb, weil die von dem angegriffenen beziehungsweise getesteten Unternehmen mit der Überprüfung des Sicherheitskonzepts beauftragte Firma den Trojaner speziell auf die verwendete Virenscanner-Software zuschneiden konnte, da Mitarbeiter sich vorher öffentlich auf Facebook über das Programm beschwert hatten.[431] Ähnliche Fälle sind schon des Öfteren bekannt geworden. Auch andere der oben genannten Methoden setzen die Interaktion des Anwenders voraus.

II.2.1.7.4 Sonderproblem: Anbieter-/Produzentenverhalten

Gerade – aber nicht ausschließlich – im Bereich der Betriebssysteme für mobile Endgeräte zeigt sich ein Problem, dass selbst grundsätzlich sorgfältig mit der Sicherheit ihrer Systeme umgehenden Nutzern keine Möglichkeit an die Hand gegeben wird, ihrer Sorgfalt überhaupt erst nachzukommen, da die Anbieter/Produzenten der Produkte gar keine oder nur stark

---

[428] Gaycken, Cyberwar, 2011, S. 52.

[429] Für mobile Endgeräte s. BSI, Lagebericht 2011, S. 18, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile

[430] Ebenf. für mobile Endgeräte s. Eckert, IT-Sicherheit, 7. Aufl. 2012, S. 87 f.

[431] http://www.spiegel.de/netzwelt/web/0,1518,772462,00.html

verzögert Updates zur Verfügung stellen.[432] Damit bleiben die bereits bekannten Sicherheitslücken entweder dauerhaft oder zumindest für eine lange Zeit im System. Für die Anwender verbleibt dann lediglich die Möglichkeit, auf die Nutzung der Geräte mit dem veralteten System zu verzichten, sofern nicht zumindest zwischenzeitig vom Hersteller ein Workaround als provisorische Lösung zur Wiederherstellung der Sicherheit angeboten wird.

II.2.2 Schutzmöglichkeiten

Im Folgenden sollen überblicksartig grundsätzliche Schutzmöglichkeiten gegen die genannten Bedrohungen aufgeführt werden. Als Orientierungspunkte dienen dabei die identifizierten Schwachstellen, die zu einer Gefährdungslage führen, beispielsweise das mangelnde Sicherheitsbewusstsein der Nutzerinnen und Nutzer.

II.2.2.1 Motivation der Angreifer verringern

Wie bereits in Kapitel II.2.1.4 dargelegt, sind die Täter zum einen durch die Herausforderung motiviert, die der Einbruch in ein fremdes System bietet; zum anderen spielen monetäre Motive eine zentrale Rolle.

Die dualistische Motivationslage im Falle von Internetkriminalität birgt das Risiko eines Paradoxons: Während Täter mit monetären Motiven von einem hohen Aufwand abgeschreckt werden, erhöht sich, wie Studienergebnisse belegen,[433] die Motivation der intrinsisch handelnden Täter, gerade in diese noch besser geschützten Systeme einzubrechen.

Ökonomisch motivierte Täter haben den Vorteil, dass das Internet als globalisierter Handlungsraum nicht über kontrollierbare Grenzen verfügt, an denen Finanzströme ohne Weiteres abgefangen werden können. Sie verfügen über Methoden, Finanzmittel etwa mit Hilfe von Mittelspersonen aus einem Graubereich in den Wirtschaftskreislauf zu überführen.[434] Eine Verfolgbarkeit dieses Finanzstroms ist – wenn überhaupt – nur sehr schwer möglich.

---

[432] Zur Updateproblematik bei mobile Endgeräten s. Eckert, IT-Sicherheit, 7. Aufl. 2012, S. 88; s. weiter Wirtgen, Warum Android-Smartphones so selten Updates bekommen, 2011, abrufbar unter: http://www.heise.de/mobil/artikel/Warum-Android-Smartphones-so-selten-Updates-bekommen-1337858.html

[433] Basamanowicz/Bouchard, Overcoming the Warez Paradox: Online Piracy Groups and Situational Crime Prevention, Policy & Internet 3, no. 2, 2011, S. 2. m.w.N.

[434] Siehe hierzu auch die Ausführungen in Kapitel II.2.1.5.2.

II.2.2.2 Beseitigung oder Reduzierung von Infektions- und Angriffspunkten

Zahlreiche IT-Risiken sind systemischer Natur, das heißt isoliert betrachtet stellen sie kein Risiko dar, wohl aber im Zusammenwirken. Hat ein Angreifer es etwa geschafft, die Daten innerhalb eines Systems zu kompromittieren, verliert jeder Authentifizierungsmechanismus seinen Wert. Die bloße Absicherung nur eines Teilbereichs eines IT-Systems ist unzureichend, um den Schutz zu gewährleisten.[435] Der Aufbau einer sicheren IT ist eine komplexe Aufgabe. Es bedarf einer konzertierten Strategie, um tatsächlich alle möglichen Angriffspunkte abzusichern. Grundlage sind die bereits oben genannten Ziele der IT-Sicherheit.[436] Als maßgeblich in diesem präventiven Bereich dürfen die vom BSI entwickelten IT-Grundschutz-Kataloge gelten, welche in den Abschnitten M1 bis M5 (Maßnahmenkataloge) umfangreiche Programme zur Vorsorge gegen IT-Risiken enthalten.[437] Diese betreffen die IT-Infrastruktur, organisatorische und personelle Maßnahmen auf Unternehmensebene sowie Maßnahmen in Bezug auf Hardware und Software.

II.2.2.2.1 Bereitstellung und Installation von Patches

Da Sicherheitslücken in Software nach wie vor der zentrale Angriffspunkt für eine Infektion von Computern sind, stellt die Bereitstellung und das zeitgerechte Einspielen von Softwarekorrekturen, so genannten Patches, zum Schließen dieser Lücken eine der wichtigsten Aufgaben im Rahmen der Sicherungsmaßnahmen dar. Als im Jahre 2003 der SQL Slammer Wurm Schäden in Höhe von geschätzt einer Milliarde Euro verursachte,[438] hatte Microsoft für die Sicherheitslücke, die der Wurm zur Verbreitung nutzte, bereits sechs Monate zuvor einen Patch ausgeliefert.[439] Nach Schätzungen der amerikanischen Ermittlungsbehörde Federal Bureau of Investigation (FBI) und der Carnegie Mellon University sind 90 Prozent aller Sicherheitsbrüche auf die Ausnutzung von Sicherheitslücken zurückzuführen, für die bereits ein Patch verfügbar war.[440] Wie bereits erwähnt, gibt es aber

---

[435] Eckert, IT-Sicherheit: Konzepte – Verfahren – Protokolle, 2009, S. 38, die sehr anschaulich die Beschreibung einer Kette wählt, die immer nur so stark ist wie ihr schwächstes Glied.

[436] S. oben Abschnitt II.2.1.3.

[437] BSI, IT-Grundschutz-Kataloge, Stand: 12. EL (Sep. 2011), abrufbar unter: https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf

[438] http://news.cnet.com/2009-1001-983540.html

[439] Tipton/Krause, Information Security Management Handbook, 2007, S. 179.

[440] Ebd.

auch IT-Systeme, insbesondere im mobilen Bereich, für die die Hersteller der Geräte ihren Kunden entweder keine oder extrem verspätet Updates zur Verfügung stellen.[441]

II.2.2.2.2 Entwicklung sicherer Software

Je komplexer die Software wird, desto schwieriger wird es, einen Programmcode zu schreiben, der frei von Fehlern ist.[442] Durch die Tendenz zur steigenden Komplexität und durch modulare Entwicklungsmodelle steigt die Zahl der Sicherheitslücken sowohl absolut als auch relativ.[443] Besonders kritisch ist die Ausnutzung von Zero-Day-Exploits,[444] wofür jedoch Programmierkenntnisse erfordern sind. Zero-Day-Exploits werden auch gehandelt.[445] Gegen die Ausnutzung dieser zuvor nicht bekannten Lücken durch regelmäßig hochgradig professionelle Angreifer ist eine Verteidigung praktisch nicht möglich. Hiergegen hilft bestenfalls und auch nur bedingt der Einsatz ausführlich getesteter Software. Nach Einschätzung des BSI haben die Software-Hersteller „ihre Mitverantwortung für die IT-Sicherheit erkannt und arbeiten aktiv daran, ihre Produkte zu verbessern. Sicherheitslücken werden deshalb nicht mehr nur ausschließlich von Dritten ‚entdeckt', sondern auch von den Herstellern selbst gemeldet. Zeit bleibt aber nach wie vor ein kritischer Faktor. Zero-Day-Angriffe [...] sind mittlerweile die Regel".[446]

II.2.2.2.3 Schulung der Nutzer

Wie dargestellt, ist oftmals der Nutzer die zentrale Schwachstelle, nicht nur im Fall des Social Engineering. Oftmals wird die schädliche Software vom Nutzer selbst installiert, weil sie eine bestimmte Funktion verspricht.[447] Dieses Problem verschärft sich mit der zunehmenden

---

[441] Zu Sicherheitslücken etwa bei Geräten mit dem mobilen Betriebssystem Android von Google s. u.a. http://heise.de/-1389329; http://heise.de/-1353977; http://heise.de/-1399337; zu Problemen beziehungsweise Verzögerungen bei Updates für das Android Betriebssystem s. u.a. Eckert, IT-Sicherheit, 7. Aufl. 2012, S. 88; s. ebenf. http://heise.de/-1247850; s. vor allem zu der deutlich stärken Verbreitung von bereits veralteten System-Versionen http://developer.android.com/resources/dashboard/platform-versions.html

[442] Zum Problem der steigenden Komplexität von Software s. Schulze, Bedingt abwehrbereit, 2006, S. 75 ff. m.w.Nachw.

[443] Gaycken, Cyberwar, 2011, S. 55.

[444] S. oben Abschnitt II.2.1.5.4. Allgemein zu Zero-Day-Exploits und Angriffsablauf vgl. Pohl, Hartmut: Zero-Day und Less-than-Zero-Day Vulnerabilities und Exploits. Risiken unveröffentlichter Sicherheitslücken. In: Zacharias, Christoph u.a. (Hrsg.): Forschungsspitzen und Spitzenforschung. Heidelberg 2009, S. 113-123.

[445] Vgl. ebda., S. 115 f. Die Aussagen insbesondere über Preise basieren zumeist auf Vermutungen. Vgl. http://www.heise.de/security/meldung/Spekulationen-ueber-Schwarzmarktpreise-fuer-Exploits-1190694.html, http://securityevaluators.com/files/papers/0daymarket.pdf

[446] BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 6, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile

[447] Beliebt sind etwa Mini-Spiele. Insbesondere auf Mobilen Geräten stellen die angebotenen Apps eine Gefahr dar. Ein Beispiel findet sich im IBM X-Force 2011 Mid-Year Trend and Risk Report, S. 79, abrufbar unter: http://www-935.ibm.com/services/us/iss/xforce/trendreports/

Bedeutung von Drive-by-Infections und ähnlicher Bedrohungen. Während in einem Unternehmensumfeld den normalen Benutzern die Installation von Fremdsoftware regelmäßig nicht möglich sein sollte, kann die Nutzung des Browsers zumeist schon deshalb nicht verhindert werden, weil dieser regelmäßig für die Arbeit benötigt wird. So erfreuen sich browserbasierte Spiele, die auf Adobe Flash basieren, auch auf Computern des Arbeitgebers großer Beliebtheit. Adobe Flash ist jedoch, wie bereits oben dargelegt,[448] durch eine Reihe von Sicherheitslücken betroffen. Auch sind es oftmals die Benutzer, die gängige Sicherheitshinweise ignorieren oder nicht kennen.

II.2.2.2.4 Nutzung sicherer IT-Systeme

Die Nutzung sicherer IT-Systeme ist eng mit den vorgenannten Strategien verknüpft. Gemeint sind der Einsatz und die Pflege eines umfassenden Sicherheitskonzepts. Ein solches Konzept muss sowohl auf Hard- und Softwareebene als auch auf der Ebene der Nutzer ansetzen. Die soeben beschriebenen Maßnahmen müssen koordiniert werden. Dies ist eine komplexe Aufgabe, die von speziell geschultem Personal wahrgenommen werden muss. Die Aufgaben reichen von der Entwicklung eines Schutzkonzepts bis hin zur Überwachung der Umsetzung und Schulung der Nutzer. Nicht in jedem Bereich kann ein Maximum an Sicherheit gefordert werden, da die Kosten für nur geringe Sicherheitszunahmen ab einem gewissen Punkt exponentiell steigen können.

II.2.2.3 Reaktion auf akute Bedrohungen

Die Erfahrung zeigt, dass eine Bedrohung, wenn sie erst einmal aufgekommen ist, durch konzertierte Maßnahmen auch sehr schnell wieder eingedämmt werden kann.[449] Vorausgesetzt, Update-Mechanismen werden genutzt und Patches eingespielt, kann eine Sicherheitslücke oftmals nur wenige Tage bekannt sein, bevor die durch sie verursachte Bedrohung wieder beseitigt wird.[450] Hierfür erscheint es jedoch erforderlich zu sein, dass möglichst viele Stellen eng zusammenarbeiten und ihre Kenntnisse austauschen. Dies schließt sowohl private als auch staatliche Stellen ein.[451] Auch zur Verbesserung des

---

[448] S. oben Abschnitt II.2.1.7.1.

[449] S. etwa das aufschlussreiche Beispiel hier: http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/02/24/cracking-down-on-botnets.aspx , sowie die Beispiele im IBM X-Force 2011 Mid-Year Trend and Risk Report, S. 45, abrufbar unter: http://www-935.ibm.com/services/us/iss/xforce/trendreports/

[450] Gaycken, Cyberwar, 2011, S. 52.

[451] S. auch die Hinweise des BSI zu dem Thema: BSI, Lagebericht IT-Sicherheit in Deutschland 2011, S. 44, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile

Reaktionsvermögens im Falle des Eintritts von Schäden durch Angriffe auf IT-Systeme halten die IT-Grundschutz-Kataloge des BSI umfangreiche Maßnahmen bereit, namentlich Maßnahmenkatalog M6 zur Notfallvorsorge.[452]

II.2.3 Vorhandene Regelungen und Maßnahmen/Status Quo

Nachfolgend wird ein Blick auf die bereits vorhandenen und in Planung befindlichen Regelungen und Maßnahmen geworfen, die im Zusammenhang mit der Bekämpfung von Internetkriminalität stehen.

II.2.3.1 Internationale Regelungen und Maßnahmen

II.2.3.1.1 Cybercrime Convention des Europarates von 2001[453]

Das Übereinkommen über Computerkriminalität des Europarates vom 23. November 2001 (englisch: Cybercrime Convention, CC) ist in Deutschland am 1. Juli 2009 in Kraft getreten. Es enthält Vorgaben für das materielle Strafrecht, das Strafverfahrensrecht und die internationale Zusammenarbeit im Bereich der Computerkriminalität. Einige Vorgaben sind zwingend, andere dagegen bieten Umsetzungsspielraum für die nationalen Staaten.[454] Ziel ist in erster Linie die Harmonisierung der Bemühungen der Unterzeichnerstaaten sowohl im materiell-rechtlichen, als auch im prozessualen Bereich. Das Abkommen wurde bislang (Stand 17. Juli 2012) von 47 Staaten unterzeichnet und davon von 36 Staaten ratifiziert. Darunter sind auch einige Staaten, die selbst nicht dem Europarat angehören.[455] Die Cybercrime Convention ist jedoch auch über ihren Unterzeichnerkreis hinaus von Einfluss auf die Gesetzgebung. Insgesamt wird sie somit von mehr als 100 Staaten weltweit als Basis für das nationale Internetstrafrecht genutzt. Dies entspricht der Intention des Europarates, die Konvention auch Nichtmitgliedern zugänglich zu machen. Der Stand der Umsetzung der Regelungen ist indes lediglich fragmentarisch, da bislang erst etwa zwei Drittel der

---

[452] BSI, IT-Grundschutz-Kataloge, Stand: 12. EL (Sep. 2011), abrufbar unter: https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf

[453] Abrufbar unter: http://conventions.coe.int/treaty/ger/treaties/html/185.htm; dazu auch Walter, Internetkriminalität, 2008, S. 26.

[454] Gercke, Analyse des Umsetzungsbedarfs der Cybercrime Konvention – Teil 1: Umsetzung im Bereich des materiellen Strafrechts, MMR 2004, 728; ders., Analyse des Umsetzungsbedarfs der Cybercrime Konvention – Teil 2: Umsetzung im Bereich des Strafverfahrensrechts, MMR 2004, 801.

[455] Der aktuelle Stand der Unterzeichnung und Ratifizierung kann unter http://www.coe.int abgerufen werden.

Unterzeichnerstaaten die Cybercrime Convention ratifiziert und umgesetzt haben; außerhalb der Europäische Union (EU) nur die USA.[456]

In strafprozessualer Hinsicht enthält die Cybercrime Convention in Artikel 23 bis 35 Vorschriften zur internationalen Zusammenarbeit und Rechtshilfe, insbesondere für den Fall, dass Beweise in elektronischer Form erhoben werden sollen. Geregelt werden die Behandlung von Rechtshilfeersuchen sowie der grenzüberschreitende Zugriff auf gespeicherte Daten ohne Rechtshilfeersuchen und die Errichtung eines 24/7-Netzwerkes für eine schnelle wechselseitige Hilfeleistung. Die Aufgabe des Artikel 35 CC übernimmt das auf polizeilicher Ebene eingerichtete G8 24/7 High Tech Crime Network (HTCN). Die deutsche Kontaktstelle ist das Bundeskriminalamt, Referat SO 43.

Als besonders nützlich hat sich für die Praxis[457] erwiesen, dass bereits durch ein formloses Ersuchen an einen anderen Vertragsstaat die Vorabsicherung beweisrelevanter Daten durch dessen Strafverfolgungsbehörden möglich ist. Diese Option der besonders schnellen zwischenstaatlichen Rechtshilfe eröffnet Artikel 29 in Verbindung mit Artikel 16 und 17 CC. Der wesentliche Unterschied zur klassischen Durchsuchung und Beschlagnahme liegt darin, dass die betroffenen Provider hierbei nicht nur zur Duldung von staatlichen Maßnahmen verpflichtet werden, sondern einer aktiven Mitwirkungspflicht unterworfen sind, wodurch insbesondere die automatische Löschung der relevanten Daten verhindert wird. Durch die auf diese Weise gewonnene Zeit (gemäß Artikel 29 Absatz 7 CC mindestens 60 Tage) ist es der ersuchenden Vertragspartei möglich, ein förmliches Rechtshilfeersuchen zu stellen, um weitere Schritte in die Wege leiten zu können.

Ein Problem, dass sich in der Praxis der Strafverfolgung stellt, wird durch das zunehmende Cloud Computing bewirkt. Eine Folge dessen ist, dass die für die Strafverfolgung relevanten Daten nicht nur an einem einzigen Ort auf einem einzigen Server abgespeichert werden, sondern teilweise weltweit an unterschiedlichen Orten, und dies ohne Zutun des Dateninhabers oder des Hostproviders. Den Strafverfolgungsbehörden ist häufig auch nicht bekannt, an welchem Ort die Daten lagern. Daher geht die Möglichkeit des

---

[456] Franosch, Schriftliche Stellungnahme zu Expertengespräch „Interetkriminalität“, S. 4. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf. Sowie: Gercke, Die Entwicklung des Internetstrafrechts 2010/2011, ZUM 2011, 609, 610 f.

[457] S. hierzu die Darstellung bei Franosch, Schriftliche Stellungnahme zu Expertengespräch „Internetkriminalität“, S. 1 f. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

Rechtshilfeersuchens gemäß Artikel 29 CC nicht selten ins Leere. Ein Auskunftsersuchen nach nationalem Recht an den jeweiligen Hostprovider ist zudem auch nicht in jedem Fall möglich, da die global agierenden Provider nicht in jedem Land, in dem sie ihre Tätigkeit ausüben, auch Niederlassungen besitzen. Eine Regelung, nach der eine Strafverfolgungsbehörde auch an einen ausländischen Provider ein Auskunftsersuchen stellen könnte, sofern dieses ausschließlich Inlandsbezug aufweist, gibt es in der Cybercrime Convention bislang nicht.[458] Das Problem wurde aber bereits von den Vertragsparteien erkannt und wird seit November 2011 durch eine Ad-hoc-Untergruppe bearbeitet, deren Ergebnisse abzuwarten bleiben.[459]

Die Cybercrime Convention ist auch in die Kritik geraten. Bemängelt wird die zunehmende Datenspeicherung, die Realzeitdatenerfassung, die vorgerichtliche Inpflichtnahme der Internet Service Provider zu Ermittlungs- und Strafverfolgungszwecken (Sektion 2) sowie die Möglichkeit präventiver Ermittlungen ohne konkreten Tatverdacht. Zudem ist kritisiert worden, dass nicht alle kooperierenden Staaten gängige rechtsstaatliche Standards erfüllen. Des Weiteren wird eine Überkriminalisierung von Bagatellfällen befürchtet.[460]

Abseits der Cybercrime Convention hat sich der Europarat mit Problemen beschäftigt, die sich den nationalen Strafverfolgungsbehörden bei der internationalen Bekämpfung von Internetkriminalität stellen. Der Europarat hat dazu auf Grundlage einer zuvor durchgeführten Studie[461] Richtlinien entwickelt, die als Vorbild für die Zusammenarbeit von Strafverfolgungsbehörden und Internetdiensteanbietern gelten sollen.[462] Dabei stand jedoch weniger die Ausgestaltung der behördlichen Befugnisse, insbesondere etwaige

---

[458] Eine vergleichbare Regelung enthält beispielsweise das Schengener Durchführungsabkommen in Artikel 52, s. zum Problem: Franosch, Schriftliche Stellungnahme zu Expertengespräch „Interetkriminalität“, S. 3. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

[459] Franosch, Schriftliche Stellungnahme zu Expertengespräch „Interetkriminalität“, S. 3. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

[460] http://epic.org/privacy/intl/ccc.html

[461] Callanan/Gercke, Co-operation between service providers and law enforcement against cybercrime – towards common best-of-breed guidelines?, 2008, abrufbar unter: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_interface2008/567%20prov-d-wg%20STUDY%20FINAL%20%282%29.pdf

[462] Europarat, Guidelines for the cooperation between law enforcement and internet service providers against cybercrime, adopted by the global Conference Cooperation against Cybercrime, 1-2 April 2008, abrufbar unter: http://www.coe.int/t/informationsociety/documents/Guidelines_cooplaw_ISP_en.pdf; näher zum Entstehungsprozess der Richtlinien: Gercke, Die Entwicklung des Internetstrafrechts im Jahr 2008, ZUM 2009, 526, 531.

Schwierigkeiten bei der Strafverfolgung, die aus unzureichender Gesetzgebung resultieren und durch solche folglich beseitigt werden könnten, im Fokus. Vielmehr hat die Studie ergeben, dass neben einigen generellen Problemen, die sich im Rahmen der Zusammenarbeit zwischen Strafverfolgungsbehörden und Internetdiensteanbietern stellen, auch diverse Bad Practices seitens beider Parteien zu verzeichnen sind. Zu den generellen Problemen zählt u. a., dass Anfragen von den beziehungsweise an die Behörden oder Anbieter Gefahr laufen, unvollständig und weniger sorgfältig bearbeitet zu werden, wenn keine klar definierten Kommunikationsstrukturen existieren.[463] Des Weiteren wurde in der Studie die Sorge zum Ausdruck gebracht, dass für das wachsende Aufkommen an Anfragen zwischen den Parteien auf beiden Seiten nicht genügend Ressourcen zur Verfügung stehen könnten.[464] Zu den Bad Practices zählt der Studie zufolge auf Seiten der Anbieter beispielsweise, dass angesichts zahlreicher paralleler Anfragen intern kein System zur Priorisierung oder Kategorisierung zur Verfügung steht, während auf Seiten der Behörden beispielsweise zu vermerken sei, dass unvollständige Antworten auf oder Ablehnungen von Anfragen hingenommen würden.[465]

Die entwickelten Richtlinien sind in weiten Teilen eher in Form von Vorschlägen gehalten.Diese enthalten daher sowohl gemeinsame Prinzipien, die einerseits für die Internetdiensteanbieter und, andererseits für die Strafverfolgungsbehörden gelten sollen, als auch Anregungen zu spezifischen Maßnahmen. Beispielsweise werden die Etablierung eines Verfahrens zur Verifizierung der anfragenden Behörde, ein regelmäßiger Austausch sowie die Meldung von relevanten Vorfällen durch die Anbieter an die Behörden genannt.[466] Indes handelt es sich tatsächlich lediglich um Richtlinien ohne jeden bindenden Charakter.[467]

---

[463] S. Callanan/Gercke, Co-operation between service providers and law enforcement against cybercrime – towards common best-of-breed guidelines?, 2008, S. 52, abrufbar unter: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_interface2008/567%20prov-d-wg%20STUDY%20FINAL%20%282%29.pdf

[464] S. Callanan/Gercke, Co-operation between service providers and law enforcement against cybercrime – towards common best-of-breed guidelines?, 2008, S. 52, abrufbar unter: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_interface2008/567%20prov-d-wg%20STUDY%20FINAL%20%282%29.pdf

[465] S. Callanan/Gercke, Co-operation between service providers and law enforcement against cybercrime – towards common best-of-breed guidelines?, 2008, S. 53 f., abrufbar unter: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_interface2008/567%20prov-d-wg%20STUDY%20FINAL%20%282%29.pdf

[466] S. http://www.coe.int/t/informationsociety/documents/Guidelines_cooplaw_ISP_en.pdf

[467] Cornelius, in: Leupold/Glossner, Teil 10, Rn. 43.

II.2.3.1.2 G8: Subgroup on High-Tech Crime

Die Subgroup on High Tech Crime (HTCSG) ist eine von sechs Unterarbeitsgruppen der G8 Roma/Lyon Arbeitsgruppe.[468] Die aktuelle Arbeit der HTCSG ist durch die Bedrohungen auf dem Gebiet der Informations- und Kommunikationstechnologien (IKT) und den sich daraus für die Strafverfolgungsbehörden ergebenden Herausforderungen geprägt. Die HTCSG beschäftigt sich hauptsächlich mit folgenden Problemen beziehungsweise Herausforderungen, denso genannten Issues of Concern: Angriffe auf IKT, Verbreitung von Schadsoftware (zum Beispiel durch Botnetze), internationale Zusammenarbeit im Rahmen der Strafverfolgung, Fragen im Zusammenhang mit Missbrauchsmöglichkeiten neu aufkommender Technologien und Vorbeugung im Zusammenhang mit Cyber-Kriminalität (zum Beispiel Zusammenarbeit mit Internet-Service-Providern). Ein besonderes Instrument ist das G8 24/7-Netzwerk Computerkriminalität, mit dem zu Strafverfolgungszwecken ohne zeitraubende Formalitäten das Einfrieren digitaler Spuren im Kreise der Mitgliedstaaten (derzeit über 50) erbeten werden kann.

II.2.3.1.3 London Conference on Cyberspace

Am 1. und 2. November 2011 wurde die vom britischen Außenministerium ausgerichtete London Conference on Cyberspace abgehalten. Dabei handelt es sich um ein internationales Treffen von Vertretern aus Politik, Industrie, der Internet-Gemeinschaft und privaten Organisationen aus insgesamt 60 Ländern.[469] Die Konferenz soll nach dem Willen der Teilnehmer in Zukunft jährlich wiederholt werden und u. a. der internationalen Konsensbildung darüber dienen, wie Internetkriminalität wirksam bekämpft werden kann.[470] Bindende Beschlüsse oder Verträge waren jedoch – zumindest im Jahr 2011 – nicht Ziel der Konferenz, stattdessen sollte die Debatte im Vordergrund stehen.[471] Die Internetkriminalität war nur eines von mehreren Kernthemen der Konferenz, doch standen bei der Diskussion über die Rolle des Staates im Internet Aspekte der Überwachung und Identifizierung der Nutzer im Vordergrund. So zeichneten sich im Wesentlichen zwei Lager ab: auf der einen Seite die Befürworter einer strengeren Regulierung des Internets auf internationaler Ebene,

---

[468] S. generell zur G8 Roma/Lyon Arbeitsgruppe: http://www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/G8/G8-Lyon-Gruppe_node.html

[469] http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/; s. auch http://www.fco.gov.uk/en/news/latest-news/?view=PressS&id=685663282

[470] http://www.spiegel.de/netzwelt/netzpolitik/0,1518,795376,00.html

[471] S. die abschließenden Anmerkungen des britischen Außenministers, abrufbar unter: http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=685672482

insbesondere Russland und China, auf der anderen Seite diejenigen Staaten, die für eine maßvolle Regulierung plädierten, so beispielsweise die USA und Großbritannien[472] Die Folgekonferenz fand vom 3. bis 5. Oktober 2012 in Budapest statt.[473]

II.2.3.1.4 Bestrebungen auf Ebene der Vereinten Nationen (United Nations, UN)

Die Vereinten Nationen haben sich schon vielfach mit Fragen der Internetkriminalität auseinandergesetzt, jedoch oft eher in abstrakter Weise oder nur mit spezifischen Einzelaspekten. Ein Beispiel dafür ist die Erforschung und Bekämpfung des Deliktsbereichs des Identitätsdiebstahls (Identity-related crime). Das United Nations Office on Drugs and Crime (UNODC) hat zu diesem Zweck eine gemeinsame Plattform für Akteure aus dem öffentlich-rechtlichen Sektor, der Wirtschaft sowie anderen Organisationen auf regionaler und internationaler Ebene errichtet, auf der diese sich regelmäßig durch eine Expertengruppe austauschen können.[474] Im selben Rahmen wurde zudem eine Studie zu den internationalen Aspekten des Identitätsdiebstahls veröffentlicht.[475] Einen Schritt hin zu umfassenderen Maßnahmen auch seitens der UN-Organisationen haben die Vereinten Nationen im Rahmen des UN Crime Congress im April 2010 in Brasilien getan.[476] Als Ergebnis des Kongresses wurde festgehalten, dass die UN bei der Harmonisierung nationaler legislativer Maßnahmen anhand eigener UN-Standards mitwirken sollte.[477] Damit haben sich die Vereinten Nationen gegen die Empfehlung der Cybercrime Convention des Europarates als weltweiten Standard entschieden.[478] Stattdessen wurde eine eigene Expertengruppe eingesetzt, die Lösungsansätze für Probleme der Internetkriminalität entwickeln soll. Die eingesetzte Expertengruppe hat ihre Arbeit inzwischen aufgenommen.[479] Die Bundesrepublik Deutschland hat zu diesem Zweck

---

[472] http://www.spiegel.de/netzwelt/netzpolitik/0,1518,795376,00.html; s. auch http://www.huffingtonpost.com/2011/11/02/london-conference-on-cyberspace_n_1071242.html

[473] S. ausführlich: http://www.cyberbudapest2012.hu

[474] S. den Abschnitt „Identity-related crime“ unter http://www.unodc.org/unodc/en/organized-crime/index.html; vgl. auch die als Basis dieser Maßnahme dienenden Resolutionen des Wirtschafts- und Sozialrates der Vereinten Nationen (ECOSOC) 2004/26, 2007/20 und 2009/22, abrufbar über dieselbe Website.

[475] Study on Fraud and the criminal misuse and falsification of identity”, einschließlich aller Anhänge abrufbar über: http://www.unodc.org/unodc/en/organized-crime/index.html

[476] Twelfth United Nations Congress on Crime Prevention and Criminal Justice, s. http://www.unodc.org/unodc/en/crime-congress/12th-crime-congress.html

[477] S. insbesondere Punkt 4 der Abschlusserklärung des Kongresses, Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, abrufbar unter: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf

[478] Gercke, Die Entwicklung des Internetstrafrechts 2009/2010, ZUM 2010, 633, 635.

[479] S. zu weiterführenden Informationen über das erste Treffen der Expertengruppe im Januar 2011 https://www.unodc.org/unodc/en/expert-group-to-conduct-study-cybercrime-jan-2011.html

Mitarbeiter aus dem Bundesministerium der Justiz (BMJ), dem BKA sowie der deutschen Vertretung bei den Vereinten Nationen entsandt.[480] Der UN Crime Congress hat überdies seinen Willen bekundet, in Zukunft generell eine stärkere Rolle bei der Unterstützung der Entwicklungsländer bei Maßnahmen gegen die Internetkriminalität einzunehmen.[481]

Weiterhin wurde das Thema IT-Sicherheit auch beim sechsten Jahrestreffen des Internet Governance Forums (IGF) der Vereinten Nationen im Jahr 2011 in Nairobi diskutiert.[482] Das IGF besitzt lediglich eine beratende Funktion, bietet jedoch eine Plattform für den Austausch unterschiedlicher Interessen. Das siebente Jahrestreffen fand vom 6. bis 9. November 2012 in Baku statt.[483]

II.2.3.2 Europäische Regelungen und Maßnahmen

Durch den Vertrag von Lissabon wurde mit Artikel 83 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)[484] eine Grundlage für Maßnahmen im Bereich der Computerkriminalität im Rahmen der EU geschaffen. Die EU ist demnach ermächtigt, Richtlinien zur Mindestregelung von Straftaten und Strafen zu erlassen.

II.2.3.2.1 Maßnahmen nach dem Stockholmer Programm

Im Bereich des Strafrechts erklärt das Stockholmer Programm[485] aus dem Jahr 2009 die Entwicklung von gemeinsamen Minimalstandards im Bereich der Kinderpornografie und der Internetkriminalität zur Priorität der unter dem Vertrag von Lissabon notwendigen Harmonisierungsbestrebungen.[486] Im April 2010 veröffentlichte die EU-Kommission einen Aktionsplan zur Umsetzung des Programms, der die angestrebten Maßnahmen

---

[480] S. die Teilnehmerliste der Expertengruppe, abrufbar unter: https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_INF_2_Rev1.pdf

[481] S. insbesondere Punkt 53 der Abschlusserklärung des Kongresses, Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, abrufbar unter: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf

[482] http://www.intgovforum.org/cms/2011-igf-nairobi/2011calendar

[483] S. http://www.intgovforum.org/cms/2012-calendar

[484] Vertrag über die Arbeitsweise der Europäischen Union, ABl. Nr. C 115 vom 9.5.2008, S. 47.

[485] Das Stockholmer Programm ist ein Programm der EU mit Richtlinien für eine gemeinsame Innen- und Sicherheitspolitik der Mitgliedstaaten für die Jahre 2010 bis 2014. The Stockholm Programme – An open and secure Europe serving and protecting citizens, ABl. Nr. C 115 vom 4.5.2010, S. 1; der deutsche Text des Programms ist abrufbar unter: http://register.consilium.europa.eu/pdf/de/09/st17/st17024.de09.pdf

[486] The Stockholm Programme – An open and secure Europe serving and protecting citizens, darin Unterpunkt 3.3.

konkretisierte.[487] Zu nennen sind eine Richtlinie zur Bekämpfung der Kinderpornografie,[488] die Unterbindung der Geldtransferprozesse im Zusammenhang mit Kinderpornografie im Internet mittels Public-Private-Partnerships (PPP), sowie eine weitere Förderung von Maßnahmen im Rahmen des Safer Internet Action Plan.[489] Im Rahmen der Bekämpfung der Computerkriminalität werden unter anderem Maßnahmen zur Stärkung der Netz- und Informationssicherheitspolitik sowie Maßnahmen zur schnellen Reaktion auf Cyber-Angriffe vorgeschlagen. Darüber hinaus wird angeregt, gesetzliche Regelungen für den Fall von Angriffen auf Informationssystem zu erlassen. Auch der Aufbau einer europäischen Plattform zur Meldung von Straftaten, die Ausarbeitung eines EU-Musterabkommens für Public-Private-Partnerships zur Bekämpfung der Computerkriminalität, Maßnahmen zur gerichtlichen Zuständigkeit in Bezug auf den Cyberspace sowie die Ratifizierung der Cybercrime Convention des Europarates werden vorgeschlagen.[490]

II.2.3.2.2 EU-Initiative: Safer Internet Action Plan (Nunmehr: Safer Internet plus Programme)[491]

Der EU-Aktionsplan Safer Internet dient nach der Vorstellung der Europäischen Kommission dazu, in ihren Mitgliedstaaten auf Chancen und Risiken des Internets aufmerksam zu machen. Kern des Safer Internet Action Plans ist die Einrichtung und der Betrieb einer Reihe von Websites und Hotlines, die aufklären sowie die Möglichkeit der Meldung schädlicher Inhalte bieten sollen. Erklärtes Ziel ist es, Eltern und Kinder für die Probleme illegaler Inhalte zu sensibilisieren. Ein weiteres Element ist die Zusammenarbeit von Strafverfolgungsbehörden insbesondereum von Nutzerinnen und Nutzern gemeldete Straftaten im Internet grenzüberschreitend zu verfolgen. Dafür hat die EU-Kommission im Mai 2012 eine „Neue

---

[487] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Aktionsplan zur Umsetzung des Stockholmer Programms, KOM(2010) 171; zu diesem Plan und den vorgeschlagenen Maßnahmen eingehend: Gercke, Die Entwicklung des Internetstrafrechts 2010/2011, ZUM 2011, 609, 612.

[488] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie und zur Aufhebung des Rahmenbeschlusses 2004/68/JI des Rates, KOM(2010) 94 endg. Der Volltext des Vorschlages und der gegenwärtige Stand des Verfahrens sind abrufbar unter: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=de&DosId=199159#404503

[489] Dazu sogleich Abschnitt II.2.3.2.2.

[490] Eingehend: Gercke, Die Entwicklung des Internetstrafrechts 2010/2011, ZUM 2011, 609, 612.

[491] http://ec.europa.eu/information_society/activities/sip/policy/programme/index_en.htm; s. Walter, Internetkriminalität, 2008, S. 28.

Strategie für ein sicheres Internet und bessere Online-Inhalte für Kinder und Jugendliche“ vorgestellt.[492]

II.2.3.2.3 Entwurf EU-Richtlinie über Angriffe auf Informationssysteme

Auf den Rahmenbeschluss über Angriffe auf Informationssysteme[493] aus dem Jahr 2005 folgte der von der EU-Kommission im November 2010 vorgelegte Vorschlag für eine Richtlinie über Angriffe auf Informationssysteme.[494] Der Vorschlag enthält weitere Harmonisierungsbestrebungen und dient dem Zweck, auch auf neuere Angriffsformen, insbesondere aus Botnetzen, zu reagieren. Die Vorgaben der Richtlinie dürften in Deutschland kaum einer weiteren Umsetzung bedürfen.[495]

II.2.3.2.4 ENISA

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) ist eine 2004 durch Verordnung[496] geschaffene Einrichtung, deren Ziel die Verbesserung der Netz- und Informationssicherheit in Europa ist[497] und die als Think Tank und Analysezentrum die Mitgliedstaaten und andere EU-Einrichtungen in Fragen der IT-Sicherheit beraten soll.[498] ENISA hat allein in jüngster Vergangenheit zahlreiche Untersuchungen zu diversen Aspekten der IT-Sicherheit veröffentlicht, die sich u. a. mit Botnetzen[499], Web Standards[500] sowie den Sicherheitsrisiken im Zusammenhang mit Cookies[501] oder Apps für mobile Endgeräte[502]

---

[492] S. die Pressemitteilung IP/12/445 vom 02.05.2012, abrufbar unter: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/445&format=HTML&aged=0&language=DE&guiLanguage=en

[493] Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl. Nr. L 69 vom 16.3.20005, S. 67.

[494] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates vom 30.9.2010, KOM(2010) 517 endg. Der Volltext des Vorschlags und der gegenwärtige Stand des Verfahrens sind abrufbar unter: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=de&DosId=199692

[495] Näher: Gercke, Die Entwicklung des Internetstrafrechts 2010/2011, ZUM 2011, 609, 613.

[496] 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 77 vom 13.3.2004, S. 1.

[497] Nähere Informationen unter: http://www.enisa.europa.eu/about-enisa

[498] MMR-Aktuell 2011, 318598.

[499] http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence

[500] http://www.enisa.europa.eu/act/application-security/web-security/a-security-analysis-of-next-generation-web-standards

[501] http://www.enisa.europa.eu/act/it/library/pp/cookies

[502] http://www.enisa.europa.eu/act/application-security/smartphone-security-1/appstore-security-5-lines-of-defence-against-malware

befassen.[503] Zu den Aufgaben von ENISA gehört auch die regelmäßige Anfertigung von Berichten über die IT-Sicherheit in der EU.[504]

Das Mandat für ENISA ist erst kürzlich durch Verordnung bis zum 13. September 2013 verlängert worden.[505] Derzeit ist zudem eine Modernisierung des Mandats in Beratung, durch das ENISA eine stärkere Rolle bei der Verhütung, Erkennung und Bewältigung von Störungen der Netz- und Informationssicherheit innerhalb der EU einnehmen würde.[506]

II.2.3.2.5 Einrichtung eines europäischen IT-Notfallteams

Ebenfalls in Vorbereitung ist die Einrichtung eines IT-Notfallteams (CERT – Computer Emergency Response Team) für die IT-Infrastrukturen der EU-Organe, das so genannte iCERT@eu.

Parallel zu den Planungen hat ENISA im Juni 2011 zudem eine Bestandsaufnahme der in der EU vorhandenen CERTs veröffentlicht.[507] Diese sollen nach dem Willen der Digitalen Agenda[508] der EU-Kommission und des Rates zufolge Teil eines bis 2012 aufzubauenden, europaweiten Netzwerkes von CERTs sein, mit dessen Hilfe es möglich werden soll, gezielter und umfassender auf zukünftige Angriffe auf IT-Systeme zu reagieren.[509] In der Bestandsaufnahme werden aus der Vielzahl der deutschen CERTs 18 explizit erfasst und dargestellt, von denen die Mehrzahl privaten Trägern, insbesondere aus der Industrie[510] und dem Finanzsektor[511], zuzuordnen sind. Öffentlich-rechtliche Träger sind einige universitäre

---

[503] Ein Überblick über ENISAs Aktivitäten im Bereich „Awareness Raising“ seit 2005 vom 15. Februar 2011 ist abrufbar unter: http://www.enisa.europa.eu/act/ar/deliverables/overview-de. Eine Gesamtübersicht über die Berichte von ENISA ist abrufbar unter: http://www.enisa.europa.eu/publications/studies/reports

[504] S. den Cyber Europe 2010 Report vom 18. April 2011, abrufbar unter: http://www.enisa.europa.eu/act/res/ce2010/ce2010report

[505] Verordnung (EU) Nr. 580/2011 des Europäischen Parlaments und des Rates vom 8. Juni 2011 zur Änderung der Verordnung (EG) Nr. 460/2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer, ABl. Nr. L 165 vom 24.6.2011, S. 3. Online abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:165:0003:0004:DE:PDF.

[506] S. die Pressemitteilung des Rates 10494/11 vom 27. Mai 2011, abrufbar unter: http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/11/145&format=HTML&aged=1&language=DE&guiLanguage=en, sowie den zugehörigen Sachstandsbericht 10296/11, abrufbar unter: http://register.consilium.europa.eu/pdf/de/11/st10/st10296.de11.pdf

[507] Inventory of CERT activities in Europe, abrufbar unter: http://www.enisa.europa.eu/act/cert/background/inv/files/inventory-of-cert-activities-in-europe

[508] S. die Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Eine Digitale Agenda für Europa“ vom 19.5.2010, KOM(2010) 245 endg., in der korrigierten Fassung vom 26.8.2010, KOM(2010) 245 endg./2, sowie unter http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[509] S. die Pressemitteilung der EU-Kommission IP/11/694 vom 10.6.2011, abrufbar unter: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/694&format=HTML&aged=0&language=DE&guiLanguage=en

[510] S. beispielsweise http://www.first.org/members/teams/sap_cert sowie http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert.htm

[511] S. beispielsweise http://www.s-cert.de/ sowie https://www.trusted-introducer.org/teams/teams-c.html#COMCERT

Institute[512] sowie der Bund. Letzterer betreibt über das BSI ein CERT für die Bundesbehörden. Zusätzlich bietet das BSI ein Bürger-CERT für Bürgerinnen und Bürger sowie kleine Unternehmen an. Die deutschen CERTs sind darüber hinaus im CERT-Verbund organisiert, der die Kooperation zwischen den Mitgliedern ermöglichen soll, ihnen aber im Übrigen ihre Autonomie belässt.[513] Um den Austausch effizient zu gestalten, haben die Mitglieder des CERT-Verbunds ein spezielles Austauschformat geschaffen, das Deutsche Advisory Format (DAF).[514]

II.2.3.2.6 Europol

Am 1. Januar 2010 ist mit dem Europol-Beschluss eine neue Rechtsgrundlage für die Befugnisse von Europol in Kraft getreten.[515] Mit dem Vertrag von Lissabon wurden die Aufgaben von Europol in Artikel 88 AEUV festgeschrieben. Europol ist seither befugt, Polizei und Strafverfolgungsbehörden der Mitgliedstaaten bei ihrer Zusammenarbeit zur Bekämpfung der Kriminalität zu unterstützen. Die Behörde soll besser als bisher in den gegenseitigen Informationsaustausch eingebunden werden.

Europol wird damit zur Zentralstelle für den polizeilichen Informationsaustausch in der EU. Die Behörde kämpft jedoch der Gemeinsamen Kontrollinstanz von Europol (GKI) zufolge mit datenschutzrechtlichen Problemen:

So hat das Projekt „Check the Web“ (CTW), in dessen Rahmen offen zugängliche islamistische Internetquellen ausgewertet und terroristische Netzaktivitäten beobachtet werden, Kritik auf sich gezogen. „Check the Web“ wird auf Initiative Deutschlands seit 2007 von Europol betrieben. Ursprünglich sollte das Portal vornehmlich dem Informationsaustausch der Mitgliedsländer dienen. Es entwickelte sich jedoch zunehmend zu einem Europol-Informationssystem. Auf Empfehlung der GKI wurde es deshalb in eine Arbeitsdatei zu Analysezwecken im Sinne des Europol-Beschlusses umgewandelt.[516] Die Umwandlung in eine Analysedatei ermöglicht nun auch die Speicherung von Personendaten. Darüber hinaus gab es in der Vergangenheit immer wieder auf europäischer Ebene Vorschläge „Check the Web“ um andere Phänomenbereiche zu erweitern. Bislang wurde dies

---

[512] S. beispielsweise http://cert.uni-stuttgart.de/ sowie https://www.cert.kit.edu/

[513] S. die (zuletzt 2004 aktualisierte) Internetpräsenz des CERT-Verbunds: http://www.cert-verbund.de/

[514] http://www.cert-verbund.de/daf/index.html

[515] Beschluss des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol), ABl. Nr. L 121 vom 15.5.2009, S. 37.

[516] Tätigkeitsbericht 2009 und 2010 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – 23. Tätigkeitsbericht –, BT-Drs. 17/5200, S. 147.

jedoch nicht konkretisiert. Für „Check the Web“ ist das BKA national der Ansprechpartner im Rahmen der Zusammenarbeit im Gemeinsamen Internetzentrum (GIZ), in dem unter Gesamtgeschäftsführung des Bundesamtes für Verfassungsschutz das BKA, der Militärische Abschirmdienst sowie der Generalbundesanwalt Fragestellungen zu islamistischen Internetseiten bearbeiten.

Bemängelt wird auch, dass Europol Cross Matching betreibt, also Daten, die via Europol ausgetauscht werden, mit eigenen Informationen abgleicht. Geplant ist auch ein Datenabgleich europäischer mit nationalen Informationssystemen.[517] Europol ist neuerdings auch berechtigt, personenbezogene Daten kommerziell zu erwerben, etwa bei Auskunfteien, darf allerdings nur insoweit darauf zugreifen, als dies zu seiner Aufgabenerfüllung unbedingt erforderlich ist.[518]

Zudem wurde 2009 eine so genannte European Cybercrime Platform (Europäische Cybercrime-Plattform, ECCP) eingerichtet, die auf drei Säulen fußt: 1. Internet Crime Reporting Online System zur Meldung von personenbezogenen Informationen über Kriminalitätsfälle, bei denen die Jurisdiktion mehrerer Mitgliedstaaten betroffen ist, sowie zur Führung des europaweiten Kriminalaktennachweises; 2. „Cyborg“-Analyse-Datei, konzentriert auf gewinnorientierte Internet-Delikte; 3. Internet FORencsic Expertise (I-FOREX) zum Austausch über bewährte Trainingsmethoden und Praktiken.[519]

II.2.3.3 Nationale Regelungen

II.2.3.3.1 Materiell-strafrechtliche Aspekte

Die Gesetzesänderung im Zuge des 41. Strafrechtsänderungsgesetzes[520] hat für eine Anpassung des materiellen Kernstrafrechts an die Gefahren der Internetkriminalität gesorgt.

Teilweise wird allerdings im Bereich des materiellen Strafrechts der neugeschaffene § 202c StGB und insbesondere dessen Nummer 2 zur Pönalisierung von bestimmten

---

[517] Tätigkeitsbericht 2009 und 2010 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – 23. Tätigkeitsbericht –, BT-Drs. 17/5200, S. 147.

[518] Ebd.

[519] Holzberger, Wer gegen wen? Gremien zur Bekämpfung der Cyberkriminalität, Bürgerrechte & Polizei/CILIP 98 (1/2011).

[520] Einundvierzigstes Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) vom 7. August 2007 (BGBl. I S. 1786).

Vorbereitungshandlungen kritisch gesehen.[521] Hier könnten sich Defizite erst aufgrund der Neuschaffung dieser Norm ergeben haben. Problematisch wird vor allem der – trotz der Zweckbestimmung zur Begehung einer Tat nach § 202a StGB und § 202b StGB sowie § 303a StGB[522] und § 303b StGB[523] – sehr weite objektive Tatbestand der Norm gesehen,[524] der grundsätzlich auch bestimmte Sachverhalte erfassen kann, bei denen ein Administrator seine eigene IT auf Schwachstellen testen möchte.[525] Zwischenzeitlich hat aber das Bundesverfassungsgericht hervorgehoben, dass es nicht ausreicht, wenn ein Computerprogramm zur Begehung der genannten Straftaten lediglich geeignet ist, sondern dass das Programm vielmehr in der Absicht entwickelt oder modifiziert worden sein muss, es zur Begehung der Straftaten einzusetzen.[526] Damit sind so genannte Dual-Use-Programme bereits nicht vom objektiven Tatbestand der Norm erfasst.[527] Zudem wird angemerkt, die Verstärkung von Abwehrmaßnahmen gegen Angriffe könne negativ beeinträchtigt werden. Damit gehe ein Absinken des generellen IT-Sicherheitsniveaus einher, da Sicherheitstests auch unter realen Bedingungen – und damit mit Hacker-Tools, die auch von Angreifern in der Absicht eines Angriffs programmiert wurden – durchgeführt werden müssten.[528] Daher stelle die von der Norm geforderte Zweckbestimmung kein hinreichendes Korrektiv dar.[529] Als Korrektiv zum Ausschluss der Strafbarkeit verblieben dann lediglich die §§ 153, 153a der

---

[521] S. hierzu etwa Ernst, Das neue Computerstrafrecht, NJW 2007, 2661; Cornelius, Zur Strafbarkeit des Anbietens von Hackertools, CR 2007, 682; s. weiter auch die Schröder, Schriftliche Stellungnahme zu Expertengespräch „Sicherheit im Netz“, S. 1; s. weiter bereits BT-Drs. 16/5449, Beschlussempfehlung und Bericht des Rechtsausschusses zum Entwurf einen StrÄndG zur Bekämpfung von Computerkriminalität.

[522] Aufgrund des Verweises in dessen Absatz 3.

[523] Aufgrund des Verweises in dessen Absatz 5.

[524] S. dazu auch bereits die Bedenken des Bundesrates gegen den Gesetzentwurf, BT-Drs. 16/3656, S. 16 f.

[525] Ernst, Das neue Computerstrafrecht, NJW 2007, 2661, 2663; s. dazu auch BT-Drs. 16/5449, Beschlussempfehlung und Bericht des Rechtsausschusses zum Entwurf einen StrÄndG zur Bekämpfung von Computerkriminalität, S. 4, wonach entsprechend Artikel 6 der Cybercrime-Convention des Europarates lediglich Computerprogramme erfasst werden sollen, „(…) die in erster Linie dafür ausgelegt oder hergestellt würden, um damit Straftaten nach den §§ 202a, 202b StGB zu begehen. Die bloße Geeignetheit zur Begehung solcher Straftaten begründe keine Strafbarkeit. Die geforderte Zweckbestimmung müsse eine Eigenschaft des Computerprogramms in dem Sinne darstellen, dass es sich um so genannte Schadsoftware handele“.

[526] BVerfG, ZUM 2009, 745, Tz. 60 ff., unter Heranziehung des Wortlautes der Norm, Tz. 61, der Gesetzessystematik, Tz. 62, sowie der Entstehungsgeschichte, Tz. 63.

[527] BVerfG, ZUM 2009, 745, Tz. 61, 63, 64.

[528] So ähnlich auch die Auffassung des Chaos Computer Club, zitiert in BVerfG, ZUM 2009, 745, Tz. 49; Cornelius, Zur Strafbarkeit des Anbietens von Hackertools, CR 2007, 682 mit einigen Beispielen für Dual-Use-Software; BVerfG, ZUM 2009, 745, Tz. 70.

[529] So bereits Fraktion DIE LINKE, BT-Drs. 16/5449, Beschlussempfehlung und Bericht des Rechtsausschusses zum Entwurf einen StrÄndG zur Bekämpfung von Computerkriminalität, S. 5; Ernst, Das neue Computerstrafrecht, NJW 2007, 2661, 2663.

Strafprozessordnung (StPO)[530] und §§ 45, 47 des Jugendgerichtsgesetzes (JGG)[531] sowie der subjektive Tatbestand, also die Frage, ob mit Vorsatz gehandelt wurde.[532] Letzteres sei wiederum problematisch, da nach dem Gesetzeswortlaut bereits Eventualvorsatz genüge, also die billigende Inkaufnahme der Vorbereitung der genannten Straftaten.[533] Das könne aber in der Regel ebenfalls anzunehmen sein, da die Eignung der Software zur Tatbegehung einem Handelnden für gewöhnlich klar sei.[534] Das Bundesverfassungsgericht sieht in bestimmten Fallkonstellationen den subjektiven Tatbestand selbst bei Personen mit legaler Verwendungsabsicht als erfüllt an, wenn das Programm gegebenenfalls nicht vertrauenswürdigen Personen zugänglich gemacht wird.[535]

Des Weiteren wird § 202c StGB mit einem Rückzug der IT-Security-Szene aus der Öffentlichkeit in Verbindung gebracht, da die Motivation gesunken sei, öffentlich auf neuartige Sicherheitslücken hinzuweisen.[536] Neben der dadurch verursachten Erweiterung des Zeitfensters für Angriffe aufgrund von länger unbekannt bleibenden Sicherheitslücken in Systemen bewirke § 202c StGB auch eine Hemmung bei der Herausbildung von IT-Sicherheitsexperten.[537]

Ob und inwieweit die letztgenannten Bedenken und/oder ein durch § 202c StGB unterstelltes generelles Absinken des Sicherheitsniveaus beziehungsweise eine Überkriminalisierung sich allerdings an tatsächlichen Entwicklungen orientieren, oder ob die Rechtsprechungspraxis den Tatbestand im Lichte des Beschlusses des Bundesverfassungsgerichts so auslegen wird, dass sich die Bedenken zerstreuen,[538] ist derzeit noch nicht nachprüfbar. Empirische oder sonstige Erkenntnisse sowie instanzgerichtliche Rechtsprechung fehlen bislang.

---

[530] Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Artikel 2 des Gesetzes vom 25. Juni 2012 (BGBl. I S. 1374).

[531] Jugendgerichtsgesetz in der Fassung der Bekanntmachung vom 11. Dezember 1974 (BGBl. I S. 3427), zuletzt geändert durch Artikel 3 des Gesetzes vom 6. Dezember 2011 (BGBl. I S. 2554).

[532] Ernst, Das neue Computerstrafrecht, NJW 2007, 2661, 2664; BVerfG, ZUM 2009, 745, Tz. 71.

[533] BVerfG, ZUM 2009, 745, Tz. 72 f.

[534] So Ernst, Das neue Computerstrafrecht, NJW 2007, 2661, 2664.

[535] BVerfG, ZUM 2009, 745, Tz. 75.

[536] Schröder, Schriftliche Stellungnahme zu Expertengespräch „Sicherheit im Netz“, S. 1.

[537] Ebd.

[538] Ernst, Das neue Computerstrafrecht, NJW 2007, 2661, 2664; s. zur Auslegung von § 202c StGB weiter auch Cornelius, Zur Strafbarkeit des Anbietens von Hackertools, CR 2007, 682 ff., der für Software mit doppeltem Verwendungszweck die Ansicht vertritt, dass es dabei auf die vom „ (…) Hersteller/Verkäufer/Nutzer gesetzten Merkmale (ankomme), die erkennbar gerade auf eine Förderung eines späteren kriminellen Einsatzes abzielen“ müssen, sowie als zusätzliches Merkmal die Vertriebspolitik und die Werbung in Betracht käme.

Ein weiterer Straftatbestand ist schließlich systematisch in der Nähe der Sachbeschädigung zu finden: Gemäß § 303a StGB (Datenveränderung) macht sich strafbar, wer rechtswidrig Daten im Sinne von § 202a Absatz 2 StGB löscht, unterdrückt, unbrauchbar macht oder verändert. Auch bestimmte Formen der Tatvorbereitung sind gemäß §§ 303a Absatz 3 in Verbindung mit 202c StGB strafbar.

II.2.3.3.2 Nebenstrafrechtliche Regelungen

Auch außerhalb des Strafgesetzbuches finden sich nunmehr Regelungen, die explizit der Bekämpfung der Computerkriminalität dienen. Hervorzuheben sind hier etwa § 17 Absatz 2 UWG, der das Sichverschaffen oder Sichern von Geschäfts- oder Betriebsgeheimnissen mittels technischer Mittel unter Strafe stellt.[539]

Die Vorschrift soll damit sowohl den Geheimbereich eines Unternehmens vor unredlichen Eingriffen schützen als auch alle Marktteilnehmer, da ein unverfälschter und funktionsfähiger Wettbewerb im Interesse der Allgemeinheit steht. Im Einzelnen erfasst ist aber auch die Weitergabe von Geheimnissen an fremde Nachrichtendienste.[540] § 17 Absatz 1 UWG regelt den Fall, bei dem das Geheimnis dem Täter im Rahmen des Dienstverhältnisses anvertraut worden ist oder sonst zugänglich gewesen sein muss. Hier ist § 17 Absatz 2 Nummer 1a UWG von Bedeutung, bei dem der Täterkreis nicht beschränkt ist, wodurch das Delikt von jedermann begangen werden kann.[541] Die Norm spricht bei der Tathandlung von „Verschaffen“ und orientiert sich bei der Auslegung des Begriffs an §§ 96 und 202a StGB.[542] Aufgrund des befürchteten, mit der Offenlegung von erfolgreichen Spionageattacken verbundenen Imageverlusts spielt § 17 Absatz 1 UWG in der Strafverfolgungspraxis eher eine untergeordnete Rolle.[543]

---

[539] § 17 Absatz 1 UWG lautet: „Strafbar macht sich, wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihm vermöge eines Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zum Zwecke des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen, mitteilt“. § 17 Absatz 2 Nummer. 1a UWG, der sich auf Absatz 1 bezieht, lautet: „Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, sich ein Geschäfts- oder Betriebsgeheimnis durch Anwendung technischer Mittel, unbefugt verschafft oder sichert“.

[540] Möhrenschläger, in: Wabnitz/Janovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 3. Aufl. 2007, Kap. 13 II 1 Rn. 2.

[541] Diemer, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, Stand: 188. EL 2012, U 43 (UWG), § 17 Rn. 34.

[542] Möhrenschläger, in: Wabnitz/Janovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 3. Aufl. 2007, Kap. 13 II 2 lit. b Rn. 20.

[543] Ebd., Kap. 13 II 1 Rn. 2.

II.2.3.3.3 Regelungen der Haftung und Verantwortlichkeit mit Steuerungswirkung für die IT-Sicherheit[544]

II.2.3.3.3.1 Haftung des Angreifers

Im Zivilrecht ist die Haftung des Angreifers umfassend geregelt. Die Fülle der möglichen Anspruchsgrundlagen kann hier nicht abschließend behandelt werden, stattdessen soll ein kurzer Überblick gegeben werden.

II.2.3.3.3.1.1 Deliktische Haftung gemäß § 823 Absatz 1 BGB

Der Schutzbereich des § 823 Absatz 1 BGB wird zwingend erst durch die Verletzung eines der enumerativ aufgeführten Rechtsgüter eröffnet, namentlich Leben, Körper, Gesundheit, Freiheit, Eigentum oder ein sonstiges Recht eines anderen.

Verletzung des Eigentums

Der Angriff auf ein IT-System kann einen Eingriff in das Recht des Eigentümers des Systems bedeuten. Der Befall mit Computerviren kann schon eine Verletzung des Eigentums darstellen. Die Integrität von Daten ist grundsätzlich von dem Eigentumsbegriff des § 823 Absatz 1 BGB umfasst.[545] Zwar kommt Daten nach der herrschenden Meinung selbst keine Sacheigenschaft zu, jedoch bezieht der zivilrechtliche Eigentumsschutz auch die Funktionalität und innere Ordnung des Eigentums mit ein.[546] Da praktisch jede Art der Datenspeicherung eine innere Ordnung voraussetzt, die durch Veränderung oder Löschung mittels eines Virus gestört oder sogar zerstört wird, stellt der Befall mit Viren regelmäßig eine Eigentumsverletzung im Sinne des § 823 Absatz 1 BGB dar.[547]

---

[544] Zur rechtlichen Würdigung der Haftung und Verantwortlichkeit eingehend Spindler, Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären – Studie im Auftrag des BSI, 2007, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Recht/Gutachten_pdf.pdf;jsessionid=48F57CABEB03774EBB4B3A1ACDB2F4C1.2_cid248?__blob=publicationFile

[545] OLG Karlsruhe NJW 1996, 200, 201; zust. Meier/Wehlau, Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, NJW 1998, 1585, 1587 ff.; Hager, in: Staudinger, §§ 823 E-I, 824, 825, 2009, § 823 BGB Rn. B 60; Imhof, Das Jahr-2000-Problem, WPK-Mitt. 1998, 136, 137; Taeger, Außervertragliche Haftung für fehlerhafte Computerprogramme, 1995, S. 261; a.A. LG Konstanz NJW 1996, 2662; AG Dachau NJW 2001, 3488.

[546] Spindler, in: Bamberger/Roth, BGB, 3. Aufl. 2012, § 823 BGB Rn. 55; Wagner, in: Münchener Kommentar zum BGB, Bd. 5, 5. Aufl. 2009, § 823 BGB Rn. 103.

[547] OLG Karlsruhe NJW 1996, 200, 201; Bartsch, Computerviren und Produkthaftung, CR 2000, 721, 723; Spindler, Das Jahr 2000-Problem in der Produkthaftung – Pflichten der Hersteller und der Softwarenutzer, NJW 1999, 3737, 3738; Spindler, IT-Sicherheit und Produkthaftung – Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer, NJW 2004, 3145, 3146; Meier/Wehlau, Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, NJW 1998, 1585, 1588; Mankowski, in: Ernst, Hacker, Cracker & Computerviren, 2004, Rn. 440 f.; Koch, Versicherbarkeit von IT-Risiken, 2005, Rn. 357 f.; Sodtalbers, Softwarehaftung im Internet, 2006, Rn. 511; Spindler, in: Bamberger/Roth, BGB, 3. Aufl. 2012, § 823 BGB Rn. 55; a.A. Bauer, Produkthaftung für Software

Auch das Tatbestandsmerkmal des Verschuldens dürfte regelmäßig kein Problem darstellen. In den meisten Fällen wird derjenige, der die Viren in Umlauf bringt, vorsätzlich handeln. Dass das genaue Opfer im Moment seiner Verletzungshandlung noch nicht bestimmt ist, schadet der Haftung nicht.

Auch die Infektion mit anderen Formen von Schadsoftware kann grundsätzlich zu einer Eigentumsverletzung führen. Hier kommt es im Einzelnen darauf an, ob die interne Ordnung der Festplatte durch die Schadsoftware verändert wird oder nicht.

Teilweise wird so weit gegangen, auch den verkörperten Datenbestand an sich als sonstiges in § 823 Absatz 1 BGB geschütztes Recht anzusehen.[548] Dies hätte den Vorteil, dass die Integrität der Daten auch dann geschützt wäre, wenn die Daten an einen Dritten ausgelagert sind. Ob diese Ansicht sich durchsetzt, bleibt abzuwarten.

Grundsätzlich kann das Eigentum auch in der Weise geschädigt werden, dass dem Eigentümer die bestimmungsgemäße Verwendung erschwert oder entzogen wird.[549] Diese Variante der Rechtsgutverletzung dürfte insbesondere in den Fällen der DDoS-Angriffe von Bedeutung sein. Aber auch die Infektion mit Schadsoftware kann die Betriebsbereitschaft eines IT-Systems erheblich einschränken. Wann jedoch die Grenze zu der von der Rechtsprechung[550] und auch dem Großteil der Literatur[551] verlangten erheblichen Einschränkung der Benutzbarkeit eines IT-Systems zu ziehen ist, ist regelmäßig eine Frage des Einzelfalles. Auch hier kann regelmäßig von einem Verschulden des Angreifers ausgegangen werden.

Leben, Körper, Gesundheit, Freiheit

Auch die Verletzung der Rechtsgüter Leben, Körper, Gesundheit oder Freiheit kann theoretisch gegeben sein.

Insbesondere dort, wo die IT als Hilfstechnik unverzichtbar ist, etwa im Bereich der Medizin, ist es möglich, dass Angriffe auf die IT zu Schäden an Leben, Körper oder Gesundheit führen.

---

nach geltendem und künftigem deutschen Recht (Teil 2), PHi 1989, 98, 105 f., nach dem die Zerstörung der Information physikalisch allenfalls eine elektronische Zustandsveränderung darstellt.

[548] Faustmann, Der deliktische Datenschutz, VuR 2006, 262 f.; Meier/Wehlau, Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, NJW 1998, 1585, 1588.

[549] Spindler, in: Bamberger/Roth, BGB, 3. Aufl. 2012, § 823 BGB Rn. 50 ff. m.w.N.

[550] BGH NJW 1983, 2313, 2314; BGH NJW-RR 2005, 673, 674; BGH NJW 1994, 517, 518.

[551] Wagner, in: Münchener Kommentar zum BGB, Bd. 5, 5. Aufl. 2009, § 823 BGB Rn. 122; Hager, in: Staudinger, §§ 823 E-I, 824, 825, 2009, § 823 Rn. B97 f.

Sonstige Rechte

Neben der Verletzung eines der bereits genannten Rechtsgüter kommt auch die eines „sonstigen Rechts“ im Sinne von § 823 Absatz 1 BGB in Betracht. Hintergrund dessen ist, dass § 823 Absatz 1 BGB nicht vor jedem beliebigen Schaden schützen soll, sondern die Schutzgüter grundsätzlich abschließend benennt. Die so genannten „sonstigen Rechte“ erweitern daher zwar einerseits den Schutzbereich der Norm, müssen jedoch andererseits auch einen den ausdrücklich genannten Rechtsgütern (Leben, Körper, Gesundheit, Freiheit, Eigentum) vergleichbaren absoluten Charakter besitzen, damit die Reichweite des § 823 Absatz 1 BGB nicht ausufert.[552] Als sonstige Rechte werden daher nur absolute, ausschließliche Rechte anerkannt (zum Beispiel das allgemeine Persönlichkeitsrecht, die Immaterialgüterrechte und der Besitz). Von besonderer Bedeutung dürfte in diesem Zusammenhang auch das Recht auf informationelle Selbstbestimmung sein. Es schützt gegen die unzulässige Erhebung, Nutzung und Verarbeitung persönlicher und personenbezogener Daten. Die Verletzung des Rechts auf informationelle Selbstbestimmung beispielsweise durch das Ausspähen von Datenkann Ansprüche auf Unterlassung, Beseitigung, Auskunft und Ersatz des materiellen und immateriellen Schadens nach den §§ 823, 1004 BGB begründen. Für einige Fälle der Internetkriminalität von Bedeutung ist des Weiteren das vom Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008 anerkannte „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme”.[553] Jeder Zugriff auf ein IT-System, durch den der Nutzer die Kontrolle über das System verliert, stellt grundsätzlich einen Eingriff in den Schutzbereich des Rechtes dar. Hierunter fällt insbesondere auch der Zugriff mit Backdoorprogrammen.[554] Offen ist noch, ob das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme ein „sonstiges Recht“ im Sinne von § 823 Absatz 1 BGB ist.[555]

---

[552] Wagner, in: Münchener Kommentar zum BGB, Bd. 5, 5. Aufl. 2009, § 823 BGB Rn. 142.

[553] Eingehend zu dem Urteil Hornung, Ein neues Grundrecht, CR 2008, 299; Hoeren, Was ist das „Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme“?, MMR 2008, 365; Bär, Anmerkung zu BVerfG: Verfassungsmäßigkeit der Online-Durchsuchung und anderer verdeckter Ermittlungsmaßnahmen in Datennetzen, MMR 2008, 325; Eifert, Informationelle Selbstbestimmung im Internet, NVwZ 2008, 521.

[554] S.o. Abschnitt II.2.1.6.1, dort Absatz: Backdoors.

[555] Dafür wohl Roßnagel/Schnabel, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, 3534, 3536; dafür auch Bartsch, Die „Vertraulichkeit und Integrität informationstechnischer Systeme“ als sonstiges Recht nach § 823 Absatz 1 BGB, CR 2008, 613, 614 f., ders., Software als Rechtsgut, CR 2010, 553, 554,

II.2.3.3.3.1.2 Deliktische Haftung gemäß § 823 Absatz 2 BGB in Verbindung mit einem Schutzgesetz

Bei den oben genannten strafrechtlichen Normen handelt es sich um Schutzgesetze im Sinne des § 823 Absatz 2 BGB. Durch die Verbindung mit § 823 Absatz 2 BGB kommt diesen eine besondere rechtsschützende Qualität zu.

II.2.3.3.3.1.3 Verantwortlichkeit nach Spezialgesetzen

In Frage kommt schließlich noch die Verletzung einiger spezialgesetzlicher Normen aus dem IT-Bereich, die nicht im Detail behandelt werden können. Hervorzuheben ist aber insbesondere § 43 Absatz 2 Nummer 3 und 4 des Bundesdatenschutzgesetzes (BDSG).[556] Diesem zufolge handelt ordnungswidrig, wer unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft (Nummer 3), oder wer die Übermittlung solcher Daten durch unrichtige Angaben erschleicht (Nummer 4).

II.2.3.3.3.2 Haftung des IT-Herstellers

II.2.3.3.3.2.1 Vertragliche Haftung

Insbesondere in Vertragsverhältnissen zwischen Unternehmern steht die vertragliche Haftung des IT-Herstellers für seine Software gegenüber den Abnehmern seiner Produkte im Vordergrund.[557] Geradezu typisch für den Bereich der Business-Software sind langfristige Vertragsverhältnisse, die neben der Lizenzgewährung oder der Herstellung oder Anpassung von Individualsoftware die Softwarepflege entweder originär oder als Zusatzleistung enthalten.[558] Hier wird auch die Absicherung der Software gegenüber neu auftretenden Sicherheitslücken oder anderen bekannt werdenden Gefahren regelmäßig direkt Vertragsbestandteil sein.

Selbstverständlich besteht eine Haftung eines Herstellers von Software nicht nur im Business-to-Business(B2B)-Bereich, sondern auch gegenüber Verbrauchern, die die Software käuflich erworben haben. Diesen gegenüber haftet der Hersteller immer im Rahmen der gesetzlichen

---

[556] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814); s. auch Spindler, in: Lorenz, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2010, S. 57.

[557] Spindler, in: FS Nagel, 2011, S. 22.

[558] S. dazu Spindler, in: FS Nagel, 2011, S. 22; Marly, Softwareüberlassungsverträge, 4. Aufl. 2004, Rn. 508; Peter, in: Schneider/von Westphalen, Software-Erstellungsverträge, 2006, Kap. G Rn. 7 ff.; Baum, Gestaltung von Software-Maintenance-Verträgen in der internationalen Praxis, CR 2002, 705 ff.; Koch, Versicherbarkeit von IT-Risiken, 2005, Rn. 505.

Gewährleistungsregeln nach dem Bürgerlichen Gesetzbuch,[559] die weder durch Allgemeine Geschäftsbedingungen noch einzelvertraglich eingeschränkt werden können.[560] Darüber hinaus sprechen einige Hersteller auch die gesetzliche Gewährleistung überschreitende Garantieleistungen aus, wie zum Beispiel eine verlängerte Dauer der Haftung beim Auftreten von Mängeln.

II.2.3.3.3.2.2 Außervertragliche Verschuldenshaftung nach § 823 Absatz 1 BGB

Voraussetzung für eine deliktische Produzentenhaftung nach § 823 Absatz 1 BGB ist zunächst die schuldhafte Verletzung eines der dort genannten Schutzgüter.[561] Nicht abschließend geklärt ist die Reichweite der Verantwortlichkeit der Hersteller in Bezug auf Angriffe Dritter, die erst durch Herstellungsfehler der Software ermöglicht wurden. Eine Produzentenhaftung[562] nach § 823 Absatz 1 BGB wird in der Literatur vor dem Hintergrund des allgemeinen Schadensrechts nicht von vornherein ausgeschlossen, da denjenigen, der eine Gefahrenquelle eröffnet, auch dann Sicherungspflichten treffen, wenn die unmittelbare Gefährdung von einem Dritten ausgeht.[563]

So trifft den Hersteller eines Produkts stets nicht nur die Pflicht, das Produkt ordnungsgemäß zu konstruieren, zu fertigen und den Nutzer zu instruieren, sondern auch die Pflicht, das Produkt zu beobachten und die Nutzer vor bekannt werdenden Gefahren zu warnen.[564] Diese Pflicht wird vom Bundesgerichtshof in ständiger Rechtsprechung weit ausgelegt, und auch bei von Dritten ausgehenden Gefahren wird davon ausgegangen, dass der Hersteller zumindest zur Warnung des Nutzers verpflichtet ist.[565]
Grundsätzlich gilt auch für die Produzentenhaftung im Deliktsrecht die zivilprozessrechtliche Beweislastverteilung. Der Geschädigte muss also alle anspruchsbegründenden Umstände

---

[559] Vgl. §§ 434 ff. BGB

[560] Zum Gewährleistungsausschluss durch AGB s. § 308 Nr. 8 lit. b BGB. Hierzu Wurmnest, in: Münchener Kommentar zum BGB, Bd. 2, 6. Aufl. 2012, § 308 Nr. 8 Rn. 4; Becker in: Bamberger/Roth, BGB, 3.Aufl. 2012, § 309 Nr. 8 BGB Rn. 20 ff.

[561] S. dazu oben Abschnitt II.2.3.3.3, dort Absatz: Deliktische Haftung gemäß § 823 Absatz 1 BGB.

[562] Grundlegend zu diesem Thema BGHZ 51, 91 ff.

[563] So schon Lehmann, Produkt- und Produzentenhaftung für Software, NJW 1992, 1721, 1722; Hohmann,Haftung der Softwarehersteller für das „Jahr 2000"-Problem, NJW 1999, 521, 524 f.; Moritz in: Kilian/Heussen, Computerrecht, Stand 30. EL 2011, Rn. 240.

[564] Grundlegend hierzu BGHZ 92, 143 ff.

[565] BGH Urteil vom 09. 12. 1986 - VI ZR 65/86NJW 1987, 1009; BGH NJW 1286, 1287; BGH NJW 1994, 3349; BGH NJW 1999, 2273.

beweisen, soweit ihm keine Beweiserleichterungen oder eine Beweislastumkehr zugutekommen.[566]

Die Verteilung der Beweislast ist aus praktischer Sicht besonders bedeutsam. Auch für IT-Produkte gelten die von der Rechtsprechung entwickelten Beweislastgrundsätze im Rahmen der Produzentenhaftung.[567] Dies bedeutet, dass zugunsten des Geschädigten eine weitreichende Beweislastumkehr gilt. Hinsichtlich der objektiven Verkehrspflichtverletzung und auch des Verschuldens muss der Produzent sich entlasten.[568] Indes obliegt dem Geschädigten die Beweislast für die Kausalität zwischen Produktfehler oder Verkehrspflichtverletzung für die eingetretene Rechtsgutsverletzung.[569]

II.2.3.3.3.2.3 Außervertragliche Verschuldenshaftung nach § 823 Absatz 2 BGB

In Frage kommt zudem eine Haftung gemäß § 823 Absatz 2 BGB in Verbindung mit der Verletzung eines Schutzgesetzes. Als Schutzgesetz im Sinne von § 823 Absatz 2 BGB kommen hier insbesondere die Pflichten des Herstellers nach dem Gesetz über die Bereitstellung von Produkten auf dem Markt (Produktsicherheitsgesetz, ProdSG) in Betracht.[570] Das bedeutet, das Bereitstellen eines Produktes auf dem Markt, ohne dass dieses gemäß § 3 Absatz 1 und 2 ProdSG die erforderliche Sicherheit aufweist, kann eine Haftung nach § 823 Absatz 2 BGB auslösen.

II.2.3.3.3.2.4 Außervertragliche, verschuldensunabhängige Haftung nach dem Produkthaftungsgesetz

Neben die verschuldensabhängige Haftung des allgemeinen Deliktsrechts tritt die verschuldensunabhängige Haftung nach dem Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz, ProdHaftG)[571] für Körper-, Gesundheits- und Sachschäden.

---

[566] Hager, in: Staudinger, §§ 823 E-I, 824, 825, 2009, § 823 Rn. F 39.

[567] Spindler, IT-Sicherheit und Produkthaftung – Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer, NJW 2004, 3145, 3146.

[568] Wagner, in: Münchener Kommentar zum BGB, Bd. 5, 5. Aufl. 2009, § 823 BGB Rn. 658; BGH NJW 1999, 1028, 1029.

[569] Wagner, in: Münchener Kommentar zum BGB, Bd. 5, 5. Aufl. 2009, § 823 BGB Rn. 658; BGH NJW 1988, 2611, 2613.

[570] Dazu unten Abschnitt II.2.3.3.3, dort Absatz: Öffentlich-rechtliche Regelung der Produktsicherheit nach dem Produktsicherheitsgesetz.

[571] Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz, ProdHaftG) vom 15. Dezember 1989 (BGBl. I S. 2198), zuletzt geändert durch Artikel 9 Absatz 3 des Gesetzes vom 19. Juli 2002 (BGBl. I S. 2674) sowie Richtlinie des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte, ABl. Nr. L 210 vom 7.8.1985, S. 29; auf der Grundlage der Produkthaftungsrichtlinie ist das deutsche Produkthaftungsgesetz erlassen worden.

Die Beweislast für den Fehler, den Schaden und den ursächlichen Zusammenhang trägt jedoch gemäß § 1 Absatz 4 ProdHaftG der Geschädigte.

Hardware unterliegt grundsätzlich den Bestimmungen des Produkthaftungsgesetzes. Für Software wird dies angenommen, wenn diese auf einem Datenträger wie einer Diskette oder einer CD-ROM gespeichert oder auf andere Weise verkörpert ist.[572] Diese Einschätzung teilt auch die EU-Kommission.[573]

Streitig ist jedoch noch die Produkteigenschaft im Sinne des Produkthaftungsgesetzes (und damit auch die Haftbarkeit des Herstellers) in Bezug auf online übertragene Software.[574] Entscheidend ist dabei die Auslegung des Begriffs der Sache im Sinne von § 2 ProdHaftG, der an den Sachbegriff des § 90 BGB anknüpft und folglich eine Verkörperung voraussetzt. Eine Ansicht verneint vor diesem Hintergrund die Produkteigenschaft im Sinne des Produkthaftungsgesetzes von online übertragener Software.[575] Eine andere stellt auf den verbraucherschützenden Zweck des Produkthaftungsgesetzes ab und nimmt zumindest dann eine Haftung an, wenn die Software nach dem Übertragungsvorgang beim Nutzer dauerhaft durch Speicherung auf einem Datenträger verkörpert wird.[576]

Nach dem Produkthaftungsgesetz hat der Hersteller insbesondere die Pflicht, seine Software so zu konstruieren, dass sie zumindest für bekannte Gefahren nicht anfällig ist.[577] Verstößt er gegen diese Pflicht, kann das im äußersten Fall dazu führen, dass ein Produkt nicht in den Handel gebracht werden kann, wenn die Gefährdung nicht behebbar ist.[578] Die

---

[572] Spindler/Klöhn, Fehlerhafte Informationen und Software – Die Auswirkungen der Schuld- und Schadensrechtsreform, VersR 2003, 410, 412; Mankowski, in: Ernst, Hacker, Cracker & Computerviren, 2004, Rn. 441; Marly, Softwareüberlassungsverträge, 4. Aufl. 2004, Rn. 1303; Sodtalbers, Softwarehaftung im Internet, 2006, Rn. 161; Koch, Versicherbarkeit von IT-Risiken, 2005, Rn. 607; Sprau, in: Palandt, 71. Aufl. 2012, § 2 ProdHaftG Rn. 1; Schiermann, in: Erman, 13. Aufl. 2011, § 2 ProdHaftG Rn. 2; Wagner, in: Münchener Kommentar zum BGB, Bd. 5, 5. Aufl. 2009, § 2 ProdHaftG Rn. 15.

[573] Stellungnahme der Kommission der Europäischen Gemeinschaften auf die Schriftliche Anfrage Nr. 706/88 von Herrn Gijs de Vries an die Kommission: Produkthaftung für Computerprogramme, v. 8.5.1989, ABl. Nr. C 114 vom 8.5.1989, S. 42.

[574] Dafür Spindler/Klöhn, Fehlerhafte Informationen und Software – Die Auswirkungen der Schuld- und Schadensrechtsreform, VersR 2003, 410, 412; Sodtalbers, Softwarehaftung im Internet, 2006, Rn. 164 ff.; Koch, Versicherbarkeit von IT-Risiken, 2005, Rn. 607; Mankowski, in: Ernst, Hacker, Cracker & Computerviren, 2004, Rn. 441; Wagner, in: Münchener Kommentar zum BGB, Bd. 5, 5. Aufl. 2009, § 2 ProdHaftG Rn. 16; dagegen Schiemann, in: Erman, 13. Aufl. 2011, § 2 ProdHaftG Rn. 2; Oechsler, in: Staudinger, §§ 826-829; ProdHaftG, 2009, § 2 ProdHaftG Rn. 65, 69a.

[575] Oechsler, in: Staudinger, §§ 826-829; ProdHaftG, 2009, § 2 ProdHaftG Rn. 11, 66.

[576] Spindler/Klöhn, Fehlerhafte Informationen und Software – Die Auswirkungen der Schuld- und Schadensrechtsreform, VersR 2003, 410, 412; Mankowski, in: Ernst, Hacker, Cracker & Computerviren, 2004, Rn. 441; Wagner, in: Münchener Kommentar zum BGB, Bd. 5, 5. Aufl. 2009, § 2 ProdHaftG Rn. 16.

[577] Vgl. Foerste, in: Foerste/Graf von Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 104 ff.

[578] Wagner, in: Münchener Kommentar zum BGB, Bd. 5, 5. Aufl. 2009, § 823 BGB Rn. 629; Oechsler, in: Staudinger, §§ 826-829; ProdHaftG, 2009, § 3 ProdHaftG Rn. 109.

Konstruktionspflichten der Hersteller orientieren sich stets am Stand der Technik zur Zeit der ersten Inverkehrgabe des Produktes.[579] Der Hersteller darf aber nicht sehenden Auges mit der Inverkehrgabe fortfahren, wenn nach diesem Zeitpunkt Sicherheitslücken bekannt werden, die die jeweilige Software betreffen und behebbar sind, denn diese entspricht dann nicht mehr dem Stand der Wissenschaft und Technik. Der Stand von Wissenschaft und Technik ist ein unbestimmter Rechtsbegriff, der der Ausfüllung bedarf.[580] Für die Ausfüllung dieser unbestimmten Rechtsbegriffe und damit die Pflichtenbestimmung im Bereich der Produkthaftung sind Standards, welche in überbetrieblichen technischen Normen niedergelegt sind, von herausragender Bedeutung. Diese Regeln werden regelmäßig von Privaten verfasst, etwa vom Deutschen Institut für Normung (DIN) e.V. oder europäischen Normungsorganisationen, und haben folglich nicht die Qualität von Rechtsnormen.[581] Ihnen kommt jedoch insofern erhebliche Bedeutung zu, als der Bundesgerichtshof in ständiger Rechtsprechung ihre Verwendung für maßgeblich bei der Bestimmung des anerkannten Stands von Wissenschaft und Technik nach der allgemeinen Verkehrsauffassung erachtet.[582] Diese technischen Normen stellen folglich eine Vermutungswirkung auf, die entfällt, wenn die in den Normen enthaltenen Standards unterschritten werden.[583] Auch die Einhaltung von anerkannten Normen entbindet die Hersteller jedoch nicht davon, selbstständig zu überprüfen, ob ihre Maßnahmen im Einzelfall ausreichen.[584] Wann von den Herstellern gefordert werden kann, über die üblichen Standards hinauszugehen, ist eine Frage des Einzelfalles.

---

[579] Zur Relevanz des Standes von Wissenschaft und Technik für die Produkthaftung bei fehlerhaften Computerprogrammen: Littbarski, in: Kilian/Heussen, Computerrechts-Handbuch, Stand: 30. EL 2011, Kap. 180 Rn. 53. Eingehend zum Konstruktionsfehler als Programmierfehler Taeger, Außervertragliche Haftung für fehlerhafte Computerprogramme, 1995, S. 244 ff.; Günther, Produkthaftung für Informationsgüter, 2001, S. 300 f.; Meier/Wehlau, Produzentenhaftung des Softwareherstellers, CR 1990, 95, 96; Reese, Produkthaftung und Produzentenhaftung für Hard- und Software, DStR 1994, 1121, 1123.

[580] Kersting in: Landmann/Rohmer, Umweltrecht, Bd. II, Stand: 63. EL 2012, § 3 KrW-/AbfG Rn. 116.

[581] Spindler, in: Bamberger/Roth, BGB, 3. Aufl. 2012, § 823 BGB Rn. 255; Wagner, in: Münchener Kommentar zum BGB, Bd. 5, 5. Aufl. 2009, § 823 BGB Rn. 578.

[582] BGH NJW 2004, 1449, 1450; BGH NJW-RR 2002, 525, 526; BGH NJW 2001, 2019, 2020; BGH VersR 1988, 632, 633; Spindler, in: Bamberger/Roth, BGB, 3. Aufl. 2012, § 823 BGB Rn. 255; Wagner, in: Münchener Kommentar zum BGB, Bd. 5, 5. Aufl. 2009, § 823 BGB Rn. 272; Reiff, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, 2006, S. 159, 161 ff.

[583] BGH NJW 1988, 2667, 2668; BGH VersR 1984, 270; BGH VersR 1972, 767, 768; OLG Celle NJW 2003, 2544; Köhler, Die haftungsrechtliche Bedeutung technischer Regeln, BB 1985, Heft 4, Beil., 10, 11; Foerste, in: Foerste/Graf von Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 42 ff.; Spindler, Unternehmensorganisationspflichten, 2. Aufl. 2011, S. 803, 805.

[584] BGH NJW 1987, 372; OLG Zweibrücken NJW 1977, 111, 111 f.; Marburger, Die haftungs- und versicherungsrechtliche Bedeutung technischer Regeln, VersR 1983, 597, 600; Spindler, Unternehmensorganisationspflichten, 2. Aufl. 2011, S. 805.

II.2.3.3.3.2.5 Öffentlich-rechtliche Regelung der Produktsicherheit nach dem Produktsicherheitsgesetz

Neben die zivilrechtliche Haftung des IT-Herstellers als Steuerungsinstrument der (IT-)Produktsicherheit treten zahlreiche öffentlich-rechtliche Normen. Neben einzelnen Spezialgesetzen wie dem Gesetz über Medizinprodukte (Medizinproduktegesetz, MPG)[585] erscheint insbesondere das kürzlich mit Wirkung zum 1. Dezember 2011 erlassene Produktsicherheitsgesetz[586] relevant. Dieses ersetzt künftig das bisherige Geräte- und Produktsicherheitsgesetz[587] (GPSG). Durch den zukünftig zu erwartenden Anstieg der Verwendung von Embedded Software, beispielsweise im Automobilbereich, werden schließlich auch im Verbraucherbereich Personenschäden denkbar, weshalb dem Produktsicherheitsgesetz zukünftig eine gesteigerte Bedeutung zukommen dürfte.

Zentraler Aspekt des das Produktsicherheitsrecht prägenden „New Approach“[588] ist die Beschränkung des Eingreifens des Staates auf das nötige Mindestmaß, um der Industrie größtmöglichen Spielraum zu geben. Die in diesem Rahmen besonders hervorzuhebende Verordnung (EG) 765/2008 hat in Deutschland auch Änderungen im materiellen Produktsicherheitsrecht angestoßen, die sich nun im neuen Produktsicherheitsgesetz niederschlagen.

Ein Produkt darf gemäß § 3 Absatz 1 und 2 ProdSG nur dann „auf dem Markt bereitgestellt werden“, wenn es „bei bestimmungsgemäßer oder vorhersehbarer Verwendung die Sicherheit und Gesundheit von Personen nicht gefährdet“. Produkte im Sinne des Gesetzes sind gemäß § 2 Nummer 22 ProdSG „Waren, Stoffe oder Zubereitungen, die durch einen Fertigungsprozess hergestellt worden sind“. § 3 Absatz 3 bis 5 ProdSG statuieren für bestimmte Konstellationen zusätzliche Hinweispflichten beziehungsweise die Pflicht, dem Produkt Gebrauchsanweisungen beizufügen. § 6 ProdSG enthält wiederum diverse zusätzliche Vorgaben in Bezug auf die Bereitstellung von Verbraucherprodukten. Dies sind gemäß § 2 Nummer 26 ProdSG „neue, gebrauchte oder wiederaufgearbeitete Produkte, die für

---

[585] Gesetz über Medizinprodukte in der Fassung der Bekanntmachung vom 7. August 2002 (BGBl. I S. 3146), zuletzt geändert durch Artikel 13 des Gesetzes vom 8. November 2011 (BGBl. I S. 2178).

[586] Gesetz über die Bereitstellung von Produkten auf dem Markt (Produktsicherheitsgesetz – ProdSG) vom 8. November 2011 (BGBl. I S. 2178).

[587] Gesetz über technische Arbeitsmittel und Verbraucherprodukte vom 6. Januar 2004 (BGBl. I S. 2, 219), zuletzt geändert durch Artikel 2 des Gesetzes vom 7. März 2011 (BGBl. I S. 338).

[588] Hierzu eingehend: Klindt, Der „new approach” im Produktrecht des europäischen Binnenmarkts: Vermutungswirkung technischer Normung, EuZW 2002, 133; Kapoor/Klindt, „New Legislative Framework“ im EU-Produktsicherheitsrecht – Neue Marktüberwachung in Europa?, EuZW 2008, 649.

Verbraucher bestimmt sind oder unter Bedingungen, die nach vernünftigem Ermessen vorhersehbar sind, von Verbrauchern benutzt werden könnten, selbst wenn sie nicht für diese bestimmt sind“ oder Produkte, „die dem Verbraucher im Rahmen einer Dienstleistung zur Verfügung gestellt werden“. Die Überwachung der Einhaltung dieser Vorschriften obliegt gemäß § 24 Absatz 1 Satz 1 ProdSG den nach Landesrecht zuständigen Behörden. Diese können gemäß § 26 Absatz 2 Satz 1 ProdSG die erforderlichen Maßnahmen treffen und sich dabei insbesondere der in § 26 Absatz 2 Satz 2 ProdSG aufgeführten Standardmaßnahmen bedienen.

Adressaten der spezifischen Regelungen des § 6 ProdSG zu Verbraucherprodukten sind ausschließlich der Hersteller, der von diesem für bestimmten Aufgaben Beauftragte (Bevollmächtigter im Sinne von § 2 Nummer 6 ProdSG) sowie der Importeur. Wie sich aus § 27 Absatz 1 Satz 1 ProdSG ergibt, richtet sich die Generalklausel des § 3 Absatz 1 und 2 ProdSG hingegen an alle Wirtschaftsakteure im Sinne von § 2 Nummer 29 ProdSG, das heißt zusätzlich auch an den Händler von Produkten.

Inwieweit IT-Produkte, das heißt Hardware und Software, unter das Produktsicherheitsgesetz fallen, ist insofern nicht abschließend zu beantworten, als mit der Ablösung des Geräte- und Produktsicherheitsgesetzes durch das Produktsicherheitsgesetz auch der maßgebliche Begriff des „Produkts“ (zumindest im Wortlaut der Legaldefinition) eine Änderung erfahren hat. Waren im Geräte- und Produktsicherheitsgesetzes mit Produkten noch „technische Arbeitsmittel“ und „Verbraucherprodukte“ gemeint, definiert § 2 Nummer 22 ProdSG den Begriff nun als „Waren, Stoffe oder Zubereitungen, die durch einen Fertigungsprozess hergestellt worden sind“. Der Gesetzesbegründung zufolge soll diese Änderung jedoch nur der Klarstellung dienen und sich aus ihr keine inhaltliche Änderung ergeben.[589] Sämtliche verkörperten Gegenstände, die durch einen Fertigungsprozess hergestellt worden sind, damit auch Hardware, lassen sich unter den Produktbegriff fassen. Außerdem lässt sich der Datenträger unter den Produktbegriff des § 2 Nummer 22 ProdSG subsumieren, auf dem Software gegebenenfalls gespeichert ist.[590] Es lässt sich zudem differenzieren zwischen Embedded Software, das heißt solcher, die in ein Endprodukt integriert ist und Steuerungsfunktionen erfüllt, und Software, die sich selbstständig nutzen lässt.

---

[589] BR-Drs. 314/11, S. 74.

[590] Hoeren/Ernstschneider, Das neue Geräte- und Produktsicherheitsgesetz und seine Anwendung auf die IT-Branche, MMR 2004, 507, 508; Wilrich, Geräte- und Produktsicherheitsgesetz (GPSG), 2004, § 2 GPSG Rn. 10.

Embedded Software nimmt aufgrund ihrer Steuerungsfunktion und Integrierung in das jeweilige Endprodukt an dessen Produkteigenschaft ohne Weiteres teil, da sie als fester Bestandteil dessen anzusehen ist.[591] Für selbstständige Software wurde in der Literatur zum Geräte- und Produktsicherheitsgesetz zum Teil vertreten, dass diese zumindest dann dem Produktbegriff unterfällt, wenn sie auf einem Datenträger gespeichert und somit verkörpert ist.[592] Die wohl herrschende Meinung stellt hingegen – vergleichbar der ähnlichen Problematik im Produkthaftungsgesetz [593] – auf Sinn und Zweck der Regelung ab, der darin besteht, Verbraucher und Arbeitnehmer vor Gesundheitsschäden durch nicht hinreichend sichere Konsumgüter zu schützen. Daran gemessen ist auch selbstständige Software unter den Produktbegriff des § 2 Nummer 22 ProdSG zu fassen, soweit sie „gefährlich“ sein kann, unabhängig von der Art der Speicherung oder Übertragung.[594] Soweit der Anwendungsbereich des Produktsicherheitsgesetzes für IT-Produkte in sachlicher Hinsicht eröffnet ist, ist aufgrund des genannten Schutzzwecks dennoch wiederum eine Einschränkung der Verantwortlichkeit zu beachten. Gemäß § 3 Absatz 1 und 2 ProdSG wird nur die „Sicherheit und Gesundheit von Personen“ geschützt. Nicht erfasst werden daher bloße Eigentums- und Vermögensschäden.[595] Der Schutzbereich kann allenfalls durch Rechtsverordnungen nach § 8 Absatz 1 ProdSG auch auf andere Rechtsgüter erweitert werden.[596] Durch diese Einschränkung ist der gerade im IT-Bereich praktisch relevante Bereich der Eigentums- und Vermögensschäden grundsätzlich vom Schutz des Produktsicherheitsgesetzes ausgenommen. Standardsoftware für Verbraucher wird in der Regel gerade keine Personenschäden verursachen. Solche dürften stattdessen eher im Arbeitsbereich auftreten, wenn Maschinen aufgrund von Softwarefehlern oder Sicherheitslücken Personen schädigen. Dies wird sich jedoch, wie eingangs bereits

---

[591] Runte/Potinecke, Software und GPSG, CR 2004, 725, 726; Zscherpe/Lutz, Geräte- und Produktsicherheitsgesetz: Anwendbarkeit auf Hard- und Software, K&R 2005, 499, 500.

[592] Hoeren/Ernstschneider, Das neue Geräte- und Produktsicherheitsgesetz und seine Anwendung auf die IT-Branche, MMR 2004, 507, 508; Zscherpe/Lutz, Geräte- und Produktsicherheitsgesetz: Anwendbarkeit auf Hard- und Software, K&R 2005, 499, 500; offen lassend Wilrich, Geräte- und Produktsicherheitsgesetz (GPSG), 2004, § 2 GPSG Rn. 10.

[593] Oben Abschnitt II.2.3.3.3, dort Absatz: Außervertragliche, verschuldensunabhängige Haftung nach dem Produkthaftungsgesetz.

[594] Zur Lage nach dem GPSG: Runte/Potinecke, Software und GPSG, CR 2004, 725, 727; Zscherpe/Lutz, Geräte- und Produktsicherheitsgesetz: Anwendbarkeit auf Hard- und Software, K&R 2005, 499, 500; Klindt, Geräte- und Produktsicherheitsgesetz (GPSG), 2007, § 2 GPSG Rn. 13.

[595] Zur Lage nach dem GPSG: Wilrich, Geräte- und Produktsicherheitsgesetz (GPSG), 2004, Einleitung Rn. 6.

[596] Zur entsprechenden Regelung im GPSG: Wilrich, Geräte- und Produktsicherheitsgesetz (GPSG), 2004, Einleitung Rn. 6, § 3 GPSG Rn. 3.

angemerkt, durch den zu erwartenden Anstieg von Embedded Software voraussichtlich ändern.beispielsweise

II.2.3.3.3.2.6 Zusammenfassung Haftung des IT-Herstellers

Im vorangegangenen Abschnitt wurden Fragen der Haftung von IT-Herstellern dargestellt. Trotz der Vielzahl der Anspruchsgrundlagen kann es im Einzelfall möglich sein, dass eine Haftung durch den IT-Hersteller nicht vorliegt. Im Rahmen der vertraglichen Haftung sind die Grenzen möglicher Konstruktionen durch das Verbraucherschutz- und AGB(Allgmeine Geschäftsbedinungen)-Recht gezogen. Eine direkte Haftung der Hersteller gegenüber dem Kunden wird jedoch nicht immer gegeben sein. Häufig wird der Endnutzer sein Softwareprodukt auch von einem Händler erwerben. Die vertraglichen Pflichten bestehen dann gegenüber diesem.

Im Bereich der deliktischen Haftung sind noch einige juristische Fragen ungeklärt. Zum einen ist der Anwendungsbereich verschiedenster Anspruchsgrundlagen für Daten umstritten, insbesondere in den Fällen, in denen keine Speicherung und somit auch keine Verkörperung erfolgt. Dies wirft auch Fragen hinsichtlich der Haftung im Bereich des Cloud Computing auf. Weiter sind die Hersteller von IT-Produkten nur in beschränktem Maße verpflichtet, die Nutzerinnen und Nutzer gegen Angriffe Dritter auf die IT zu schützen. Sie haben sich, wie jeder andere Hersteller, im Rahmen der deliktischen Produzentenhaftung und des Produkthaftungsgesetzes zu halten. Eine darüber hinausgehende Verpflichtung lässt sich nicht herleiten.

Der Anwendungsbereich des Produktsicherheitsgesetzes ist in Bezug auf IT-Produkte unproblematisch für Hardware und zumindest weitestgehend für Software eröffnet. Allerdings schützt das Produktsicherheitsgesetzes grundsätzlich nur vor Personenschäden, nicht hingegen Eigentums- und Vermögensschäden.

II.2.3.3.3.3 Haftung des IT-Nutzers

Wie oben gezeigt,[597] geht die größte Bedrohung für die IT-Sicherheit von konzertierten Angriffen mittels Botnetzen aus. An diese Botnetze angeschlossen sind oft auch private Computer, die vom Betreiber des Botnetzes ferngesteuert werden, ohne dass der Nutzer davon Kenntnis hat. Diesen Angriffen wäre der Boden entzogen, wenn es für die Betreiber der Botnetze nicht mehr möglich wäre, weitere Rechner („Bots“) zu infizieren. Eine

[597] S.o. Abschnitt II.2.1.5.1.

Verbesserung der IT-Sicherheit auf Seiten der Anwender verspricht deshalb die allgemeine IT-Sicherheitslage zu verbessern. Zu einer Haftung des IT-Nutzers kann es einerseits auf vertraglicher Grundlage und andererseits außervertraglich auf Grundlage des allgemeinen Deliktsrechts kommen. Die juristische Debatte steht hierzu jedoch noch am Anfang. Gesicherte Auffassungen dazu, welche Verkehrssicherungspflichten den IT-Nutzer im Rahmen der deliktischen Haftung treffen, gibt es daher noch nicht. Allerdings hat sich der Bundesgerichtshof in einer Entscheidung zur Haftung als Betreiber eines WLAN-Netzes geäußert.[598]

II.2.3.3.3.3.1 Vertragliche Haftung im Arbeitsverhältnis

Im Allgemeinen ist eine vertragliche Haftung des privaten IT-Nutzers in der Regel nicht denkbar.[599]

Eine Ausnahme bildet hier die Haftung innerhalb eines Arbeitsverhältnisses. Dieser kommt aufgrund der Tatsache, dass Arbeitnehmer in vielen Branchen mittlerweile ihre privaten Endgeräte auch beruflich einsetzen (Stichwort: BYOD – Bring Your Own Device), eine gesteigerte Bedeutung zu. Kommt es im beruflichen Rahmen zur Nutzung von Hardware oder Software, die im Eigentum des Arbeitgebers steht, oder ist solche auf andere Weise dem Einfluss des Arbeitnehmers ausgesetzt (beispielsweise indem sie mit einem Computer oder internetfähigen Handy des Arbeitnehmers vernetzt ist), sind die allgemeinen Grundsätze über die Haftung von Arbeitnehmern[600] anwendbar. Gleiches gilt, wenn durch den Einsatz von privater Hard- oder Software durch den Mitarbeiter dem Arbeitgeber oder einem Dritten Schäden entstehen.

II.2.3.3.3.3.2 Außervertragliche Verschuldenshaftung gemäß § 823 BGB

Hingegen ergibt sich die Möglichkeit einer Verschuldenshaftung gegenüber Dritten aufgrund von § 823 BGB, insbesondere dessen Absatz 1. Anknüpfungspunkt für die Haftung kann beispielsweise sein, dass der Nutzer fahrlässig Viren oder andere schadhafte Programme[601] an die Endgeräte Dritter verbreitet, weil er seinen Rechner nicht ausreichend gegen Angreifer geschützt hat und dieser in der Folge in ein Botnetz eingebunden wurde.[602]

---

[598] Siehe unten – Fußnote 612.

[599] Spindler, in: Lorenz, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2010, S. 57.

[600] BAG GS Beschluss vom 27.09.1994 – GS 1/89; NZA 1994, 1083 m.w.N.

[601] Zu den einzelnen Bedrohungen und Angriffsformen oben Abschnitte II.2.1.5 und II.2.1.6.

[602] Spindler, in: Lorenz, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2010, S. 57 f.

Das Vorliegen einer in einem solchen Fall von mittelbarer Schädigung oder Schädigung durch Unterlassen für die Haftungsbegründung erforderlichen Verletzung einer Verkehrssicherungspflicht ist einerseits vom Einzelfall abhängig, andererseits aber auch insofern problematisch, als die Verkehrssicherungspflichten von IT-Nutzern im Allgemeinen noch nicht abschließend geklärt sind.[603] Während IT-Hersteller, wie oben dargestellt,[604] eine Verkehrssicherungspflicht aufgrund der Schaffung einer Gefahrenquelle trifft, kann aber zumindest für den Nutzer eines bereits kompromittierten IT-Systems (das heißt auch schon eines einzelnen Rechners) eine Verkehrssicherungspflicht aufgrund der Beherrschung einer Gefahrenquelle angenommen werden.[605] Er ist mithin verpflichtet, die notwendigen und zumutbaren Vorkehrungen zu treffen, um eine Schädigung anderer durch die Gefahrenquelle zu verhindern.[606] Diese Pflicht kann allerdings nicht so weit verstanden werden, dass es eine allgemeine Fürsorgepflicht für Dritte gäbe. Es bedarf stets einer konkreten Pflichtenlage zum Schutz der Rechtsgüter eines Dritten, um eine Verkehrssicherungspflicht annehmen zu können.[607]

Zu berücksichtigen ist jedoch, dass den Geschädigten aufgrund eines eigenen Versagens beim Schutz seiner IT und der daraus resultierenden Infektionsanfälligkeit ein Mitverschulden treffen kann, das grundsätzlich nach denselben Maßstäben zu beurteilen ist wie das Verschulden des Schädigers und dessen Haftungsumfang schließlich abmildert.[608] Insofern stehen sich Selbst- und Fremdschutzpflichten quasi spiegelbildlich gegenüber.[609]

Bei der Frage, welche Sorgfaltspflichten im Einzelnen an die Nutzer von IT-Systemen zu stellen sind, ist grundsätzlich auf die berechtigten Erwartungen der betroffenen Verkehrskreise abzustellen.[610] Ob Erwartungen berechtigt sind, richtet sich maßgeblich nach

---

[603] Spindler, in: Lorenz, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2010, S. 58.

[604] S.o. Kapitel II.2.3.3.3, dort Absatz: Außervertragliche Verschuldenshaftung nach § 823 Abs. 1I BGB.

[605] Spindler, in: Lorenz, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2010, S. 58.

[606] Spindler, in: Bamberger/Roth, BGB, 3. Aufl. 2012, § 823 Rn. 24.

[607] Spindler, in: Bamberger/Roth, BGB, 3. Aufl. 2012, § 823 Rn. 227; Koch, Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, 801, 803.

[608] S. dazu Spindler, in: Lorenz, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2010, S. 60.

[609] Spindler, in: Lorenz, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2010, S. 68; Libertus, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, MMR 2005, 507, 509.

[610] BGH NJW-RR 2002, 525, 526; BGH NJW 1978, 1629; BGH NJW 1990, 906, 907; Spindler, in: Bamberger/Roth, BGB, 3. Aufl. 2012, § 823 Rn. 234; Libertus, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, MMR 2005, 507, 509; Koch, Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, 801, 804.

der technischen und wirtschaftlichen Zumutbarkeit.[611] Eine grobe Unterscheidung lässt sich zudem vornehmen zwischen privaten Nutzern und solchen, die IT-Systeme ihrerseits professionell einsetzen.

Verkehrssicherungspflichten privater IT-Nutzer

Für den Umfang der möglichen Verkehrssicherungspflichten eines privaten Betreibers eines IT-Systems hat der Bundesgerichtshof bisher in seiner WLAN-Entscheidung grundlegende Vorgaben gemacht.[612] Wendet man die dort entwickelten Grundsätze an, kann man davon ausgehen, dass von Privaten verlangt werden kann, solche Sicherungsmaßnahmen zu treffen, die ohne großen Aufwand und nähere technische Kenntnisse aktiviert werden können.[613] Insofern werden auf jeden Fall die Aktivierung von Firewalls und die Nutzung von Virenscannern verlangt werden können,[614] ebenso wie das Einspielen von vom Softwarehersteller bereitgestellten Patches. Von einem pauschalen Ausschluss der Verkehrssicherungspflichten privater IT-Nutzer, die als Sender elektronischer Kommunikation unter Umständen Computerviren verbreiten, wie vereinzelt vertreten wurde, kann demzufolge nicht mehr ausgegangen werden.[615]

Verkehrssicherungspflichten professioneller IT-Nutzer

Professionelle Nutzer von IT-Technik, wie etwa Unternehmen, sind grundsätzlich denselben Bedrohungen ausgesetzt wie private Nutzer. Ein wesentlicher Unterschied ergibt sich jedoch daraus, dass ihnen im Hinblick auf ihre Verkehrssicherungspflichten ein größeres Maß an Sicherheitsvorkehrungen zugemutet werden kann. Dies ergibt sich daraus, dass ein Unternehmen, das IT-Technik gezielt und umfangreich zur Erledigung seiner Geschäfte einsetzt, zum einen eine größere Gefahrenquelle schafft beziehungsweise beherrscht und zum

---

[611] Koch, Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, 801, 804; Libertus, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, MMR 2005, 507, 509; Spindler, in: Bamberger/Roth, BGB, 3. Aufl. 2012, § 823 Rn. 240.

[612] BGH GRUR 2010, 633.

[613] Zwar war Gegenstand der zugrunde liegenden BGH-Entscheidung nicht die Haftung wegen einer Verkehrssicherungspflichtverletzung, sondern die Frage nach der Störerhaftung, aber das Urteil lässt den Schluss zu, dass diese Störerhaftung auf der Verletzung einer Verkehrssicherungspflicht beruht. So auch Stang/Hühner, Störerhaftung des WLAN-Inhabers, Anmerkung zu BGH, Urt. v. 12.5.2010 – I ZR 121/08 – Sommer unseres Lebens, GRUR 2010, 633, 636.

[614] Siehe näher hierzu: Spindler, in: Lorenz, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2010, S. 61; Libertus, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, MMR 2005, 507, 509.

[615] So aber Koch, Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, 801, 805; dagegen bereits Libertus, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, MMR 2005, 507, 509 f.

anderen von ihm auch technisches Know-How und finanzielle Mittel erwartet werden können.[616] Insofern könnten sich die zu erwartenden Maßnahmen u. a. auch an der Größe des Unternehmens zu orientieren. Von Einfluss auf die zu erwartenden Sicherheitsmaßahmen ist schließlich auch die Frage, in welchem Maße das Unternehmen mit welchen Rechtsgütern Dritter über seine IT-Technik in Kontakt kommt.[617]

Auf der anderen Seite ist in die berechtigten Erwartungen der betroffenen Verkehrskreise auch einzubeziehen, inwieweit beispielsweise den Empfängern elektronischer Kommunikation (E-Mails etc.) zuzumuten ist, sich selbst vor Computerviren zu schützen. Auch in dieser Hinsicht ist Unternehmen mehr Aufwand zuzumuten als Privatpersonen, weshalb vereinzelt vertreten wurde, dass in der elektronischen B2B-Kommunikation das sendende Unternehmen keine Verkehrssicherungspflicht gegenüber dem empfangenden Unternehmen treffe, da dessen Selbstschutz vorausgesetzt werden dürfe.[618] Da in der Regel aber jedes Unternehmen nicht nur Sender, sondern zugleich auch Empfänger elektronischer Kommunikationsmittel ist, läuft es zwangsläufig auf eine Pflicht zur Einrichtung geeigneter – und gegenüber privaten Nutzern wirksamerer – Schutzmittel hinaus, sei es in Form der Verkehrssicherungspflicht oder in Form der Pflicht zum Selbstschutz.[619]

II.2.3.3.4 Infrastrukturbezogene Regelungen

Die §§ 108ff. des Telekommunikationsgesetzes (TKG) dienen dem Schutz der öffentlichen Sicherheit. Vornehmlich sind im TKG die Regelungsadressaten die Betreiber von Telekommunikationsanlagen. Nach § 109 Absatz 1 TKG wird jedoch auch jeder Telekommunikationsdiensteanbieter dazu verpflichtet, Maßnahmen und technische Vorkehrungen zum Schutze des Fernmeldegeheimnisses und personenbezogener Daten zu ergreifen, sowie solche Maßnahmen zu treffen, die unerlaubte Zugriffe auf Telekommunikations- und Datenverarbeitungssysteme verhindern. Damit soll sowohl die

---

[616] Spindler, in: Lorenz, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2010, S. 65; Libertus, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, MMR 2005, 507, 509.

[617] Spindler, in: Lorenz, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2010, S. 65; es wird darauf hingewiesen, dass die Projektgruppe „Demokratie und Staat“ der Enquete-Kommission sich u.a. mit der Frage einer obligatorischen Verschlüsselung elektronischer Kommunikation im Justiz-Bereich beschäftigt.

[618] Koch, Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, 801, 805.

[619] Zu der Spiegelbildlichkeit beider Pflichten s. bereits oben II.2.3.3.3, dort Abschnitt: Außervertragliche Verschuldenshaftung gemäß § 823 BGB und Fußtnote 608.

Vertraulichkeit der Telekommunikation, als auch der störungsfreie Betrieb gewährleistet werden.[620]

Die Betreiber von Telekommunikationsanlagen sind gemäß § 109 Absatz 2 TKG dazu verpflichtet, angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen, u. a. zum Schutz gegen äußere Angriffe. Dabei geht es in erster Linie um Datensicherung, sodass Daten vor Beschädigung, Zerstörung, Verlust oder unbefugter Veränderung und Missbrauch, also vor Angriffen von Außenstehenden[621] oder unberechtigter Datenverwendung von Mitarbeitern, geschützt sind.[622] Welche Maßnahmen als angemessen im Sinne des § 109 Absatz 2 TKG anzusehen sind, bestimmt sich nach dem Einzelfall.[623]

Um zu bestimmen, welche Maßnahmen in Betracht kommen, muss der Betreiber gemäß § 109 Absatz 4 TKG einen Sicherheitsbeauftragten benennen und ein Sicherheitskonzept erarbeiten, welches dann der Bundesnetzagentur mit einer Erklärung über den Fortschritt oder die Machbarkeit der Maßnahmen vorgelegt wird. Stellt die Bundesnetzagentur im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, kann sie deren unverzügliche Beseitigung verlangen (§ 109 Absatz 4 Satz 5 TKG). Legt der Betreiber entgegen der Vorschrift ein Sicherheitskonzept nicht oder nicht rechtzeitig vor, stellt dies gemäß § 149 Absatz 1 Nummer 21 TKG eine Ordnungswidrigkeit dar, die gemäß § 149 Absatz 2 Satz 1 TKG mit einer Geldbuße von bis zu 100 000 Euro geahndet werden kann. Aufgrund von § 17 Absatz 2 des Gesetzes über Ordnungswidrigkeiten (OWiG)[624] kann fahrlässiges Verhalten allerdings nur mit der Hälfte des Höchstsatzes geahndet werden, da § 149 Absatz 1 Nummer 21 TKG im Höchstsatz keine Unterscheidung zwischen Vorsatz und Fahrlässigkeit trifft. Sollte dieser Betrag jedoch den wirtschaftlichen Vorteil, den der Betreiber aus der Verletzung der Vorschrift hatte, nicht übersteigen, kann er auch überschritten werden (§ 149 Absatz 2 Satz 3 TKG).

Schutzmaßnahmen im telekommunikationsinfrastrukturellen Bereich lassen sich daher auf § 109 TKG stützen. Zur Durchsetzung der Maßnahmen kann die Bundesnetzagentur als

---

[620] Koenig/Loetz/Neumann, TKR, 2004, S. 209

[621] Schommertz, in: Scheuerle/Mayen, TKG, 2. Aufl. 2008, § 109 Rn. 6.

[622] Spindler, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010, S. 90

[623] Koenig/Loetz/Neumann, TKR, 2004, S. 209.

[624] Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I, S. 602), zuletzt geändert durch Artikel 2 des Gesetzes vom 29. Juli 2009 (BGBl. I, S. 2353).

zuständige Behörde im Sinne des § 116 TKG nach §§ 115, 126 TKG Anordnungen und andere Maßnahmen treffen.[625]

II.2.3.3.5 Sonstige Regelungen mit Steuerungswirkung für die IT-Sicherheit

Eine Anreizwirkung für Unternehmen zur Verbesserung der betrieblichen IT-Sicherheit geht von den Eigenkapitalvorschriften des Basler Ausschusses für Bankenaufsicht, kurz: Basel II, aus. Diese Regeln sind über die EU-Richtlinien 2006/48/EG[626] und 2006/49/EG[627] in ihrer Umsetzung für die EU-Mitgliedstaaten verbindlich geworden. Ziel der Regelungen ist zwar die Schaffung einheitlicher Wettbewerbsbedingungen bei der Kreditvergabe und die Sicherung einer angemessenen Ausstattung der Kreditinstitute mit Eigenkapital. Auswirkungen sind jedoch mittelbar auch in Unternehmen als Kreditnehmer zu verzeichnen. Kreditinstitute sind infolge von Basel II gehalten, bei der Risikoanalyse vor der Vergabe von Krediten nunmehr auch bestimmte „soft facts“ in die Kalkulation mit einzubeziehen, zu denen etwa auch die IT-Sicherheit des um Kredite ersuchenden Unternehmens gehört.

Auf diese Weise besitzt die IT-Sicherheit für Unternehmen eine handfeste finanzielle Bedeutung bei der Unternehmensgestaltung.

II.2.3.3.6 Rechtsdurchsetzung

II.2.3.3.6.1 Sicherung von Beweisen durch Strafverfolgungsbehörden

Die effektive Rechtsdurchsetzung bedarf der Täterfeststellung und für eine rechtskräftige Verurteilung der Sicherung von Beweisen.

Für die Täterfeststellung und Beweissicherung bei Taten im Internet sind drei Arten von Daten relevant: Bestandsdaten, Nutzungs- und Verkehrsdaten sowie Inhaltsdaten. Bestandsdaten[628] sind diejenigen personenbezogenen Daten, die für die Begründung des Vertragsverhältnisses zwischen Nutzer und Dienstanbieter notwendig sind. Diese umfassen in der Regel den Namen und die Adresse des Nutzers sowie die Anschlusskennung, also üblicherweise die Rufnummer. Sie sagen folglich nichts darüber aus, ob und in welchem

---

[625] Spindler, in: Kloepfer, Schutz kritischer Infrastrukturen, 2010, S. 91 m.w.N.

[626] Richtlinie 2006/48/EG des Europäischen Parlaments und des Rates vom 14. Juni 2006 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute (Neufassung), ABl. Nr. L 177 vom 30.6.2006, S. 1.

[627] Richtlinie 2006/49/EG des Europäischen Parlaments und des Rates vom 14. Juni 2006 über die angemessene Eigenkapitalausstattung von Wertpapierfirmen und Kreditinstituten (Neufassung), ABl. Nr. L 177 vom 30.6.2006, S. 201.

[628] Der Begriff wird durch § 3 Nr. 3 TKG legal definiert.

Umfang eine Nutzung tatsächlich stattgefunden hat. Nutzungs-[629] und Verkehrsdaten[630] geben Auskunft über die Nummer oder Kennung der beteiligten Anschlüsse, Beginn und Ende der Nutzung, als auch die Datenmenge, also den Umfang der Nutzung von Telekommunikationsdiensten. Inhaltsdaten sind die mittels Kommunikation ausgetauschten Informationen, oder auch Inhalte von lokal gespeicherten Dateien.[631]

II.2.3.3.6.2 Erteilung von Bestandsdatenauskünften

Anbieter von Telemediendiensten dürfen nach § 14 Absatz 2 TMG[632] auf Anordnung zuständiger Stellen und bei Vorliegen weiterer Merkmale[633] Auskünfte über Bestandsdaten erteilen. Die Norm selbst befugt den Dienstanbieter in datenschutzrechtlicher Hinsicht, sie ermächtigt jedoch nicht die anfragende Stelle, die Daten tatsächlich abzufragen. Die Behörde kann durch § 94 StPO[634] ermächtigt sein, eine Sicherstellung und Beschlagnahme vorzunehmen.

Weitaus häufiger werden Bestandsdaten bei Telekommunikationsdienstleistern abgefragt.[635] Der Diensteanbieter wird datenschutzrechtlich durch § 113 TKG[636] grundsätzlich verpflichtet, Daten an Behörden zu übermitteln.

Das Bundesverfassungsgericht sieht, wenn die Auskunftserteilung unter mittelbarer Nutzung von gespeicherten Verkehrsdaten, wie etwa dynamischer IP-Adressen, erfolgt, einen Eingriff in Artikel 10 Absatz 1 GG als gegeben an, da eine Auskunft über einen Nutzer einer IP-Adresse auch immer eine Aussage darüber enthalte, dass ein Telekommunikationsvorgang stattgefunden habe.[637] Einen Richtervorbehalt hat es jedoch für eine solche Auskunft nach

---

[629] § 15 Abs. 1 S. 1 TMG.

[630] § 3 Nr. 30 TKG.

[631] Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, S. 269 a.E.

[632] Telemediengesetz vom 26. Februar 2007 (BGBl. I, S. 179), zuletzt geändert durch das Gesetz vom 31. Mai 2010 (BGBl. I, S. 692).

[633] Die Auskunft muss für Zwecke der Strafverfolgung, zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich sein.

[634] Strafprozessordnung in der Fassung vom 7. April 1987 (BGBl. I, S. 1074, 1319), zuletzt geändert durch Gesetz vom 23. Juni 2011 (BGBl. I, S. 1266).

[635] 2010 führten 6,0 Mio. Ersuchen von Sicherheitsbehörden zu 36,0 Mio. Abfragen bei Telekommunikationsdienstanbietern, siehe Bundesnetzagentur, Jahresbericht 2010, S. 125, abrufbar unter: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/Jahresbericht2010pdf.pdf?__blob=publicationFile.

[636] Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I, S. 1190), zuletzt geändert durch Gesetz vom 24. März 2011 (BGBl. I, S. 506).

[637] BVerfGE 125, 260, 342, Tz. 259 – Vorratsdatenspeicherung.

Bestandsdaten als nicht zwingend angesehen und sich damit an seiner bisherigen Rechtsprechung orientiert. Gleichwohl sieht das Bundesverfassungsgericht das Transparenzgebot aber nur dann als nicht verletzt an, wenn ein Betroffener grundsätzlich über den Vorgang einer mittelbaren Datenauskunft benachrichtigt wird.[638]

Ergänzungstext des SV Alvar Freude

Derzeit wird dieser Benachrichtigungspflicht in der Regel nicht nachgekommen.

Nach Ansicht des Bundesverfassungsgerichts beinhalte die Strafprozessordnung keinen „numerus clausus“ für Eingriffe in Artikel 10 Absatz 1 GG. Derartige Eingriffe müssten daher nicht ausschließlich auf §§ 100g, 100a StPO gestützt werden.[639] Begründet wurde dies damit, dass zwar in Artikel 10 Absatz 1 GG eingegriffen werde, der Staat aber selbst keinen Zugriff auf die verwendeten Verkehrsdaten erhalte, sondern sich der TK-Anbieter dezentraler Speicherstellen bedient, was den Eingriff abmildere.[640] Das Bundesverfassungsgericht versteht § 113 TKG demnach so, dass dieser „auf die jeweiligen fachgesetzlichen Eingriffsgrundlagen verweist und für den Zugriff auf die Daten zumindest einen hinreichenden Anfangsverdacht gemäß §§ 161, 163 StPO oder eine konkrete Gefahr im Sinne der polizeilichen Generalklauseln voraussetzt“.[641]

II.2.3.3.6.3 Beauskunftung von Nutzungs- und Verkehrsdaten

Nutzungs- und Verkehrsdaten können bei Telekommunikationsdienstleistern nach § 100g StPO beauskunftet werden. Telekommunikationsdienstleister dürfen diese gemäß der §§ 97ff. TKG sowohl zu Abrechnungszwecken als auch für die Aufklärung und Verhinderung von Störungen und Missbräuchen speichern.

Die Telekommunikationsdienstleister unterliegen dabei jedoch strengen datenschutzrechtlichen Anforderungen.[642]

Unabhängig davon sind nach der Richtlinie der EU über die Vorratsspeicherung von Daten[643], die Anbieter von Telekommunikationsdiensten dazu verpflichtet, Verkehrsdaten mindestens

---

[638] BVerfGE 125, 260, 344, Tz. 263 – Vorratsdatenspeicherung, wonach aber Ausnahmen gelten, wenn durch die Benachrichtigung der Zweck der Datenauskunft vereitelt wird oder Interessen Dritter oder des Betroffenen entgegenstehen.

[639] Eckhardt/Schütze, Vorratsdatenspeicherung nach dem BVerfG: „Nach dem Gesetz ist vor dem Gesetz...“, CR 2010, 225, 228.

[640] BVerfG, Urt. v. 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Tz. 256; dazu Eckhardt/Schütze, Vorratsdatenspeicherung nach dem BVerfG: „Nach dem Gesetz ist vor dem Gesetz...“, CR 2010, 225, 228.

[641] BVerfG, Urt. v. 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Tz. 289.

[642] Vgl. BGH Urteil v. 13.01.2011 – Az. III ZR 146/10

sechs Monate zu speichern.[644] Die Richtlinie wurde in Deutschland bisher nicht verfassungskonform umgesetzt, da das Bundesverfassungsgericht die entsprechenden Umsetzungsnormen (§§ 113a, 113b TKG und § 100g Absatz 1 Satz 1 StPO) mit Urteil vom 2. März 2010 für nichtig erklärt hat.[645] Bisher gesammelte Vorratsdaten waren daher umgehend von den Telekommunikationsunternehmen im Anschluss an die Entscheidung zu löschen.

In seiner Entscheidung hat das Bundesverfassungsgericht ausgeführt, dass es für eine verfassungskonforme Umsetzung „hinreichend anspruchsvoller und normenklarer Regelungen“[646] bezüglich der Datensicherheit, des Umfangs der Datenverwendung, der Transparenz und des Rechtsschutzes bedürfe. Bei den vorgesehenen pauschalen Speicherfristen handle es sich um einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“[647].

Eine verfassungs- und europarechtskonforme Umsetzung der EU-Richtlinie in nationales Recht ist bisher noch nicht erfolgt. Die EU-Kommission hat daher gegen Deutschland am 31. Mai 2012 beim Europäischen Gerichtshof Klage wegen Nichtumsetzung der Richtlinie eingereicht. Bei Erfolg der Klage der EU-Kommission wäre hiermit auch die Zahlung eines Zwangsgeldes ab dem Tag des Urteils verbunden.[648]

Parallel hierzu hatte die EU-Kommission bereits im April 2011 nach der Evaluation[649] angekündigt, einen Vorschlag für eine überarbeitete Richtlinie zur Speicherung von Vorratsdaten vorzulegen. Dieser ist jedoch derzeit nicht absehbar. Außerdem wird der Europäische Gerichtshof aufgrund eines vom Irischen High Court angestrengten Vorabentscheidungsverfahrens[650] u. a. zu prüfen haben, ob die EU-Richtlinie zur Vorratsdatenspeicherung mit der Europäischen Grundrechtecharta vereinbar ist.

---

[643] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. Nr. L 105 vom 13.4.2006, S. 54.

[644] Art. 6 der Richtlinie 2006/24/EG.

[645] BVerfG, Urt. v. 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

[646] BVerfG, Urt. vom 02.03.2010 - 1 BvR 256/08, Tz. 220.

[647] BVerfG, Urt. vom 02.03.2010 - 1 BvR 256/08, Tz. 210.

[648] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/530&format=HTML&aged=0&language=DE&guiLanguage=en

[649] http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf

[650] Vorabentscheidungsersuchen des High Court of Ireland (Irland), eingereicht am 11. Juni 2012 – Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Irland und The Attorney General, Rs. C-293/12, abrufbar unter:

II.2.3.3.6.4 Ermittlung von Inhaltsdaten

Zur Ermittlung von Inhaltsdaten sind – vom Standpunkt der (auch technischen) Machbarkeit betrachtet – mehrere Methoden denkbar.

II.2.3.3.6.4.1 Beschlagnahme von Datenträgern

Datenträger – inklusive der darauf gespeicherten Daten – können nach §§ 94ff. StPO sichergestellt und beschlagnahmt werden. Die Befugnis zur Auswertung der aufgefundenen Daten richtet sich nach der Art der Daten, also etwa danach, ob die Daten höchstpersönlichen Inhalt haben oder nicht.

II.2.3.3.6.4.2 Öffentlich zugängliche Daten (virtuelle Streife)

Unabhängig von der Beschlagnahme von Hardware können durch die Polizei Recherchen auf Grundlage des § 163 StPO[651] durchgeführt werden soweit Daten öffentlich zugänglich sind. Öffentlich zugänglich sind diejenigen Daten, die jedem Internetnutzer ohne Zugangssperre oder Passwort zugänglich sind. Da in diesem Fall ein Grundrechtseingriff nicht vorliegt, bedarf es keiner speziellen Befugnisnorm.

Ergänzungstext der Fraktionen der SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN

Mit der Ausdifferenzierung der Kommunikations- und Veröffentlichungsformen in den neuen sozialen Netzwerken verschwimmt die Grenze zwischen öffentlich und nicht-öffentlich zugänglichen Informationen. Etwa die Erlangung auch für größere – aber prinzipiell geschlossene – Freundesgruppen vorbehaltene Informationen könnte als spezielle Form der „verdeckten Ermittlung“ beziehungsweise einer „Überwachung“ im Sinne des TKG gewertet werden.

---

http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d58137302027de4437af509098f919f0de.e34KaxiLc3eQc40LaxqMbN4Oa3qLe0?text=&docid=125859&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=3547468.

[651] § 163 Abs. 1 StPO lautet: „Die Behörden und Beamten des Polizeidienstes haben Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten. Zu diesem Zweck sind sie befugt, alle Behörden um Auskunft zu ersuchen, bei Gefahr im Verzug auch, die Auskunft zu verlangen, sowie Ermittlungen jeder Art vorzunehmen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln.“.

II.2.3.3.6.4.3 Zugriff beim Telekommunikationsdienstleister

Ein Zugriff auf Inhaltsdaten kann auf Grundlage und in den Grenzen von §§ 100a, 100b StPO sowie der Telekommunikations-Überwachungsverordnung[652] erfolgen. Umstritten ist die rechtliche Ausgestaltung der Überwachung von E-Mail-Verkehr und des Auslesens von E-Mail-Korrespondenz.

Der Bundesgerichtshof entschied am 31. März 2009, dass E-Mails beim Telekommunikationsdienstleister nach den Regelungen über die Postbeschlagnahme nach § 99 StPO beschlagnahmt werden können, da kein Telekommunikationsvorgang während der Speicherung der Nachricht beim Telekommunikationsdienstleister gegeben sei.[653] Die Anwendbarkeit einer Postbeschlagnahme sieht der Bundesgerichtshof darin begründet, dass eine E-Mail mit dem herkömmlichen Telegramm vergleichbar sei.[654] Das Bundesverfassungsgericht hat hier für Klarheit gesorgt, indem es am 16. Juni 2009 urteilte, dass E-Mails, die beim Telekommunikationsdienstleister gespeichert sind, zwar dem Fernmeldegeheimnis unterliegen, gleichwohl aber nach § 94 StPO beschlagnahmt werden können.[655] Nach Ansicht des Gerichts ist § 94 StPO taugliche Ermächtigungsgrundlage für Eingriffe in Artikel 10 Absatz 1 GG.[656] Es sei ferner nicht erkennbar, dass der Gesetzgeber einen Eingriff in das Fernmeldegeheimnis nur nach den Vorschriften der §§ 100a und 100g StPO zulassen wollte.[657]

Kritiker dieses Urteils gehen davon aus, dass E-Mails beim Telekommunikationsdienstleister dem Fernmeldegeheimnis unterliegen, so dass auf sie nur nach den strengeren Vorschriften der §§ 100a, 100b StPO zugegriffen werden kann[658], da diese Normen speziell und abschließend seien.

Mit der Übertragung der E-Mail auf den Rechner des Nutzers endet der Schutz des Fernmeldegeheimnisses aus Artikel 10 Absatz 1 GG,[659] da die Kommunikation nicht mehr der

---

[652] Telekommunikations-Überwachungsverordnung vom 3. November 2005 (BGBl. I, S. 3136), zuletzt geändert durch Gesetz vom 25. Dezember 2008 (BGBl. I, S. 3083); erlassen auf Grund des § 110 Abs. 2, 6 S. 2 und Abs. 8 S. 2 des Telekommunikationsgesetzes vom 22.06.2004.

[653] BGH, Beschl. v. 31.03.2009 – 1 StR 76/09 = NJW 2009, 1828.

[654] BGH, Beschl. v. 31.03.2009 – 1 StR 76/09 = NJW 2009, 1828.

[655] BVerfG, Urt. v. 16.06.2009 – 2 BvR 902/06 = NJW 2009, 2431, 2433.

[656] BVerfG, Urt. v. 16.06.2009 – 2 BvR 902/06 = NJW 2009, 2431, 2433.

[657] BVerfG, Urt. v. 16.06.2009 – 2 BvR 902/06 = NJW 2009, 2431, 2433.

[658] Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, S. 327; Rössel, Beschlagnahme von E-Mails beim Mailbox-Provider, ITRB 2004, S. 10-11; Störing, Strafprozessualer Zugriff auf E-Mailboxen, CR 2009, S. 475, 479.

[659] BVerfG, Urt. v. 02.03.2006 – 2 BvR 2099/04 = NJW 2006, 976, 978, Tz. 72.

spezifischen Gefahr ausgesetzt ist, die bei einer Übermittlung durch Dritte besteht.[660] Ab diesem Zeitpunkt untersteht die E-Mail nur mehr dem Schutz durch das Recht auf informationelle Selbstbestimmung,[661] sie kann daher dann gemäß § 94 StPO beschlagnahmt werden.

II.2.3.3.6.4.4 Online-Durchsuchung

Mit Hilfe der Online-Durchsuchung soll es ermöglicht werden, die auf dem Computer einer überwachten Person gespeicherten Dateien (zum Beispiel Dokumente, E-Mail-Korrespondenz, Bilder etc.) einzusehen, ohne dass die überwachte Person hiervon Kenntnis erlangt.[662] Die Online-Durchsuchung kann aufgrund von § 20k des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Artikel 1 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, Bundeskriminalamtgesetz – BKAG)[663] durchgeführt werden.

Nach einer Initiative des Landes Nordrhein-Westfalen, das mit § 5 Absatz 2 Nummer 11 Alternative 2 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen[664] eine Ermächtigung zur Online-Durchsuchung zur Gefahrenabwehr schaffen wollte, nahm das Bundesverfassungsgericht in 2008 ausführlich zur präventiven Online-Durchsuchung Stellung.[665] Eine präventive Online-Durchsuchung sei aufgrund des schwerwiegenden Eingriffs in das – mit dem Urteil richterrechtlich neu geschaffene – „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ nur in sehr engen Grenzen möglich. Sie müsse hinreichend klar gesetzlich geregelt sein,[666] es müsse eine konkrete Gefahr für ein überragend wichtiges Rechtsgut vorliegen[667] und sie bedürfe stets der Anordnung durch einen Richter.[668] Überragend wichtig sind Leib, Leben und Freiheit

---

[660] BVerfG, Urt. v. 02.03.2006 – 2 BvR 2099/04 = NJW 2006, 976, 978, Tz. 73.

[661] BVerfG, Urt. v. 02.03.2006 – 2 BvR 2099/04 = NJW 2006, 976, 978, Tz. 72.

[662] Braun, Ozapftis – (Un)Zulässigkeit von „Staatstrojanern“, K&R 2011, 681.

[663] Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz) vom 7. Juli 1997 (BGBl. I, S. 1650), zuletzt geändert durch Art. 2 des Gesetzes vom 6. Juni 2009 (BGBl. I, S. 1226).

[664] Verfassungsschutzgesetz Nordrhein-Westfalen, hier in der durch das Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20.12.2006 (NWGVBl, S. 620) geänderten Fassung.

[665] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07 = NJW 2008, 822 .

[666] BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, Tz. 207-228.

[667] BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, Tz. 247.

[668] BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, Tz. 257.

der Person sowie solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, also auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen. Eine Regelung, die diese Erfordernisse erfüllt, ist auf Bundesebene durch § 20k BKAG[669] für das Bundeskriminalamt gegeben. § 20k Absatz 7 BKAG bestimmt zudem zum Schutz des Betroffenen, dass die Maßnahme unzulässig ist, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Werden dennoch Daten aus diesem Kernbereich erlangt, dürfen diese nicht verwertet werden und sind unverzüglich zu löschen. Eine repressive Online-Durchsuchung, das heißt eine Durchsuchung, die der Aufklärung einer Straftat dient, ist nach Auffassung des 3. Strafsenates des Bundesgerichtshofs derzeit nicht mit geltendem Recht vereinbar.[670]

II.2.3.3.6.4.5 Quellen-Telekommunikationsüberwachung

Mit der Online-Durchsuchung verbunden, aber in ihrem funktionalen Umfang dieser gegenüber beschränkt, ist die so genannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ).[671] Ziel der Quellen-TKÜ ist die Überwachung von Telekommunikation (zum Beispiel von Skype- oder verschlüsselten VoIP-Telefonaten) direkt an der Quelle, also ehe diese vor der Übertragung verschlüsselt werden kann, beziehungsweise nachdem sie auf dem Zielgerät des Kommunikationsvorgangs wieder entschlüsselt wurde. Das Bundesverfassungsgericht hat in seiner Entscheidung zur Online-Durchsuchung[672] im Rahmen eines so genannten *obiter dictums*, also in die Entscheidung nicht tragenden Ausführungen, zur Quellen-TKÜ festgehalten, dass „mit der Infiltration die entscheidende Hürde genommen ist, um das System insgesamt auszuspähen“.[673] Eine Quellen-TKÜ könne demnach nur ein durch §§ 100a, 100b StPO, dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz) oder landesrechtlichen Vorschriften erlaubter Eingriff in Artikel 10 Absatz 1 GG sein, wenn sich die Überwachung ausschließlich auf Daten

---

[669] Gegen § 20k BKAG sind seit 2009 zwei Verfassungsbeschwerden beim BVerfG anhängig (Az. 1 BvR 966/09, 1 BvR 1140/09), für die eine Entscheidung über die Annahme noch im Jahr 2012 angestrebt wird, s. http://www.bundesverfassungsgericht.de/organisation/erledigungen_2012.html .

[670] BGH, Beschl. vom 31.01.2007 – StB 18/06.

[671] Braun, Ozapftis – (Un)Zulässigkeit von „Staatstrojanern“, K&R 2011, 681.

[672] BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07

[673] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, Tz. 190 = NJW 2008, 822, 826.

aus einem laufenden Telekommunikationsvorgang beschränke,[674] und nicht etwa auch gespeicherte Daten oder die sonstige Kommunikation am Standort des Computers überwacht werde. Diese Beschränkung müsse durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein.[675]

Die Quellen-TKÜ wird von der Rechtsprechung der Amts- und Landgerichte sowie teilweise auch nach Auffassung in der Literatur auf § 100a StPO gestützt, der für diese besondere Form der Telekommunikationsüberwachung eine „Annexkompetenz“ enthalte.[676] Es wird jedoch auch die Meinung vertreten,[677] dass die §§ 100a, 100b StPO als Rechtsgrundlagen nicht ausreichend seien. Begründet wird diese Auffassung damit, dass die geltende Regelung des § 100a StPO eine mögliche Beeinträchtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht ausreichend berücksichtige.

Zudem ist bislang noch nicht abschließend geklärt, in welcher Art und Weise eine technische Abgrenzung von Software-Funktionalitäten zwischen Quellen-TKÜ und Online-Durchsuchung dauerhaft sichergestellt werden kann.

II.2.3.3.6.4.6 Einsatz von Ermittlungs-Software (so genannter Staatstrojaner)

Sowohl bei der Online-Überwachung als auch der Quellen-TKÜ sind sowohl die gesetzlichen Grundlagen als auch die Vorgaben des Bundesverfassungsgerichts einzuhalten.

Das bedeutet insbesondere, dass die für die Maßnahmen verwendete Software in technischer Hinsicht nicht mehr zulassen darf, als rechtlich zulässig ist. Dies folgt den Ausführungen des Bundesverfassungsgerichts, nach denen ein möglichst weitgehender Schutz der Integrität des Zielsystems und die Beschränkung auf die laufende Kommunikation sichergestellt werden soll. Darüber hinaus sollen technische Vorkehrungen gegen Missbrauch getroffen werden.

Aufgrund eines Ermittlungsverfahrens bei der Staatsanwaltschaft Landshut[678] wurde vom Bayerischen Landesbeauftragten für den Datenschutz, Dr. Thomas Petri, als auch dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, geprüft,

---

[674] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, Tz. 190 = NJW 2008, 822, 826.

[675] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, Tz. 190 = NJW 2008, 822, 826.

[676] (LG Hamburg vom 31.08.2010, Aktenzeichen 608 Qs 17/10; KMR/Bär § 100 a StPO Rn 31b f.; Meyer-Goßner 53. Aufl., § 100 a StPO Rn 7 i KK-StPO/Nack, 6. Aufl., § 100 a Rn 27; Beck OK-StPO/Graf Rn 114 ff; AG Bayreuth MMR 2010, 266).

[677] Felix Hermonies Recht u Politik 2011, 193; Andreas Popp Zeitschrift für Datenschutz 2012, 51; Thomas Stadler MMR 2012, 18; Dominik Brodowski Juristische Rundschau 2011, 533

[678] Braun, Ozapftis – (Un)Zulässigkeit von „Staatstrojanern“, K&R 2011, 681 (683); Dominik Brodowski Juristische Rundschau 2011, 533

ob die bisher in der Praxis verwendete Software der bayerischen Ermittlungsbehörden und des Bundeskriminalamtes diesen rechtlichen und technischen Anforderungen genügt.

Der Bayerische Landesbeauftragte für den Datenschutz kommt in seinem Bericht[679] zu dem Ergebnis, dass keine Anhaltspunkte festgestellt werden konnten, dass bei den Maßnahmen der Staatsanwaltschaften tatsächliche rechtswidrige Zugriffe auf Mikrofone beziehungsweise Kameras erfolgten oder Keylogger zum Einsatz kamen.[680]

Hinsichtlich der technischen Durchführung der Überwachungsmaßnahmen hat der Bayerische Landesdatenschutzbeauftragte allerdings auf Möglichkeiten des Missbrauchs der eingesetzten Software hingewiesen. Diese könnten sich beispielsweise durch die in der Software verankerte Nachladefunktion ergeben. Zudem sei eine Überprüfung der einzelnen Funktionalitäten aufgrund der Schwierigkeiten bei der Einsichtnahme in den Quellcode der Software nicht möglich. Auch sei die Quellen-Telekommunikationsüberwachung von der Online-Durchsuchung durch klare Vorgaben abzugrenzen.
Soweit an der Quellen-TKÜ festgehalten werde, empfiehlt er daher „dringend, Bestimmungen zu schaffen, die der erhöhten Eingriffsintensität und den technischen Besonderheiten der Quellen-TKÜ gerecht werden.“[681]

Alternativtext der Fraktion der SPD und SV Alvar Freude

Mit der Online-Durchsuchung verbunden, aber in ihrem funktionalen Umfang dieser gegenüber beschränkt, ist die sogenannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ).[682] Ziel der Quellen-TKÜ ist die Überwachung von Telekommunikation (beispielsweise von Skype- oder anderen verschlüsselten VoIP-Telefonaten) direkt an der Quelle, also ehe diese vor der Übertragung verschlüsselt werden kann beziehungsweise nachdem sie auf dem Zielgerät des Kommunikationsvorgangs wieder entschlüsselt wurde.
Das Bundesverfassungsgericht hat in seiner Entscheidung zur Online-Durchsuchung[683] zur Quellen-TKÜ festgehalten, dass „mit der Infiltration die entscheidende Hürde genommen ist, um das System insgesamt auszuspähen“.[684]
Ob eine Quellen-TKÜ auf der Grundlage der bestehenden §§ 100a, 100b StPO ein erlaubter

[679] http://www.datenschutz-bayern.de/0/bericht-qtkue.pdf

[680] http://www.stmi.bayern.de/presse/archiv/2012/274.php

[681] http://www.datenschutz-bayern.de/presse/20120802_Quellen-TKUE.html

[682] Braun, Ozapftis – (Un)Zulässigkeit von „Staatstrojanern“, K&R 2011, 681.

[683] BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07.

[684] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, Tz. 190 = NJW 2008, 822, 826.

Eingriff sein kann, ließ das Gericht offen.- Es betonte aber drei Anforderungen, die eine solche Überwachungssoftware erfüllen muss: „Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer 'Quellen-Telekommunikationsüberwachung', wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein.“[685] Entsprechend sind die Bedingungen zur Durchführung mindestens den Anforderungen unterworfen, dass ausschließlich Telekommunikationsvorgänge abgehört werden dürfen und dass dies sowohl rechtlich wie auch technisch sicherzustellen ist.

Beim bisherigen Einsatz der Software sind diese Anforderungen nicht erfüllt worden. Sofern keine neue Rechtsgrundlage für den Eingriff geschaffen wird, ist der §§ 100a, 100b StPO nach diesen Vorgaben weiterhin nicht hinreichend. Das ist dadurch begründet, dass die geltende Regelung des § 100a StPO eine mögliche Beeinträchtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht ausreichend berücksichtigt. Zudem enthält diese Vorschrift keine Schutzvorkehrungen, um rechtlich und technisch sicherzustellen, dass die Überwachung nur die laufende Telekommunikation erfassen würde. Dazu müssten Bestimmungen in § 100a StPO Eingang finden, die der erhöhten Eingriffsintensität und den technischen Besonderheiten der Quellen-TKÜ gerecht werden.

In der juristischen Fachliteratur vertritt die Mehrheit die Ansicht, dass die bisherige Rechtslage nicht ausreichend ist, um eine Quellen-TKÜ durchzuführen. So ziehen die Juristen Ulf Buermeyer und Matthias Bäcker den Schluss: „§100a StPO ist keine taugliche Grundlage für eine Quellen-TKÜ, sofern dazu Software auf dem betroffenen Endgerät installiert werden soll. So begreiflich der Wunsch der Sicherheitsbehörden sein mag, VoIP-Gespräche ebenso abhören zu können wie Festnetz- und Mobilfunktelefonate – im Rechtsstaat des Grundgesetzes trifft allein der Gesetzgeber die Entscheidung, in welche Grundrechte unter welchen Voraussetzungen eingegriffen werden darf. Sofern der politische Wille besteht, auch die Überwachung der Telefonie über das Internet zu repressiven Zwecken zuzulassen, müsste

[685] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, Tz. 190 = NJW 2008, 822, 826.

also der Bund eine spezifische Ermächtigungsgrundlage schaffen, die insbesondere den Vorgaben der OD-Entscheidung des BVerfG Rechnung zu tragen hätte.“[686]

Armin Nack, Vorsitzender des 1. Strafsenats des Bundesgerichtshofs, vertritt im Karlsruher Kommentar zur Strafprozessordnung seit 2008 eine vermittelnde Ansicht, indem er solche Maßnahmen auf der Grundlage der geltenden Strafprozessordnung nur „für eine Übergangszeit“ zulassen will. Dass der Bundesgesetzgeber zwischenzeitlich hätte handeln können, ist allerdings kaum zu bestreiten und nicht zuletzt durch die Novelle des BKA-Gesetzes belegt, die ja als Reaktion auf die Entscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung beschlossen wurde und eine Rechtsgrundlage für eine Quellen-TKÜ enthält (§ 20 l BKAG). Der innenpolitische Sprecher der CDU/CSU-Fraktion im Deutschen Bundestag, Hans-Peter Uhl, forderte daher in seiner Pressemitteilung vom 10. Oktober 2011, vergleichbare explizite Rechtsgrundlagen zu schaffen, wo es sie noch nicht gibt.[687] Auch Wolfgang Bär, Richter am Oberlandesgericht und lange Zeit ein Befürworter der Quellen-TKÜ schon nach geltender Strafprozessordnung, ist hiervon unter dem Eindruck des Landshuter Trojaner-Skandals abgerückt und vertritt nunmehr, dass es zumindest einer Klarstellung in der Strafprozessordnung bedürfe.[688]

Demgegenüber gibt es einige (ältere) Stimmen aus der untergerichtlichen Rechtsprechung, die eine Quellen-TKÜ für zulässig erklären.[689] Dieser folgend vertritt dies derzeit auch der Praktiker-Kommentar zur Strafprozessordnung von Meyer-Goßner (in der Bearbeitung von Schmitt, § 100a StPO Rn. 7a)[690] sowie Löffelmann im Anwaltskommentar zur Strafprozessordnung, § 100a StPO Rn. 18.[691] Das Amtsgericht Berlin-Tiergarten hat eine Quellen-TKÜ-Maßnahme in einer bisher unveröffentlichten Entscheidung hingegen

[686] Buermeyer, Ulf/Bäcker, Matthias: „Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO. In: HRR-Strafrecht 10 (2009), S. 433-441, hier S. 440-441. Diese Auffassung teilt die nahezu einhellige Meinung inder wissenschaftlichen Literatur, vgl. etwa Albrecht, JurPC Web-Dok. 59/2011; Albrecht/Dienst JurPC 5/2012; Becker/Meinicke StV 2011, 50; Böckenförde JZ 2008, 925, 934; Braun K&R 2011, 681; Heckmann (in seiner Stellungnahme in der internen Anhörung des BMJ im Januar 2012); Hoffmann-Riem JZ 2008, 1009, 1014; Hornung CR 2008, 299, 300; Vogel/Brodowski StV 2009, 632 und Wolter SK-StPO § 100a Rn. 30.

[687] Vgl. dazu Pressemitteilung der CDU/CSU-Fraktion vom 10. Oktober 2011, abrufbar unter folgendem Link: http://www.cducsu.de/Titel__pressemittei-lung_erforderliche_rechtsgrundlagen_fuer_alle_sicherheitsbehoerden_schaf-fen/TabID__6/SubTabID__7/InhaltTypID__1/InhaltID__19908/Inhalte.aspx

[688] Bär, Wolfgang: MMR 2011, 691.

[689] LG Hamburg, Beschluss vom 13. September 2010 - 608 Qs 17/10 - MMR 2011, 693; AG Bayreuth, Beschluss vom 17. September 2009 - Gs 911/09 - MMR 2010, 266; LG Landshut, Beschluss 4 Qs 346/10.

[690] Meyer-Goßner, Strafprozessordnung: Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, Kommentar (QUELLENANGABE WIRD NOCH VERVOLLSTÄNDIGT).

[691] Krekeler/Löffelmann/Sommer, AnwaltKommentar StPO (QUELLENANGABE WIRD NOCH VERVOLLSTÄNDIGT)

abgelehnt.

Soweit Funktionen über das Abhören von Telekommunikationsvorgängen hinausgingen, also unter der Bezeichnung „Quellen-TKÜ“ letztlich eine Online-Durchsuchung durchgeführt wurde, liegt bereits eine Entscheidung eines Instanzgerichtes vor. Der Einsatz des Quellen-TKÜ-Trojaners des Bayerischen Landeskriminalamtes, der den Computer eines Verdächtigen über mehrere Monate hinweg auch mit Hilfe einer Screenshot-Funktion überwachte, die alle dreißig Sekunden ein Bildschirmfoto des Skype-Fensters- und des Browser-Inhalts erstellte und diese Bilder über das Internet übertrug, wurde vom Landgericht Landshut mit rechtskräftigem Beschluss vom 20. Januar 2011 als rechtswidrig festgestellt, während das Gericht das Ausleiten von Telefonaten als rechtmäßig betrachtete. [692]

Der praktische Einsatz der Quellen-TKÜ ist von erheblichen rechtlichen und technischen Problemen gekennzeichnet. Durch die Veröffentlichungen des Chaos Computer Clubs (CCC) wurde zum einen die Tatsache publik, dass die von privaten Dienstleistern gekaufte Trojaner-Software für die Quellen-TKÜ in Bundes- und Landesbehörden eklatante handwerkliche Mängel aufweist, den Vorgaben aus Karlsruhe nicht entspricht und die Behörden mangels Einsicht in den Quelltext die tatsächliche Funktionalität der Software nicht überprüfen konnten.[693] Die Schnittstelle der Fernsteuerung des Torjaners konnte aufgrund von technischen Unzulänglichkeiten von Dritten genutzt werden, die Kommandos an den Trojaner waren weder verschlüsselt noch authentifiziert. Der Bundesdatenschutzbeauftragte Peter Schaar bestätigte teilweise die Analyse in seinem nach der Veröffentlichung des CCC erarbeiteten Berichts zur Quellen-TKÜ vom 31. Januar 2012. Gleichzeitig konnte er seinem Prüfauftrag jedoch nur begrenzt nachkommen, da auch ihm bis heute eine Offenlegung des Quellcodes der verwendeten Software unter Verweis auf Betriebs- und Geschäftsgeheimnisse des Herstellers verweigert wurde. An der gegenseitigen Authentifizierung zwischen dem Quellen-TKÜ-Trojaner arbeitet die Firma Digitask, welche die Behörden beliefert, erst seit der Veröffentlichung des CCC.[694] Fest steht jedoch, dass über mehrere Jahre eine Software für die Quellen-TKÜ eingesetzt wurde, die den Anforderungen des Bundesverfassungsgerichts nicht genügt.

---

[692] Vgl. hierzu Beschluss Az. 4 Qs 346/10 LG Landshut, S. 7.

[693] Vgl. https://www.ccc.de/de/updates/2011/staatstrojaner.

[694] Stellungnahme von Digitask vom 11. Oktober 2011. (QUELLENANGABE WIRD NOCH VERVOLLSTÄNDIGT)

II.2.3.3.6.5 Ausbildung und Training des Strafverfolgungspersonals

Die technische Entwicklung bringt nicht nur auf Täterseite neue Möglichkeiten zur Deliktsbegehung mit sich, sondern eröffnet ebenso den Strafverfolgungsbehörden im Rahmen ihrer Ermittlungstätigkeiten neue Chancen. Zur effektiven Verbrechensbekämpfung sowie zur Fehler- und Missbrauchsvorbeugung ist jedoch erforderlich, dass den Behörden nicht nur die entsprechenden Mittel zur Verfügung gestellt werden, sondern ebenso, dass die Ermittler hinreichend aus- und fortgebildet werden.[695]

II.2.3.3.6.6 Technische und personelle Ausstattung der Strafverfolgungsbehörden[696]

II.2.3.3.6.6.1 Computer-Forensik

Computer-Forensik bezeichnet Methoden zur Gewinnung von Erkenntnissen über beobachtete oder festgestellte Unregelmäßigkeiten oder Vorgänge,[697] die gerichtsverwertbare,[698] digitale Beweise erbringen.[699] Dabei ist ein standardisiertes Vorgehen erforderlich, das ein zu untersuchendes System möglichst unangetastet lässt, um flüchtige Speicherinhalte nicht zu verlieren oder zu verändern.[700] So kann zum Beispiel der Systemstart eines Windows-Systems die Datumsstempel einer Vielzahl von Dateien verändern.[701] Daher darf, um das Beweismaterial intakt zu erhalten, eine forensische Analyse nur an einer Systemkopie durchgeführt werden.[702] Eine bemerkenswerte Sammlung zum standardisierten Vorgehen auf dem Gebiet der Computer-Forensik ist im Leitfaden „IT-Forensik“[703] des BSI im März 2011 herausgegeben worden. Dieser Leitfaden soll auch als Hilfe für die Arbeit von

---

[695] Gercke, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 1.

[696] Gercke, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 1.

[697] Fox/Kelm, Computer-Forensik, DuD 2004, 491.

[698] Willer/Hoppen, Computerforensik – Technische Möglichkeiten und Grenzen, CR 2007, 610.

[699] Brunst, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 987.

[700] Fox/Kelm, Computer-Forensik, DuD 2004, 491; BSI, Leitfaden „IT-Forensik“, Version 1.0.1 (März 2011), S. 24, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile

[701] Willer/Hoppen, Computerforensik – Technische Möglichkeiten und Grenzen, CR 2007, 610.

[702] BSI, Leitfaden „IT-Forensik“, Version 1.0.1 (März 2011), S. 26, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile; Willer/Hoppen, Computerforensik – Technische Möglichkeiten und Grenzen, CR 2007, 610, 612.

[703] BSI, Leitfaden „IT-Forensik“, Version 1.0.1 (März 2011), abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile

Strafverfolgungsbehörden dienen[704] und bildet den aktuellen Stand der Computer-Forensik ab.

Zusätzlich sind spezielle Programme erforderlich, die ein System zu analysieren helfen.[705] Den Strafverfolgungsbehörden stehen dabei inzwischen umfangreiche digitale Werkzeugsammlungen, so genannte Toolkits, zur Verfügung. Ein bei Strafverfolgungsbehörden verbreitetes[706] Toolkit ist *EnCase* der Firma Guidance Software. Dieses und ähnliche Toolkits können Systemabbilder vielfältig untersuchen und so zum Beispiel bekannte kinderpornographische Bilder aus großen Datenmengen filtern, E-Mails auffinden und darstellen sowie temporäre Dateien auswerten und so helfen, das Nutzungsverhalten des Verdächtigen zu ermitteln.[707]

II.2.3.3.6.6.2 Einsatz von Internettechnik für die Fahndung[708]

Der einfache Zugang zu Internetinhalten und die weite Verbreitung von Internetanschlüssen bringen für Strafverfolgungsbehörden auch neue Möglichkeiten der öffentlichen Fahndung mit sich. So konnte in einem vielbeachteten Fall das auf Fotos digital verfremdete Bild eines Kinderschänders wieder erkennbar gemacht und zur Fahndung ausgeschrieben werden.[709] Der Täter konnte daraufhin gefasst und verurteilt werden. Die Online-Fahndung stellt eine Ausschreibung zur Festnahme nach § 131 StPO, beziehungsweise eine Ausschreibung zur Aufenthaltsermittlung nach § 131a StPO dar und darf nach § 131 Absatz 3 StPO, beziehungsweise § 131a Absatz 3 StPO auch öffentlich erfolgen. Neben der Online-Fahndung bietet das Internet auch die Möglichkeit, die Kontaktaufnahme zwischen Bürgern und Behörde zu erleichtern. Die Mehrheit[710] der Polizeibehörden der Bundesländer bietet inzwischen die Möglichkeit, online Strafanzeige zu erstatten. Über diese so genannten Onlinewachen können auch anonyme Hinweise abgegeben werden. Weitere Möglichkeiten

---

[704] BSI, Leitfaden „IT-Forensik“, Version 1.0.1 (März 2011), S. 9, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile

[705] Fox/Kelm, Computer-Forensik, DuD 2004, 491; Willer/Hoppen, Computerforensik – Technische Möglichkeiten und Grenzen, CR 2007, 610, 614.

[706] BSI, Leitfaden „IT-Forensik“, Version 1.0.1 (März 2011), S. 213 f., abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile

[707] Willer/Hoppen, Computerforensik – Technische Möglichkeiten und Grenzen, CR 2007, 610, 615.

[708] Gercke, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 7.

[709] Brunst, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 940; http://www.tagesspiegel.de/weltspiegel/interpol-identifiziert-kinderschaender-vico/1070836.html; http://www.spiegel.de/panorama/justiz/0,1518,572232,00.html

[710] Einen solchen Service bieten bisher nicht der Freistaat Bayern, die Freie Hansestadt Bremen, Rheinland-Pfalz, das Saarland und der Freistaat Thüringen.

sind besonders in der jüngsten Vergangenheit durch die Nutzung von sozialen Netzwerken wie Facebook zur Fahndungsunterstützung entstanden. Dabei ließen sich bereits einige Erfolge erzielen, sodass sich die Nutzung sozialer Netzwerke für die Zukunft anbietet.[711]

II.2.3.3.6.6.3 Aus- und Weiterbildung des Personals

Neben den technischen Ressourcen ist vor allem erforderlich, dass das zur Strafverfolgung eingesetzte Personal über ein hohes Maß an technischen Kenntnissen verfügt. Entsprechende Angebote zur Weiterbildung existieren sowohl auf Landes- als auch auf Bundesebene, beispielsweise zahlreiche Lehrgänge in polizeilichen Ausbildungseinrichtungen. Zudem führt das BKA „deutschlandweite Fortbildungsveranstaltungen“ durch und die „Justizministerien der Länder richten Internettagungen aus, auch das Tagungsprogramm der Deutschen Richterakademie enthält jedes Jahr mehrere solche Veranstaltungen.“[712] Darüber hinaus findet eine intensive Schulung von EDV-Forensikern statt, die den Strafverfolgungsbehörden des Bundes und der Länder zugutekommt. Die internationalen Aus- und Weiterbildungsprogramme, die u. a. von Interpol und Europol ausgerichtet werden, richten sich an Justiz und Polizei und decken ein breites Spektrum der EDV-Forensik ab.

Das prinzipielle Angebot dieser Lehrgänge, Fortbildungen usw. darf jedoch nicht über ein Manko hinwegtäuschen, das in der Praxis kritisiert wird. So setze „die Wahrnehmung von Aus- und Fortbildungsangeboten häufig Eigeninitiative der Fortbildungsinteressierten“ voraus. Zudem sei „die hohe tägliche Arbeitsbelastung bei Justiz und Polizei oft ein Hindernis bei der Anmeldung auf Lehrgängen oder Tagungen, sofern eine Teilnahme nicht, was jedenfalls bei der Justiz die Ausnahme darstellt, verpflichtend ist.“[713]

Zur Verbesserung dieser Situation wurde im Mai 2010 die „Arbeitsgruppe zur Bekämpfung der Informations- und Kommunikationskriminalität“ ins Leben gerufen und im Juni 2011 als ständige Einrichtung etabliert. Diese hat u. a. die Schaffung einer gemeinsamen Informationsplattform für Justiz und Polizei vorgeschlagen. Diese soll zum einen ein auf dem Wikipedia-Prinzip basierendes Online-Lexikon mit IT-relevantem Wissen beinhalten. Zum anderen soll das Lexikon flankiert werden von einem Kommunikationsforum, in dem die Inhalte auch von den Nutzern (ausschließlich aus Justiz und Polizei) diskutiert werden

---

[711] Franosch, Schriftliche Stellungnahme zu Expertengespräch „Internetkriminalität“, S. 13. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

[712] Ebd., S. 4.

[713] Ebd., S. 5.

können, „damit der Informationsfluss nicht lediglich von der Redaktion zu den Nutzern verläuft, sondern auch zwischen den Nutzern, um Informationen sehr schnell verfügbar zu machen“.[714]

II.2.3.3.6.7 Einsatz von Anonymisierungstechnologien und Verschlüsselung

Parallel zu den Möglichkeiten der Strafverfolgungsbehörden kann auch der Täter verschiedene, an sich legale Mittel missbrauchen, um die Arbeit der Strafverfolgungsbehörden zu erschweren. Dabei sind drei Methoden der Verschleierung für Taten im Internet oder mit Internettechnik als Tatmittel von besonderer Bedeutung. Der Täter kann einerseits einen anonymen Internetzugang benutzen; er kann andererseits versuchen seine IP-Adresse zu verschleiern und schließlich kann er Kommunikationsdaten und lokale Daten durch Verschlüsselung gegen Zugriff sichern.[715]

II.2.3.3.6.8 Internationale Zusammenarbeit[716]

Hinsichtlich der Rechtsdurchsetzung bestehen auf internationaler Ebene mehrere Organisationen der grenzübergreifenden Zusammenarbeit. So nimmt das BKA sowohl bei Interpol als auch bei Europol Aufgaben für die Bundesrepublik Deutschland wahr. Neben Europol existiert im Rahmen der EU zudem die Justizbehörde der Union, Eurojust. Diese ist durch Artikel 85 AEUV seit dem Vertrag von Lissabon auch primärrechtlich verankert und dient der Koordinierung und Zusammenarbeit der Strafverfolgungsbehörden der Mitgliedstaaten. Eurojust[717] bemängelte 2010 in seinem Jahresbericht, dass nationale Behörden sich ausschließlich auf die Aufklärung von Straftaten innerhalb ihres Hoheitsgebiets beschränkten, anstatt diese auf EU-Ebene zu bekämpfen.[718] Ob und inwieweit dies auf deutsche Strafverfolgungsbehörden zutrifft, lässt sich dem Jahresbericht nicht entnehmen.

---

[714] Franosch, Schriftliche Stellungnahme zu Expertengespräch „Internetkriminalität“, S. 5. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

[715] Gercke, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 22; s. auch Franosch, Schriftliche Stellungnahme zu Expertengespräch „Sicherheit im Netz“, S. 9 f., der die Anonymität im Internet zu den fünf größten Schwierigkeiten zählt, vor denen die Strafverfolgungsbehörden bei ihren Ermittlungen stehen. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

[716] S. hierzu auch Franosch, Schriftliche Stellungnahme zu Expertengespräch „Internetkriminalität“, S. 6. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

[717] Eurojust hat den Status einer EU-Agentur und koordiniert grenzüberschreitende Strafverfahren auf EU-Ebene.

[718] Eurojust, Eurojust Jahresbericht 2010, S. 31.

Schließlich existiert innerhalb der EU noch das European Judicial Network (Europäische Justizielle Netz, EJN), das insbesondere die Abwicklung von Rechtshilfeersuchen zwischen den nationalen Kontaktstellen erleichtern soll. Im Gegensatz zu Eurojust ist das EJN jedoch nicht zentralistisch organisiert, sondern ein eher loser Verbund, der sich über regelmäßige Treffen organisiert. In Deutschland existieret je eine Kontaktstelle in jedem Bundesland, sowie beim Generalbundesanwalt und dem Bundesamt für Justiz.

II.3. Spionage

II.3.1 Definition des Begriffs der Spionage

Als Definition des Begriffs der Spionage wird vorgeschlagen:

> IT-Spionage oder Internet-Spionage ist das rechtswidrige Sichverschaffen von fremden, geschützten Daten, die auf einem Computer oder sonstigen informationstechnischen Systemen gespeichert sind, unter Verwendung von Computerprogrammen oder sonstigen technischen Mitteln.

Ein Arbeitsbegriff ist erforderlich, da ein feststehender, legal definierter Begriff für Spionage ebenso wenig existiert wie für Sabotage.[719] Für den Arbeitsbegriff kann zunächst auf vorhandene Abgrenzungsversuche aus dem Strafrecht zurückgegriffen werden. Anhaltspunkte bieten die §§ 202a ff. des Strafgesetzbuches (StGB), in denen seit dem 7. August 2007 die IT-Spionage geregelt ist. Umfasst ist sowohl das Ausspähen (§ 202a StGB), das Abfangen (§ 202b StGB), als auch das Vorbereiten dieser Straftaten (§ 202c StGB). Der hier vorgeschlagene Definitionsversuch von IT- oder Internet-Spionage macht sich Elemente aus diesen Vorschriften zu eigen.

II.3.1.1 Vorhandene Definitionen

Ausgangspunkt für eine Begriffsdefinition ist § 202a StGB:

> „(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird [...] bestraft.
>
> (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden."

§ 202a Absatz 1 StGB verwendet in der Überschrift den Begriff des Ausspähens, im Normtext den Begriff des Zugangsverschaffens. Gemeint ist damit, dass der Täter sich oder einem Dritten Herrschaft über die Daten verschafft.[720] Für die Tathandlung reicht aus, dass der Täter von den Daten Kenntnis nimmt oder – ohne Kenntnisnahme – sich oder einem Dritten Besitz

---

[719] S. unten Abschnitt II.4.1.

[720] Kühl, in: Lackner/Kühl, StGB, 27. Aufl. 2011, § 202a Rn. 5.

verschafft.[721] Nach dem Willen des Gesetzgebers soll aber nicht nur die Kenntnisnahme, sondern auch das bloße Eindringen in ein IT-System unter Strafe gestellt werden.[722] Auch die landesverräterische Ausspähung gemäß § 96 Absatz 1 StGB erfordert keine Kenntnisnahme des Inhalts, sondern versteht unter „Verschaffen“ bereits jede Handlung, durch die der Täter Kenntnis des Geheimnisses erlangt, ohne dass er dessen Bedeutung verstehen muss.[723] Die hier vorgeschlagene Definition bedient sich ebenfalls dieses Begriffs; andernfalls wären alle Spionagehandlungen von der Definition ausgenommen, bei denen der Spion nicht weiß, welche Inhalte er ausspäht. Vor allem im Hinblick darauf, dass IT-Systeme auch in der Hoffnung auf Zufallsfunde ausgespäht werden, würde dies jedoch eine zu große Einengung bedeuten.

Die hier vorgeschlagene Definition ist jedoch hinsichtlich der Tathandlung enger als § 202a Absatz 1 StGB, indem sie verlangt, dass das Ausspähen unter Verwendung von Computerprogrammen oder sonstigen technischen Mitteln geschieht. Hierbei bezieht sich die Definition sowohl auf § 202b StGB, der dieses Tatbestandsmerkmal ebenfalls verwendet („Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten [...] verschafft, wird [...] bestraft,...“) als auch auf § 202c Absatz 1 Nummer 2 StGB[724], der u. a. die Verwendung von Computerprogrammen unter Strafe stellt, deren Zweck die Begehung einer der in §§ 202a, 202b StGB genannten Straftaten ist. Mit der Verwendung dieses Definitionsmerkmals wird die Internet-Spionage vom reinen Datenausspähen im Sinne des § 202a Absatz 1 StGB abgegrenzt. Es sind alle diejenigen Tathandlungen ausgeschlossen, bei denen sich der Spion ohne Verwendung einer Schadsoftware oder eines Brute-Force Algorithmus zur Ermittlung von Passwörtern o. Ä. Zugang verschafft.[725]

II.3.1.2 Abgrenzung vom Begriff Sabotage

Die Grenzen zwischen IT-Spionage und IT-Sabotage verschwimmen bei der Frage, ob die unbemerkte Installation eines Computerprogramms auf einem fremden Rechner zur

---

[721] Lenckner/Eisele, in: Schönke/Schröder, StGB, 28. Aufl. 2010, § 202a Rn. 10; Kühl, in: Lackner/Kühl, StGB, 27. Aufl. 2011, § 202a Rn. 5.

[722] BT-Drs. 16/3556, S. 7 ff.

[723] Sternberg-Lieben, in: Schönke/Schröder, StGB, 28. Aufl. 2010, § 96 Rn. 4.

[724] Zur Auslegung von § 202c StGB entsprechend den Vorgaben durch das BVerfG s. oben II.2.3.3.1.

[725] Zum Beispiel gewaltsames Aufbrechen des Gehäuses und Auswerten von proprietärer Steuerungssoftware eines Glücksspielautomaten, Etter, Noch einmal: Systematisches Entleeren von Glücksspielautomaten, CR 1988, 1021, 1024.

Ermöglichung eines weiteren, tiefer gehenden Eindringens (so genannte Backdoor-Trojaner) als Sabotage- oder Spionageakt zu verstehen ist. Zwar ist Sabotage oftmals eine Vorstufe beziehungsweise notwendiges Hilfsmittel für Spionagezwecke – und gleichermaßen Spionage auch für Sabotagezwecke –, doch unterscheiden sich Sabotage und Spionage im Wesentlichen durch die verfolgten Ziele. Während Sabotage durch Datenveränderung der Störung von (technischen) Abläufen beziehungsweise der Zerstörung von Sachsubstanz dient, ist das Hauptziel der Spionage die Informationsgewinnung, ohne dass die betroffenen IT-Systeme zerstört oder beschädigt werden.

II.3.2 Bedeutung des Internets für Spionage

Hier kann im Wesentlichen auf die allgemein für den gesamten Bereich der Internetkriminalität gültigen Gegebenheiten verwiesen werden.[726] Zu erwähnen wären noch folgende Aspekte:

Spionagewerkzeuge sind im Internet erhältlich.[727] Besondere Hacking- oder Coding-Kenntnisse sind nicht immer erforderlich, um Spionageakte auszuführen, da einige Hacker-Tools vollautomatisiert ablaufen und auch von so genannten Script-Kiddies, also unerfahrenen Hackern, die sich vorbereiteter Hacking-Tools bedienen, verwendet werden können.[728]

Wer im Internet spioniert, muss nicht aufwendig und teuer angeworben oder ausgebildet werden; er muss nicht unter größtem Risiko in Unternehmen oder Behörden eingeschleust werden; er muss kein Doppelleben führen und auch das Entdeckungsrisiko minimiert sich dahingehend, dass zwar die Datenverbindung gekappt wird, der im Ausland sitzende Spion aber häufig weder Inhaftierung noch Verhöre zu befürchten hat. Somit ist IT-Spionage im Verhältnis zur „klassischen“ Spionage einfach, risikoarm und kostengünstig.[729]

Die Möglichkeit der Verschleierung der eigenen Identität führt dazu, dass Spionageakte von Ermittlungsbehörden und -diensten oft nicht ohne Weiteres als feindliche Akte ausländischer Staaten oder Organisationen erkannt werden können, sodass Spionage über das Internet für

---

[726] S. auch oben Abschnitte II.2.1.6 und II.2.1.7.

[727] Gercke, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 16.

[728] Ernst, Computerstrafrecht 2007, DS 2007, 335, 337 f.; Gaycken, Cyberwar, 2011, S. 50.

[729] Gaycken, Cyberwar, 2011, S. 139.

diese Späher politisch-militärisch wesentlich geringere Risiken bieten dürfte als die „herkömmliche“ Spionage.[730]

Auch im Verfassungsschutzbericht 2011 wird neben der Gefahr der „klassischen“ Spionage durch Diplomaten und durch als Journalisten getarnte Agenten auch die Verwendung des Internets als Spionagemittel besonders hervorgehoben.[731]

Zusammenfassend lässt sich daher sagen, dass die IT-Spionage kaum noch mit der „herkömmlichen“ Spionage vergleichbar ist, insbesondere da der Zugriff auf Daten durch deren Körperlosigkeit sowie die wachsende Vernetzung mittlerweile keine körperliche Anwesenheit des Täters mehr voraussetzt (und sei es nur zur Installation von Abhörgeräten in Telefonen). In Bezug auf die finanzielle, technische und personelle Hemmschwelle hat sich die Spionage durch ihren IT-Bezug nunmehr folglich der normalen Internetkriminalität angenähert, sodass der Unterschied zwischen beiden Bereichen in erster Linie definitorischer Natur ist.

II.3.3 Akteure

Es lassen sich einzelne Gruppen von Akteuren zusammenfassen. Während bei einigen Akteuren die Begehung von Straftaten im Vordergrund steht und sie daher überwiegend als Täter auftreten, sind andere Akteure vielfältig motiviert und können daher wechselnd sowohl als Täter als auch als Opfer auftreten.

II.3.3.1 Hacker[732]

Entstanden ist die Hackercommunity ursprünglich in einem nicht-kommerziellen Kontext, zu einer Zeit, als Sicherheitstechnik noch nicht vertrieben wurde. Auch der universitäre Einfluss war stark. Dabei spielte eine Rolle, dass Rechner an Universitäten, die zu Forschungszwecken benutzt wurden, zum Hacken eingesetzt werden konnten. Eine Kultur des Teilens und Tauschens von Informationen war das vorherrschende Paradigma, aus dem auch die Open-Source-Szene hervorging.

---

[730] Gaycken, Cyberwar, 2011, S. 140.

[731] Bundesamt für Verfassungsschutz, Verfassungsschutzbericht 2011, S. 350 ff., abrufbar unter: http://www.verfassungsschutz.de/download/SHOW/vsbericht_2011_vorabfassung.pdf

[732] Die Ausführungen in Kapitel II.3.3.1 beruhen auf einem von der Sachverständigen Constanze Kurz am 19. Februar 2010 in der FAZ veröffentlichten Artikel. Online abrufbar unter: http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/aus-dem-maschinenraum-der-hacker-1939779.html

Eine Definition des Begriffs findet sich im „Hacker‘s Dictionary“: Ein Hacker sei „eine Person, die Spaß daran hat, die Feinheiten programmierbarer Systeme zu erforschen und ihre Möglichkeiten auszureizen“.[733] Das trifft die Essenz des Hackens aber nur bedingt, denn neben Neugier und wachsender Erfahrung spielen eine typische Geisteshaltung und eine gewisse Skepsis gegenüber den Angaben der Hersteller von Systemen eine Rolle. Als der Begriff des Computer-Hackers Ende der fünfziger Jahre erfunden wurde, hatte er durchaus keine negative oder destruktive Konnotation. Hacken bedeutete, durch technische Operationen Grenzen zu finden und zu erweitern, aber auch, Wissen zu teilen und gemeinsam an technischen Systemen zu forschen. Bis heute versteht man unter Hacken die Fähigkeit, Technik in unerwarteter, neuer Weise zu verwenden, die vom Hersteller nicht unbedingt intendiert ist. Es geht darum, die Fähigkeiten eines Computers auszureizen und Sperren, die eine solche Nutzung verhindern, gegebenenfalls zu umgehen. Auch wollen Hacker sich nicht damit zufriedengeben, dass ein technisches System etwa aus Gründen eines Geschäftsmodells eingeschränkt wird.

Mit einem solchen intimen Verständnis aller Kleinigkeiten und Details von Technologien, die vielleicht neue Wege, neue Möglichkeiten eröffnen, geht auch eine gesellschaftliche Verantwortung einher. Dies wird jedem Hacker bewusst, sobald er zum ersten Mal eine echte technische Grenze überschreitet und verborgene Daten offenlegt. Hinzu kommt die Verantwortung, mehr über die technischen Systeme herauszufinden, die unseren Alltag immer weitgehender beherrschen. Denn Technik hat letztlich stets auch politische Implikationen.

Die Hacker-Ethik, eine Sammlung ethischer Werte, die für die Hacker-Kultur als maßgeblich betrachtet wird,[734] hält dazu an, betroffene Systeme so zu hacken, dass möglichst wenig oder kein Schaden verursacht wird. Es soll lediglich der Beleg einer vorhandenen Sicherheitslücke erbracht werden, aber beispielsweise keine Daten verändert oder gelöscht werden. Heute übliche Angriffsmethoden wie Botnetze (siehe Kapitel II.2.1.5.1) widersprechen einer solchen Hackerethik eindeutig. Auch legen die Betroffenen Wert darauf, dass Fähigkeiten, Erfolge, Kompetenzen und Erfahrungen anerkannt werden. Hacker wollen nach ihrem Handeln beurteilt werden, die Hackercommunity ist insofern meritokratisch organisiert.

Im Laufe der Zeit hat sich jedoch das Image der Hacker verändert, nicht zuletzt in den Medien, weil auch Kriminelle sich gern als Hacker bezeichnen.

---

[733] Raymond, The new hacker's dictionary, 3. Aufl. 1996, S. 233.

[734] http://www.ccc.de/hackerethics

II.3.3.2 Organisierte Kriminalität

Auch im Feld der Spionage spielen organisierte Kriminalitätsformen eine Rolle. Dabei kann aber auf die Ausführungen in Kapitel II.2 zur Kriminalität im Internet verwiesen werden.[735]

II.3.3.3 Staaten

Aufgrund fehlender Fakten ist es schwer festzustellen, ob überhaupt und in welchem Umfang Staaten Spionageangriffe auf andere Staaten unternommen haben. Lediglich in letzter Zeit sind einige Fälle in Medienberichten öffentlich geworden, bei denen mutmaßlich Spionageangriffe anderer Staaten auf Deutschland registriert worden sind. So wurde im August 2007 berichtet, dass China mutmaßlich das deutsche Kanzleramt mit Trojanern infizierte, um so an vertrauliche Daten zu gelangen. Der Verfassungsschutz soll dabei das Ausspähen von 160 Gigabyte Daten verhindert haben.[736] Russland soll im November 2008 mit einem Virus[737] Computer des amerikanischen Verteidigungsministeriums Pentagon ausspioniert haben.[738] Nach einem anderen Angriff auf das Pentagon, bei dem 24 000 sensible Dokumente ausgespäht wurden,[739] legte das US-Verteidigungsministerium im Juli 2011 ein Strategiepapier[740] zur Bekämpfung von Attacken aus dem Cyberspace vor.

Die Mehrzahl der Spionageangriffe aus dem Ausland stammt dem Verfassungsschutzbericht 2011 zufolge aus Russland und China.[741]

Mutmaßlich richten Geheimdienste sich nicht nur gegen staatliche Ziele, sondern betreiben mit großer Wahrscheinlichkeit auch Wirtschafts- und Industriespionage. Die Aufklärungsziele sind dabei zum einen Großunternehmen wie Google, dem bei einer mutmaßlich aus China stammenden Attacke , u. a. der Quellcode des Authentifizierungssystems Gaia gestohlen wurde, welches in nahezu allen Google-Diensten zur Anwendung kommt.[742] Aber auch die mittelständische Wirtschaft gilt als Zielobjekt, da sie anscheinend aufgrund der hohen Kosten nur über weniger effektive Abwehrmöglichkeiten verfügt und auch die Gefahren der

---

[735] S. oben II.2.1.5.4.

[736] http://www.heise.de/newsticker/meldung/China-spaeht-angeblich-PCs-des-Bundeskanzleramtes-aus-167017.html

[737] http://www.f-secure.com/v-descs/worm_w32_agent_btz.shtml#additional

[738] http://www.heise.de/newsticker/meldung/Virusangriff-auf-Pentagon-Rechner-soll-von-Russland-ausgegangen-sein-218635.html

[739] http://www.heise.de/newsticker/meldung/USA-legen-Verteidigungsstrategie-fuer-den-Cyberspace-vor-1279764.html

[740] „Department of Defense Strategy for Operating in Cyberspace“, abrufbar unter: http://www.defense.gov/news/d20110714cyber.pdf

[741] Bundesamt für Verfassungsschutz, Verfassungsschutzbericht 2011, S. 321, abrufbar unter: http://www.verfassungsschutz.de/download/SHOW/vsbericht_2011_vorabfassung.pdf

[742] http://www.nytimes.com/2010/04/20/technology/20google.html

Wirtschaftsspionage unterschätzt.[743] So forderte erst kürzlich der damalige Präsident des Verfassungsschutzes, Heinz Fromm, einen besseren Schutz vor Wirtschaftsspionage für deutsche Unternehmen.[744] Von besonderem Interesse für staatliche Geheimdienste ist die Gewinnung von Informationen, Forschungsergebnissen und Bauplänen bezüglich militärisch nutzbarer Güter sowie Dual-Use-Gütern, also zivilen Produkten, die auch militärisch genutzt werden können.[745]

II.3.3.4 Wirtschaft

Wirtschaftsunternehmen könnten ein Interesse daran haben, an vertrauliche Informationen von staatlichen Stellen und anderen privatwirtschaftlichen Unternehmen zu gelangen. Die denkbaren Spionageziele sind dabei vielfältig. Zum einen könnte sich ein Unternehmen über den Stand bei einem Vergabeverfahren öffentlicher Aufträge oder eines Investitionsvorhabens informieren wollen, um seine Position durch Anpassung des eigenen Angebots zu verbessern. Das Ausspähen von technischen Lösungen im Vorfeld einer Patentanmeldung oder deren Anmeldung in Patentämtern kann einem Unternehmen ebenso einen Vorteil verschaffen wie die Kenntniserlangung über den Ermittlungsstand in einem Kartellverfahren. Aber auch auf lokaler Ebene kann das Ausspähen von Daten, zum Beispiel bei der Vergabe öffentlicher Aufträge, eine große Rolle spielen.

Es ist nicht immer feststellbar, ob hinter Angreifern Wirtschaftsunternehmen oder staatliche Behörden stehen. Dennoch dürften auch Fälle von Wirtschaftsspionage eindeutig zu den berichteten Sachverhalten gehören, zumal sich bei einigen Staaten politisch motivierte von wirtschaftlich motivierten Angriffen nur schwer trennen lassen, etwa beim Zugang zu Hochtechnologie.[746] Zwar sind keine Fälle bekannt, in denen Wirtschaftsunternehmen gezielt Konkurrenten ausspähen; doch ist anzunehmen, dass frühere Spionageaktivitäten inzwischen per Internet (wesentlich effizienter) fortgesetzt werden.

Hinzu kommen aber wohl auch Wirtschaftsunternehmen, die die schon früher bestehende Wirtschaftsspionage auf das Internet erstrecken, um Unternehmensgeheimnisse ihrer Konkurrenten auszuspähen.

---

[743] Bundesamt für Verfassungsschutz, Verfassungsschutzbericht 2011, S. 354, abrufbar unter: http://www.verfassungsschutz.de/download/SHOW/vsbericht_2011_vorabfassung.pdf

[744] http://www.noz.de/deutschland-und-welt/politik/53496986/die-bedrohungslage-bleibt-ernst

[745] Möhrenschläger, in: Wabnitz/Janovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 3. Aufl. 2007, Kap. 13 II 1 Rn. 2.

[746] S. http://www.handelsblatt.com/unternehmen/mittelstand/mittelstand-im-visier-von-wirtschaftsspionen/3127338.html

II.3.3.5 Weitere Akteure

Zu den Akteuren zählen auch Personen(-gruppen), die ergänzend tätig werden und den Drahtziehern beispielsweise erst das für den Angriff erforderliche Wissen und die Ausrüstung verschaffen. Dies können die Produzenten von Schadsoftware sein, aber auch Mittelspersonen, die lediglich als „Dealer“ der Schadsoftware auftreten. Insofern kommen all jene in Betracht, die den Drahtziehern der Angriffe Ressourcen bereitstellen oder programmiertechnische Auftragsarbeit leisten (vergleich zum Handel mit Zero-Day-Exploits Kapitel II.2.2.2.2).

II.3.4 Bedrohungen, Angriffsmittel und Schutzmöglichkeiten

Hinsichtlich der Angriffsmittel, Ursachen und Motivationen kann auf die Ausführungen in Kapitel II.2 zur Kriminalität im Internet verwiesen werden.[747] Speziell in Bezug auf Spionage ist lediglich anzumerken, dass sich die einschlägigen Attacken von der übrigen Kriminalität im Internet insofern unterscheiden, als sich ihre Ausmaße nicht selten in größeren Dimensionen bewegen.

II.3.5 Vorhandene Regelungen und Maßnahmen zum Schutz vor Spionage

II.3.5.1 Internationale Regelungen und Maßnahmen

Wie schon in Kapitel II.2 zur Kriminalität im Internet ausgeführt, bedingt die Globalität des Internets erhebliche Anstrengungen in der internationalen Zusammenarbeit. Auf die dortigen Ausführungen sei auch an dieser Stelle verwiesen.[748]

II.3.5.2 Nationale Regelungen und Maßnahmen

Über die bereits in Kapitel II.2 zur Kriminalität im Internet aufgeführten Grundlagen hinaus sind hier einige spionage-spezifische Regelungen und Maßnahmen hervorzuheben:

---

[747] S. oben Abschnitte II.2.1.4, II.2.1.5, II.2.1.6, II.2.1.7 sowie II.2.2.

[748] S. oben Abschnitt II.2.3.1.

II.3.5.2.1 Strafverfolgung

II.3.5.2.1.1 Landesverrat und Gefährdung der äußeren Sicherheit

Die Strafvorschriften der §§ 93 ff. StGB sind Normen, die den Missbrauch von Staatsgeheimnissen unter Strafe stellen. Hierbei handelt es sich nicht um spezifische, ausschließlich Internet-Spionage betreffende Vorschriften, sondern um solche, die Spionage im Allgemeinen unter Strafe stellen. Dazu gehören:

- § 94 StGB (Landesverrat),
- § 95 StGB (Offenbarung von Staatsgeheimnissen),
- § 96 StGB (Landesverräterische Ausspähung; Auskundschaften von Staatsgeheimnissen),
- § 97 StGB (Preisgabe von Staatsgeheimnissen),
- § 97a StGB (Verrat illegaler Geheimnisse),
- § 97b StGB (Verrat in irriger Annahme eines illegalen Geheimnisses),
- § 98 StGB (Landesverräterische Agententätigkeit),
- § 99 StGB (Geheimdienstliche Agententätigkeit).

Die genannten Normen basieren größtenteils auf dem Begriff des Staatsgeheimnisses im Sinne von § 93 StGB. Staatsgeheimnisse sind der darin enthaltenen Legaldefinition zufolge „Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheim gehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden“.

II.3.5.2.1.2 Rechtsdurchsetzung

Wie schon allgemein in Kapitel II.2 zur Kriminalität im Internet ausgeführt, gilt auch für die Bekämpfung von Spionageakten, dass nicht nur materielle Regeln, sondern auch deren Durchsetzung (englisch: enforcement) maßgeblich ist.[749]

Bei der Bekämpfung von Kriminalität im Internet spielt insbesondere die hohe technische Komplexität von Datenverarbeitungsvorgängen und Telekommunikation eine wesentliche Rolle. In diesem Zusammenhang wird von Praxisseite auch auf das Erfordernis entsprechender Aus- und Weiterbildung der in der Strafverfolgung tätigen Personen

[749] S. hierzu oben Abschnitt II.2.3.3.6.

verwiesen.[750] Relevant sind die Beherrschung der erforderlichen Ermittlungsmethoden und der entsprechenden forensischen Auswertungs- und Ermittlungssoftware sowohl für die Polizei und Staatsanwaltschaft als auch für die Gerichte. Auf Bundes- und Länderebene wird hierzu ein entsprechendes Schulungsangebot in Form von Lehrgängen, Fortbildungsveranstaltungen und Internettagungen durch das Bundeskriminalamt (BKA), die Justizministerien der Länder, die Deutsche Richterakademie und das Bundesamt für Sicherheit in der Informationstechnik (BSI) angeboten und gefördert. [751]

Neben diesen Faktoren von technischem Hintergrundwissen der Strafverfolgungsbehörden sind auch die strafprozessualen Rahmenbedingungen maßgeblich für den Erfolg oder Misserfolg der Bekämpfung von Spionageakten und Kriminalität im Internet. Die Strafprozessordnung bietet durchaus brauchbare Instrumente zur Täterermittlung. So werden von der Praxisseite die Maßnahmen der Telekommunikationsüberwachung und Observation (§§ 100a, 100g, 100h StPO) sowie die verdeckte personale Internetermittlung als erfolgreich beschrieben.[752] Gerade angesichts der Anonymisierungsmöglichkeiten, die das Internet bietet, werden Ermittlungen etwa in sozialen Netzwerken zukünftig an Bedeutung gewinnen.

II.3.5.2.2 Sonstige Maßnahmen und Anreize

Für die Frage, welche technischen oder sonstigen Schutzmaßnahmen bestehen, die den Schutz durch die genannten strafrechtlichen Normen flankieren, kann an dieser Stelle auf die einschlägigen Ausführungen in Kapitel II.2 zur Kriminalität im Internet verwiesen werden, insbesondere auf die Regelung des § 17 Absatz 1, 2 Nummer 1a UWG, der eine Form der „herkömmlichen“ Spionage pönalisiert.

Speziell im Hinblick auf Spionage ist überdies zu bedenken, dass zumindest nicht auszuschließen ist, dass es sich bei den Akteuren auf Täterseite um Akteure aus dem globalen politischen Bereich handelt. Anders als bei sonstigen Tätern wird die Rechtsdurchsetzung in diesen Fällen zusätzlich dadurch erschwert, dass der rein justizielle Bereich der Strafverfolgung überlagert wird von politisch-diplomatischen Erwägungen, die etwaigen Strafverfolgungsmaßnahmen und selbst der offiziellen öffentlichen Kommunikation über etwaige Verfahren im Wege stehen könnten.

---

[750] Franosch, Schriftliche Stellungnahme zu Expertengespräch „Internetkriminalität“, S. 4. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

[751] Ebd.

[752] Ebd., S. 13.

II.3.6 Risikoeinschätzung

Für die Einschätzung der Risiken ist das Wissen über die relevanten Faktoren maßgeblich, die Spionage begünstigen oder ihr auch entgegenstehen und schließlich der Grad und das potenzielle Ausmaß von Schäden. Eine Risikoanalyse ist hier nicht anders als bei anderen Technologien (zum Beispiel im Industrieanlagenrecht) anhand folgender Kriterien durchzuführen:

- Bedrohte Akteure (Staat, Wirtschaft, Gesellschaft),
- Bedrohte Rechtsgüter,
- Wahrscheinlichkeit und Ausmaß des Schadens sowie eine
- Kosten-Nutzen-Abwägung.

Rechtsgüter können hier unmittelbar und mittelbar bedroht sein. Konkret sind dies:

- Finanzielle Schäden, entstanden durch entwendete Passwörter, Kreditkartendaten, gehackte PayPal-Accounts o. Ä.[753] Dies gilt erst recht für Phishing-Attacken, die dazu führen, dass erwünschte vereinfachte Zahlungsmethoden von Nutzerinnen und Nutzern nicht mehr verwandt werden,
- Digitale Identitäten[754] und deren Missbrauch beziehungsweise „Diebstahl“,
- Verlust vertraulicher Unternehmensdaten[755],
- Missbrauch von Netzwerkressourcen[756],
- Ruf- und Markenschädigungen[757],
- das Recht auf informationelle Selbstbestimmung beziehungsweise auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[758].

Organisierte Kriminalität kann durch Spionage erhebliche Schäden anrichten. Sie kann, wenn sie den großen Profit erkennt, die notwendigen Mittel aufbringen sowie Vertriebswege für

---

[753] Panda/Mangla, Protecting Data from the Cyber Theft – a Virulent Disease, Journal of Emerging Technologies in Web Intelligence, Vol. 2 (2010), No. 2, 152.

[754] Zum Begriff: Gercke, Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden, MMR 2008, 291, 291 f.

[755] Panda/Mangla, Protecting Data from the Cyber Theft – a Virulent Disease, Journal, Journal of Emerging Technologies in Web Intelligence, Vol. 2 (2010), No. 2, 152.

[756] Ebd., No. 2, 152.

[757] Ebd.

[758] Wie vom Bundesverfassungsgericht beschrieben in BVerfGE 120, 274 ff. – Online-Durchsuchung.

erlangte Informationen schaffen oder zur Verfügung stellen.[759] Aufgrund der höheren Professionalisierung ist es ebenfalls nicht ausgeschlossen, dass sich die organisierte Kriminalität eines Innentäters bedient, um Informationsinfrastrukturen anzugreifen wodurch sie nicht auf einen Angriff über das Internet angewiesen ist.[760] Damit wären auch entkoppelte Netze und Systeme gefährdet. Militärisch-nachrichtendienstliche Angreifer können durch Wirtschaftsspionage fremde Volkswirtschaften zugunsten der eigenen Volkswirtschaft schädigen.[761] Diese Angreifer verfügen zudem über die notwendigen Mittel, großangelegte Operationen vorzubereiten und durchzuführen.

Nach Aussage des BSI werden Spionage-Angriffe gegen die Bundesverwaltung insbesondere durch mit Schadsoftware infizierte Dokumente geführt.[762] Aus den dem BSI vorliegenden Daten lässt sich jedoch nicht schließen, ob es sich dabei um staatliche Angreifer oder Angreifer aus dem Bereich der organisierten Kriminalität handelt.[763] Um sich einen präziseren Überblick zu verschaffen, fehlen derzeit hinreichende Forschungserkenntnisse.

[759] Gaycken, Schriftliche Stellungnahme zu Expertengespräch „Sicherheit im Netz“, S.2.

[760] Ebd.

[761] Ebd.

[762] Könen, Schriftliche Stellungnahme zu Expertengespräch „Sicherheit im Netz“, Frage 1 c).

[763] Ebd.

II.4. Sabotage

II.4.1 Definition des Begriffs der Sabotage

Als Definition des Begriffs der Sabotage wird vorgeschlagen:

> Nutzung von IT und des Internets zur absichtlichen Beeinträchtigung und Zerstörung von wirtschaftlichen, staatlichen oder gesellschaftlichen Rechtsgütern, die für die Sicherheit der Bundesrepublik Deutschland und die Gesamtwirtschaft bedeutsam sind , um ein ideologisches, politisches oder wirtschaftliches Ziel durchzusetzen.

Ein Arbeitsbegriff ist erforderlich, da der Terminus der Sabotage uneinheitlich verwandt wird:

- „Sachen, die in erhöhtem Maße der Gefahr eines gemeingefährlichen Missbrauchs (Sabotage) ausgesetzt sind“[764],
- „absichtliche [planmäßige] Beeinträchtigung der Leistungsfähigkeit politischer, militärischer oder wirtschaftlicher Einrichtungen durch [passiven] Widerstand, Störung des Arbeitsablaufs oder Beschädigung und Zerstörung von Anlagen, Maschinen o.Ä.“[765],
- „aewusste Beeinträchtigung von militärischen oder politischen Aktionen oder von Produktionsabläufen zum Beispiel durch (passiven) Widerstand oder durch Zerstörung wichtiger Anlagen und Einrichtungen.“[766].

Konkretere und präziser gefasste Begriffe finden sich im Strafgesetzbuch, namentlich in §§ 87, 88, 109e und 303b StGB. Demnach definiert § 87 Absatz 2 StGB die Sabotagehandlungen als:

„1. Handlungen, die den Tatbestand der §§ 109e, 305, 306 bis 306c, 307 bis 309, 313, 315, 315b, 316b, 316c Abs. 1 Nr. 2, der §§ 317 oder 318 verwirklichen, und

2. andere Handlungen, durch die der Betrieb eines für die Landesverteidigung, den Schutz der Zivilbevölkerung gegen Kriegsgefahren oder für die Gesamtwirtschaft wichtigen Unternehmens dadurch verhindert oder gestört wird, daß eine dem Betrieb dienende Sache

---

[764] Sonntag, IT-Sicherheit kritischer Infrastrukturen, 2005, S. 153, unter Bezugnahme auf VGH Baden-Württemberg, JZ 1983, 104 f., der selbst allerdings den Begriff „Sabotage“ nicht nennt.

[765] Duden, Das große Wörterbuch der deutschen Sprache, 3. Aufl. 1999, Bd. 7.

[766] Brockhaus – Die Enzyklopädie: in 24 Bänden, 20. Aufl. 1998, Bd. 18.

zerstört, beschädigt, beseitigt, verändert oder unbrauchbar gemacht oder daß die für den Betrieb bestimmte Energie entzogen wird.“

Im Kern enthält Nummer 2 die auch hier relevante Definition, die allerdings verengt ist auf den Schutz bestimmter kritischer Einrichtungen und Infrastrukturen oder Unternehmen.

Breiter ist demgegenüber in § 303b StGB der Begriff der Computersabotage angelegt, der schon bei einer erheblichen Störung einer (bedeutsamen) Datenverarbeitung eingreift, sei es durch Dateneingabe oder Manipulation von Datenverarbeitungsanlagen oder Datenträgern (Absatz 1). Strafverschärfend wirken auch hier nach Absatz 4 Nummer 3 Angriffe auf für die Sicherheit der Bundesrepublik Deutschland lebenswichtigen Einrichtungen.

Daraus wird die uneinheitliche Verwendung deutlich: Computersabotage reiht sich in die EDV-bezogenen Delikte ein, während Sabotage nach § 87 StGB deutlich auf die Gefährdungen des Gemeinwesens bezogen ist. Die Computersabotage nach § 303b StGB gehört daher eher in den anderweitig zu diskutierenden Zusammenhang der Kriminalität im Internet[767] . Auch die Polizeiliche Kriminalstatistik (PKS) 2011 folgt dieser Gewichtung, indem sie Computersabotage im Sinne von § 303b StGB als einen Bestandteil von „IuK-Kriminalität im engeren Sinne“ qualifiziert.[768]

Sabotage ist schließlich gegenüber terroristischen Akten der umfassendere Begriff, da Terrorismus hier als Akte krimineller Vereinigungen im Sinne von § 129a StGB verstanden wird.

II.4.2 Bedeutung des Internets für Sabotage

Das Internet spielt sowohl als Hilfsmittel als auch als Ziel von Sabotageakten eine große Rolle, denn neben den auch für den Bereich der Internetkriminalität gültigen Gegebenheiten (Unabhängigkeit von Tat- und Handlungsort, einfache Angreifer-Identitätsverschleierung und -fingierung durch Botnetze u. Ä., Erschwerung der Ermittlung und Strafverfolgung) ist

---

[767] Vgl. hierzu die Ausführungen in Kapitel II.II.1.3.

[768] BMI, Polizeiliche Kriminalstatistik 2011, S. 4, abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2012/PKS2011.pdf?__blob=publicationFile; im Cybercrime Bundeslagebild 2010 des BKA wird hierfür der Begriff „Cybercrime im engeren Sinne“ verwendet, der wiederum definiert wird als alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden und bei denen Elemente der elektronischen Datenverarbeitung (EDV) wesentlich für die Tatausführung sind, vgl. BKA, Cybercrime Bundeslagebild 2010, S. 5, abrufbar unter: http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf

insbesondere ein Aspekt hervorzuheben: Aufgrund der hohen Vernetzung der Dienste und Infrastrukturen lassen sich mit verhältnismäßig geringem Aufwand sehr schnell hohe Schäden und Wirkungen erzielen, zum Beispiel durch Angriffe auf die Verteilerknoten der Backbone-Netze des Internets oder durch sehr schnelle Verbreitung von Schadsoftware.

Beispielhaft sei hier auf den Fall verwiesen, dass die IT-Systeme eines Kraftwerkes (oder einer beliebigen anderen Anlage aus dem Bereich Kritischer Infrastrukturen) mit dem Internet verbunden sind. Dadurch ist es nicht erforderlich, dass Saboteure zuerst beispielsweise über Innentäter auf das Anlagengelände gelangen, um vor Ort in das IT-System einzudringen. Stattdessen können sich die Täter aller der genannten, allgemeingültigen Vorteile der Internetkriminalität zunutze machen.[769]

II.4.3 Akteure/Konstellationen

Wie aus der hier zugrunde gelegten Definition hervorgeht, lassen sich im Wesentlichen drei Kategorien von Sabotageakten benennen: politisch motiviert,ideologisch motiviert und wirtschaftlich motiviert. Zu bedenken ist aber, dass die hier zugrunde gelegte Definition auch ein Erheblichkeitskriterium enthält. Erfasst wird nicht jede Beeinträchtigung oder Zerstörung beliebiger, sondern erst für die Sicherheit der Bundesrepublik Deutschland und die Gesamtwirtschaft bedeutsamer wirtschaftlicher, staatlicher oder gesellschaftlicher Rechtsgüter. Gemessen daran, dürfen realistischerweise nur solche Akteure in Betracht gezogen werden, die potenziell auch über entsprechende Mittel verfügen, Angriffe dieser Ausmaße zu planen, die nötigen Mittel aufzubringen sowie die Durchführung zu bewerkstelligen.

Auf Täterseite sind als potenzielle Verantwortliche von Sabotageakten daher zum einen Staaten zu nennen, zum anderen größere nicht-staatliche Gruppierungen (zum Beispiel Terror-Organisationen oder andere Aktivisten, die sich gegen bestimmte politisch inkriminierte Unternehmen oder Organisationen richten), aber auch große Wirtschaftsunternehmen (Wirtschaftssabotage).

Gesicherte Erkenntnisse über konkrete Hintergründe und Personenkonstellationen liegen allerdings in den seltensten Fällen vor, sodass in der Regel lediglich über Zusammenhänge

[769] S. hierzu auch das Beispiel Stuxnet, unten Abschnitt II.4.4.1.

spekuliert werden kann (siehe auch Kapitel II.4.4.1 sowie II.4.4.2 zu den Beispielen des Stuxnet-Computerwurms und des Angriffs auf Estland).

Zu bedenken ist schließlich noch, dass zu den Akteuren nicht nur die Drahtzieher der Sabotageakte zu zählen sind, sondern ebenso diejenigen Personen(-gruppen), die ergänzend tätig werden und den Drahtziehern beispielsweise erst das für den Angriff erforderliche Equipment verschaffen. Dies können die Produzenten von Schadsoftware sein, aber auch Mittelspersonen, die lediglich als „Dealer“ der Schadsoftware auftreten. Insofern kommen all jene in Betracht, die den Drahtziehern der Angriffe Ressourcen bereitstellen oder für sie programmiertechnische Auftragsarbeit leisten.

II.4.4 Bedrohungen, Angriffsmittel und Schutzmöglichkeiten

Über die bereits in Kapitel II.2 zur Kriminalität im Internet geschilderten Grundlagen hinaus sind hier besonders zwei bekannt gewordene Beispiele hervorzuheben:

II.4.4.1 Angriff mit hochentwickelter Malware (zum Beispiel Stuxnet)

Im Juni 2010 wurde der so genannte Stuxnet-Computerwurm entdeckt,[770] dessen Angriffstechnik die komplexe Interaktion von Software und menschlichem Fehlverhalten beziehungsweise dessen Ausnutzung demonstriert. Seine Schadroutine war speziell für den Angriff auf ein IT-System der Firma Siemens zur Überwachung, Steuerung und Automatisierung technischer Prozesse ausgerichtet (so genannte SCADA-Systeme), insbesondere wohl[771] von im Iran befindlichen Industrieanlagen zur Urananreicherung.[772] Die Steuerungssoftware für Industrieanlagen befand sich auf IT-Systemen mit dem Betriebssystem Microsoft Windows. Stuxnet nutzte mehrere gewisse zuvor nicht bekannte Sicherheitslücken, so genannte Zero-Day-Exploits[773], aus, um die Kontrolle auf die Software und damit die Steuerungsanlagen zu erhalten.[774]

---

[770] S. ausführlich dazu Gaycken, Cyberwar, 2011, S. 175 ff.

[771] Zweifelnd Gaycken, Cyberwar, 2011, S. 18, s. weiter ausführlich zu den Argumenten, warum Gaycken eine gezielte Entwicklung für die Beeinträchtigung des iranischen Atomprogramms für unwahrscheinlich erachtet und andere Beweggründe als wahrscheinlicher ansieht, S. 177 ff.

[772] Gaycken, Cyberwar, 2011, S. 175.

[773] Siehe zum Begriff Zero-Day-Exploits auch Kapitel II.2.2.2.2 .

[774] Gaycken, Cyberwar, 2011, S. 18, 176.

Auch wenn sich die Funktionsweise technisch nicht von anderen Computerwürmern unterscheidet,[775] fällt die bis dahin nicht dagewesene hohe Qualität und Komplexität der Schadsoftware auf. [776] Die Entwicklungkosten des Stuxnet-Wurms sollen nur mit erheblichem Personal- und Sachaufwand möglich gewesen sein.[777]

Jüngst wurde schließlich ein Bericht der New York Times veröffentlicht, demzufolge die Entwicklung und der Einsatz von Stuxnet von der US-amerikanischen Regierung in Auftrag gegeben worden sein soll, ohne dass diese Information aber offiziell bestätigt wurde.[778]

II.4.4.2 DDoS-Angriff auf Estland

Als Paradebeispiel für breitflächige Sabotage über das Internet kann der in der Geschichte wohl bislang größte DDoS-Angriff[779] im Jahr 2007 auf Estland angesehen werden.[780] Denn es wurden über eine Million Computer in den mehrere Wochen andauernden Angriff eingebunden,[781] die wiederum Bestandteil vieler verschiedener Botnetze gewesen sein mussten.[782] Hierdurch wurde nicht, wie üblich, eine einzelne Internetseite mittels einer Flut von Zugriffen lahmgelegt, sondern vielmehr kam es zu Ausfällen zentraler Internetdienste, wie etwa diverser Bank- und Zahlungssysteme, den meistgenutzten Websites und auch Regierungswebsites sowie des Internetverzeichnisdienstes.[783] Der gesamte Finanz- und Kommunikationssektor war landesweit beeinträchtigt. Die estnische IT-Infrastruktur stellte dabei ein besonders attraktives Cyber-Angriffsziel dar, da das baltische Land eine der weltweit am stärksten vernetzten Nationen ist.[784]

Die Angriffe standen zeitlich in Zusammenhang mit der Demontierung eines sowjetischen Denkmals in Form eines Rote-Armee-Bronzesoldaten in der Stadt Tallin.[785] Die Rückverfolgung der Kommunikation einiger Botnetz-Client-Computer weist auf Botnetz-

---

[775] Gaycken, Cyberwar, 2011, S. 18.

[776] Ebd., S. 18, insbesondere zu den technischen Details s. S. 176 f.

[777] So ähnlich Gaycken, Cyberwar, 2011, S. 18, 176 f.; http://www.golem.de/1009/78278-2.html; ähnlich die Einschätzung von Symantec, vgl. http://www.symantec.com/business/theme.jsp?themeid=stuxnet sowie von Kaspersky, vgl. http://www.golem.de/1009/78245.html, die nur Staaten dazu in der Lage sehen.

[778] S. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1

[779] Zum Begriff des DDoS-Angriffs siehe Kapitel II.2.1.5.1.

[780] S. dazu ausf. Clarke/Knake, Cyberwar, 2010, S. 11 ff.; s. weiter Gaycken, Cyberwar, 2011, S. 169 ff.

[781] Gaycken, Cyberwar, 2011, S. 170.

[782] Clarke/Knake, Cyberwar, 2010, S. 14 f.

[783] S. hierzu auch Gercke, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 3.

[784] Clarke/Knake, Cyberwar, 2010, S. 13 ff.

[785] Ebd., S. 12 f.

Kontroll-Rechner mit Standort im heutigen Russland hin. Darüber hinaus wird in Estland auf einen in Kyrillisch geschriebenen Computercode im Zusammenhang mit den Angriffen verwiesen. Die russische Regierung dementierte aber eine Beteiligung explizit.[786] Organisierte Kriminalitätsstrukturen sind zwar aufgrund des hohen Ressourcenbedarfs für einen Angriff dieser Größenordnung wahrscheinlich, der Ursprung und die mögliche Kombination der angreifenden Akteure ist aber nicht mit Sicherheit auszumachen und bleibt daher spekulativ.[787]

II.4.5 Vorhandene Regelungen und Maßnahmen zum Schutz vor Sabotage

Über die bereits in Kapitel II.2 zur Kriminalität im Internet aufgeführten Grundlagen hinaus sind hier einige sabotage-spezifische Regelungen und Maßnahmen hervorzuheben:

II.4.5.1 Internationale Regelungen und Maßnahmen

Wie schon in Kapitel II.2 zur Kriminalität im Internet ausgeführt, bedingt die Globalität des Internets erhebliche Anstrengungen in der internationalen Zusammenarbeit. Auf die dortigen Ausführungen sei auch an dieser Stelle verwiesen.[788] Darüber hinaus sind einige Aktivitäten auf EU-Ebene zu verzeichnen, die sich durch ihre Fokussierung auf Kritische Infrastrukturen letztlich auch mit dem Schutz vor Sabotageakten beschäftigen und bereits in Kapitel II.1 über den Schutz Kritischer Infrastruktur en im Internet dargelegt wurden.

II.4.5.2 Nationale Regelungen und Maßnahmen

II.4.5.2.1 Strafverfolgung

II.4.5.2.1.1 Einschlägige Normen

Speziell für den Bereich der Sabotage sind vor allem die folgenden strafrechtlichen Bestimmungen zu nennen, wobei entsprechend der Arbeitsdefinition die Computersabotage zur Internetkriminalität gerechnet[789] und daher hier nicht aufgeführt wird:

- § 87 StGB (Agententätigkeit zu Sabotagezwecken)[790],

---

[786] Clarke/Knake, Cyberwar, 2010, S. 15.

[787] Gaycken, Cyberwar, 2011, S. 170.

[788] S. Abschnitt II.2.3.1.

[789] Siehe dazu die Begründung in Kapitel II.4.1.

- § 88 StGB (Verfassungsfeindliche Sabotage),
- § 109e Absatz 1 StGB (Sabotagehandlungen an Verteidigungsmitteln)[791],
- § 109f StGB (Sicherheitsgefährdender Nachrichtendienst),
- § 317 StGB (Störung von Telekommunikationsanlagen)[792] sowie
- flankierende Bestimmungen (so genannte Vorfeldkriminalisierung):
  - § 91 StGB (Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat)[793],
  - § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten)[794].

II.4.5.2.1.2 Steuerungswirkung des Strafrechts

Strafrechtliche Normen entfalten zwar grundsätzlich eine Abschreckungswirkung (Generalprävention), doch kann dies allein insbesondere hinsichtlich Sabotage nicht genügen. Denn gerade hier werden Täter von vornherein entsprechende Sanktionen ins Kalkül ziehen, sodass Strafnormen zwar einen notwendigen, aber keinen hinreichenden Schutz vermitteln können. Erforderlich sind vielmehr zahlreiche flankierende Maßnahmen, sowohl in anderen Rechtsgebieten (Öffentliches Sicherheitsrecht, Zivilrecht) als auch politisch, wie etwa die Stärkung der Medienkompetenzen, um Sabotageakten präventiv entgegen zu treten.

Erforderlich sind organisatorische, aber auch weitere Maßnahmen, um Fehlerquellen im komplexen System „Mensch-IT“ zu beherrschen. Hierzu gehören sowohl technische Maßnahmen (Produktsicherheit) als auch organisatorische Kontrollen etc., um zu verhindern, dass Nutzer Sicherheitsmaßnahmen einfach umgehen (zum Beispiel Vergabe zu einfacher Passwörter). Menschliches Fehlverhalten muss dabei möglichst beim Design und den rechtlichen Anforderungen von IT-Anlagen und Infrastrukturen in Betracht gezogen und

---

[790] § 87 Absatz 2 StGB lautet: „Sabotagehandlungen im Sinne des Absatz 1 sind 1. Handlungen, die den Tatbestand der §§ 109e, [...] 317 [...] StGB verwirklichen, und 2. andere Handlungen, durch die der Betrieb eines für die Landesverteidigung, den Schutz der Zivilbevölkerung gegen Kriegsgefahren oder für die Gesamtwirtschaft wichtigen Unternehmens dadurch verhindert oder gestört wird, dass eine dem Betrieb dienende Sache zerstört, beschädigt, beseitigt, verändert oder unbrauchbar gemacht oder dass die für den Betrieb bestimmte Energie entzogen wird“.

[791] § 109e Absatz 1 StGB lautet: „Wer ein Wehrmittel oder eine Einrichtung oder Anlage, die ganz oder vorwiegend der Landesverteidigung oder dem Schutz der Zivilbevölkerung gegen Kriegsgefahren dient, unbefugt zerstört, beschädigt, verändert, unbrauchbar macht oder beseitigt und dadurch die Sicherheit der Bundesrepublik Deutschland, die Schlagkraft der Truppe oder Menschenleben gefährdet, wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft“.

[792] § 317 Absatz 1 StGB lautet: „Wer den Betrieb einer öffentlichen Zwecken dienenden Telekommunikationsanlage dadurch verhindert oder gefährdet, dass er eine dem Betrieb dienende Sache zerstört, beschädigt, beseitigt, verändert oder unbrauchbar macht oder die für den Betrieb bestimmte elektrische Kraft entzieht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft“.

[793] Gercke, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 27.

[794] Ebd., Rn. 17.

durch technische Sicherheitsvorkehrung eingegrenzt werden, wie der Fall des (simulierten) Angriffs durch die Firma Netragard verdeutlicht.[795]

II.4.5.2.1.3 Rechtsdurchsetzung

Wie schon allgemein für den Bereich der Kriminalität im Internet in Kapitel II.2 ausgeführt, gilt auch für die Sabotagebekämpfung, dass nicht nur materielle Regelungen, sondern auch deren Durchsetzung (englisch: enforcement) maßgeblich für die Bekämpfung von Sabotage ist.

Ähnlich wie in Bezug auf Spionageakte[796] ist auch hier anzumerken, dass sich nicht ausschließen lässt, dass es sich bei den Akteuren auf Täterseite um solche aus dem globalen politischen Bereich handelt. Dies verdeutlichen auch die oben genannten Spekulationen über Spionageakte staatlicher Herkunft.[797] Durch die Überlagerung der rein justiziellen Strafverfolgung durch politisch-diplomatische Erwägungen könnten etwaigen Strafverfolgungsmaßnahmen daher von vornherein gewisse Grenzen gesetzt sein.

II.4.5.2.2 Infrastrukturbezogene Regelungen

Hinsichtlich solcher Maßnahmen, die den Schutz durch die genannten strafrechtlichen Normen flankieren, besteht weitgehend Kongruenz zu den weiteren Bereichen der Kriminalität im Internet. Insofern ist auf die betreffenden Abschnitte zu verweisen.[798] Speziell in Bezug auf Sabotage sind jedoch insbesondere auf das Post- und Telekommunikationssicherstellungsgesetz (PTSG)[799] hinzuweisen, welches eine den §§ 108 ff. TKG[800] vergleichbare Stoßrichtung aufweist.

Anwendungsbereich des Post- und Telekommunikationssicherstellungsgesetz ist die Sicherstellung einer Mindestversorgung mit Postdienstleistungen oder Telekommunikationsdiensten im Falle von erheblichen Störungen wie Naturkatastrophen, schweren Unglücksfällen oder Sabotagehandlungen (§ 1 Absatz 2 PTSG). Die

---

[795] http://www.spiegel.de/netzwelt/web/0,1518,772462,00.html: Eine als Werbegeschenk getarnt infizierte USB-Maus hat einen Trojaner in das Unternehmensnetzwerk geschleust. Hier hätte etwa eine Ausdehnung der Sicherheitsscanner auf jegliche USB-Anschlüsse den Angriff womöglich verhindert.

[796] S. oben Abschnitt II.3.5.2.2.

[797] Siehe hierzu auch Kapitel II.3.3.3

[798] Siehe dazu die Kapitel II.2.3.3.2, II.2.3.3.3, II.2.3.3.4 sowie II.2.3.3.5.

[799] Gesetz zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten in besonderen Fällen vom 24. März 2011 (BGBl. I S. 506, 941).

[800] Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 1 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958).

Anwendungsbereiche von Post- und Telekommunikationssicherstellungsgesetz und Telekommunikationsgesetz überschneiden sich dahingehend, dass sie beide im Falle von (erheblichen) Störungen der Telekommunikationsnetze, -anlagen und -dienstleistungen Schutzvorkehrungen vorsehen:[801] Während § 109 Absatz 2 TKG eine Verpflichtung der Anbieter zur generellen Vorsorge gegen Störungen, Angriffe und Katastrophen ausspricht, erlegen §§ 2 und 5 PTSG den Post- beziehungsweise Telekommunikationsunternehmen die Pflicht auf, im Falle des Eintritts der in § 1 Absatz 2 PTSG genannten Szenarien bestimmte Dienstleistungen aufrecht zu erhalten. Dies verlangt zwangsläufig das Treffen von Vorsorgemaßnahmen, die mit solchen gemäß § 109 Absatz 2 TKG identisch sein können. Hinsichtlich des Anwendungsbereichs von § 109 TKG besteht im Verhältnis mit dem Post- und Telekommunikationssicherstellungsgesetz Streit.[802] Das Post- und Telekommunikationssicherstellungsgesetz ist gegenüber § 109 Absatz 2 TKG eine vorrangige Regelung (lex specialis).[803]

II.4.5.2.3 Initiativen

Der Bereich der IT-bezogenen Sabotage überschneidet sich in wesentlichen Teilen mit dem des Schutzes Kritischer Infrastrukturen. Dies hat den Hintergrund, dass sich nach der hier zugrunde gelegten Definition von Sabotage Angriffe gegen für die Sicherheit der Bundesrepublik Deutschland und die Gesamtwirtschaft bedeutsame wirtschaftliche, staatliche oder gesellschaftliche Rechtsgüter zu richten haben und die Beeinträchtigung dieser Güter auch mittelbar als Folge von oder Teil einer Kettenreaktion nach unmittelbar IT-bezogenen Angriffen eintreten kann. Für die Initiativen in diesem Bereich wird deshalb auf Kapitel II.1 zum Schutz Kritischer IT-Infrastrukturen verwiesen.

II.4.6 Defizitanalyse

Die Defizite betreffen sowohl die IT-Sicherheit im Allgemeinen als auch die für Sabotage hervorzuhebenden folgenden Besonderheiten:

Mit den technischen Gegebenheiten entwickeln sich zwangsläufig parallel auch die Angriffsmöglichkeiten auf IT-Systeme weiter, und dies in einem höheren Tempo als der

---

[801] Bock, in: Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 109 Rn. 12, 16.

[802] BITKOM, Stellungnahme zu BT-Drs. 15/2316; Bock, in: Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 109 Rn. 16.

[803] Scheurle/Mayen/Schommertz, TKG-Kommentar, 2. Aufl. 2008, Rn. 2; Bock, in: Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 109 Rn. 12; Spindler, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010, S. 92.

Gesetzgeber neue Gesetze entwickeln oder bestehende anpassen kann. Die insofern drohenden Gefahren sind kein Alleinstellungsmerkmal des Bereichs der Sabotage, sondern betreffen die gesamte IT-bezogene Kriminalität. Jedoch ist zu beachten, dass davon insbesondere groß angelegte Schutzmechanismen betroffen sind, wie sie beispielsweise die §§ 108 ff. TKG und das Post- und Telekommunikationssicherstellungsgesetz beschreiben.

II.4.7 Risikoeinschätzung

Für die Einschätzung der Risiken ist das Wissen über die relevanten Faktoren maßgeblich, die Sabotage begünstigen oder ihr auch entgegenstehen und schließlich der Grad und das potenzielle Ausmaß von Schäden. Eine Risikoanalyse ist hier nicht anders als bei anderen Technologien anhand folgender Kriterien durchzuführen (zum Beispiel im Industrieanlagenrecht):

- Bedrohte Akteure (Staat, Wirtschaft, Gesellschaft),
- Bedrohte Rechtsgüter,
- Wahrscheinlichkeit und Ausmaß des Schadens sowie eine
- Kosten-Nutzen-Abwägung.

Auszugehen ist bei der Einschätzung von der oben genannten Definition des Sabotagebegriffs. Das darin enthaltene Erheblichkeitskriterium engt auf der einen Seite den Kreis der relevanten schädlichen Handlungen ein, da nur Angriffe auf für die Bundesrepublik Deutschland und die Gesamtwirtschaft bedeutsame wirtschaftliche, staatliche oder gesellschaftliche Rechtsgüter erfasst werden. Auf der anderen Seite bedeutet dies aber auch, dass das Augenmerk nicht allein auf die unmittelbaren Angriffsziele und -folgen gerichtet werden darf, sondern gerade auch mittelbare Folgen in Betracht gezogen werden müssen. Dies gilt vor allem für die Fälle, in denen sich Angriffe gegen (Kritische) Infrastrukturen wenden, da diese qua definitionem kettenreaktionsartige Folgen nach sich ziehen.

Auf Seiten der unmittelbar bedrohten Rechtsgüter lässt sich zunächst die Integrität der Sachsubstanz möglicher Sabotageziele (IT-Systeme als solche, aber auch von diesen abhängige technische Anlagen, wie zum Beispiel Kraftwerke, Produktionsanlagen und Verkehrsinfrastruktur) ausmachen, ebenso wie die körperliche Unversehrtheit und das Leben potenzieller menschlicher Opfer. Auf Seiten der potenziell mittelbar betroffenen Rechtsgüter sind in jedem Fall auch wieder die körperliche Unversehrtheit und das Leben menschlicher Opfer zu nennen, aber nicht zuletzt, aufgrund der gesamtwirtschaftlichen Bedeutsamkeit der Angriffsziele, umfangreiche wirtschaftliche Rechtsgüter. Eine genauere Identifizierung ließe

sich am besten anhand konkreter Sabotage-Szenarien vornehmen, die die Dimensionen der Folgen näher beleuchten. Das Ausmaß der Risiken hängt auch von möglichen Gegenmaßnahmen und deren Effektivität ab. Zudem ist das Ergebnis einer Risikoeinschätzung in besonderem Maße von dem der Defizitanalyse abhängig und insofern nicht isoliert beurteilbar. Auch für diesen Bereich ergeben sich daher Forschungsdefizite. Die Erkenntnisgewinnung könnte sich dabei u. a. an bestimmten Sabotage-Szenarien orientieren, welche dann zugleich einer Wahrscheinlichkeitseinschätzung unterzogen werden könnten.[804]

Soweit bereits Erkenntnisse vorliegen, kann festgestellt werden, dass die Gefahr durch Terrorismus vermutlich gering ist. „Während es technisch möglich ist, Schäden mit Terrorwirkung zu verursachen, sind solche Angriffe stark voraussetzungsreich".[805] Die konspirative Organisation erschwert das Ansammeln der notwendigen Ressourcen.[806] Für die nahe oder mittlere Zukunft sieht das BSI keine Entwicklungen zu cyberterroristischen Gefahren im engeren Sinne.[807] Allerdings wird teilweise spekuliert, ob erfolgte Angriffe aus Sicherheitsgründen geheim gehalten wurden.[808] Es bleibt ebenso zu bedenken, dass terroristische Vereinigungen die notwendige Rechenkraft und Programmierleistung einkaufen könnten, ohne dass der Beauftragte das Ziel des Auftraggebers kennt.[809] Beschlagnahmte Al-Qaida-Rechner zeigen zudem, dass sich Terroristen zunehmend mit Internet-Technik auseinandersetzen.[810]

Sabotage, insbesondere Wirtschaftssabotage, könnte sich zu einem Geschäftsfeld der organisierten Kriminalität entwickeln. So könnten durch gezielte Sabotageakte Börsenkurse manipuliert und so Gewinne erzielt werden.[811] Für militärisch-nachrichtendienstliche Angreifer bietet die gezielte Wirtschaftsmanipulation die Möglichkeit, einem fremden Land erheblichen Schaden zuzufügen, ohne dass eine militärische Auseinandersetzung notwendig ist.

---

[804] In diese Richtung bereits Fischer, www.infrastrukturInternet-Cyberterror.Netzwerk – Analyse und Simulation strategischer Angriffe auf die kritische Infrastruktur Internet, 2007.

[805] Gaycken, Schriftliche Stellungnahme zu Expertengespräch „Sicherheit im Netz", S. 1.

[806] Ebda.

[807] Könen, Schriftliche Stellungnahme zu Expertengespräch „Sicherheit im Netz", Frage 2 a.E.

[808] Brunst, Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet, in: Wade/Maljevic, A War on Terror?, 2010, S. 52 f.

[809] Ebd., S. 70.

[810] Ebd.

[811] Gaycken, Schriftliche Stellungnahme zu Expertengespräch „Sicherheit im Netz", S. 2.

III. Handlungsempfehlungen

Handlungsempfehlungen

zum Kapitel „Zugang zum Internet und Infrastruktur des Internets“

Streitig gestellt von der Fraktion DIE LINKE.

Thema: Breitband

Um das gesellschaftliche und ökonomische Potenzial der Digitalisierung voll nutzen zu können, bedarf es einer hochleistungsfähigen Breitband-Infrastruktur. Die Enquete-Kommission weist darauf hin, dass der Ausbau beschleunigt werden muss. Eine gut ausgebaute digitale Infrastruktur ist unverzichtbar für eine moderne demokratische Gesellschaft und eine international wettbewerbsfähige Wirtschaft. Ein flächendeckender Breitbandausbau schafft die Voraussetzungen für die Teilhabe aller Bevölkerungsgruppen und Regionen am Fortschritt sowie an den Möglichkeiten der digitalen Gesellschaft. Die Zukunftsfähigkeit vieler Kommunen hängt maßgeblich von Standortfaktoren wie der Breitbandanbindung ab.

Mit der Vergabe nicht mehr für den Rundfunk benötigter Frequenzen („Digitale Dividende“) konnte die Versorgung des ländlichen Raums mit mobilem Breitband verbessert werden. Dies gelang, da die Nutzung der Frequenzen an die Auflage gebunden ist, zunächst in den unzureichend mit Breitband versorgten „weißen Flecken“ den neuen Mobilfunkstandard der vierten Generation, LTE, auf- und auszubauen. So steht heute bereits für über 99 Prozent aller deutschen Haushalte ein Breitbandanschluss von mindestens 1 Mbit/s zur Verfügung. Für über 48 Prozent ist sogar ein ultrabreitbandiger Anschluss von 50 Mbit/s gegeben.[812]

Neben dieser bisherigen Erfolge muss der Breitbandausbau weiter vorangetrieben werden. Die Attraktivität ländlicher Gewerbe- und Wohngebiete leidet unter mangelnder Anbindung an das Internet.

[812] Vgl. BMWi: Rösler: Ausbau des hochleistungsfähigen Internet geht zügig voran. Pressemitteilung vom 6. März 2012. Online abrufbar unter: http://www.zukunft-breitband.de/BBA/Navigation/Service/presse,did=479764.html .
sowie: Aktuelle Breitbandverfügbarkeit in Deutschland (Stand Ende 2011). Erhebung des TÜV Rheinland im Auftrag des BMWi. Ende 2011. Online abrufbar unter: http://www.zukunft-breitband.de/BBA/Redaktion/PDF/aktuelle-breitbandverfuegbarkeit-in-deutschland,property=pdf,bereich=bba,sprache=de,rwb=true.pdf

Ergänzungstext der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN :

In Deutschland sind noch immer viele Haushalte unterversorgt. Deutschland nimmt im europäischen Vergleich einen der mittleren Plätze bei der Breitbandversorgung ein. Auch beim Glasfaserausbau existiert in Deutschland ein gravierender Rückstand gegenüber anderen Industrienationen.

Das Ziel muss ein schnelles Internet für alle sein, auch in ländlichen Räumen. Eine digitale Spaltung muss vermieden beziehungsweise überwunden werden. Hierbei ist jedoch auch die Inanspruchnahme der zur Verfügung stehenden schnellen breitbandigen Anschlüsse (so genannte take-up-rate) durch die Kundinnen und Kunden entscheidend. Bisher kann noch keine wesentliche Steigerung bei der Nachfrage nach ultrabreitbandigen Anschlüssen verzeichnet werden.

Breitbandanwendungen ermöglichen zusätzliche wirtschaftliche Wachstumsimpulse. Schnelles Internet ist die Vorbedingung für Effizienzsteigerungen, Innovationen und neue Geschäftsmodelle mit erheblichem wirtschaftlichem Potenzial, insbesondere auch im Bereich des Mittelstands.

Die Arbeitswelt von heute und morgen ist immer mehr von der Digitalisierung geprägt. Der Zugang zum Internet und damit zu Wissen und Informationen entscheidet zunehmend über den wirtschaftlichen Erfolg von Unternehmen und die berufliche Perspektiven der Beschäftigten.

Die Verdichtung und Beschleunigung von Informationen durch das Internet, sei es in sozialen Netzwerken, Mediatheken oder anderen digitalen Informationsangeboten, ist von großer sozialer, kultureller und wirtschaftlicher Bedeutung. Eine flächendeckende hochwertige Breitbandinfrastruktur ist deshalb aus Sicht der Enquete-Kommission integraler Bestandteil einer zeitgemäßen Netzpolitik.

Das Internet mit seinen neuen Informations- und Kommunikationsmöglichkeiten eröffnet große Chancen für demokratische Meinungsbildungs- und Beteiligungsprozesse.

Zur Erreichung dieser Ziele empfiehlt die Enquete-Kommission dem Deutschen Bundestag:

– eine klare Wettbewerbsorientierung und innovations- und investitionsfreundliche Regulierung zu verfolgen,

– möglichst unbürokratische und kostenreduzierende Regulierungsansätze zu finden, die auf netzgebundene Märkte abgestimmt sind.

Open Access-Marktmodelle

Darüber hinaus regt die Enquete-Kommission an, Open Access-Marktmodelle rechtlich zu klären und praktisch umzusetzen, um innovative Geschäftsmodelle und effiziente technische Lösungen für den NGA-Ausbau zu unterstützen, bei der die Investitionsrisiken und -kosten möglichst breit über die Marktteilnehmer verteilt werden.

Weiterentwicklung staatlicher Förderprogramme zur Verbesserung der Breitbandversorgung

Die Enquete-Kommission empfiehlt mit Blick auf Wirtschaftlichkeitslücken im Breitbandausbau, unter Berücksichtigung der Mitnutzung von bestehenden Infrastrukturen staatliche Förderprogramme weiterzuentwickeln und aufeinander abzustimmen. Diese sollen im Einzelnen

- zusätzliche Impulse für den Breitbandausbau im ländlichen Raum geben;
- eine möglichst große Hebelwirkung für private Investitionen entfalten;
- konsequenter als bisher auf die Ziele Qualitätsentwicklung und Hochgeschwindigkeitsnetze orientiert werden;
- mit Hilfe von Zinsverbilligungen bei langjähriger Laufzeit zusätzliche Breitbandinvestitionen von Kommunen und Unternehmen stimulieren.

Der Breitbandausbau in Deutschland ist kontinuierlich zu beobachten und bereits durchgeführte Maßnahmen sind regelmäßig auf ihre Wirksamkeit hin zu evaluieren.

Investitions- und wettbewerbsfreundliche Regulierung als Voraussetzung eines marktgetriebenen Breitbandausbaus

Der marktgetriebene Breitbandausbau setzt Investitionssicherheit und wirtschaftliche Attraktivität für die Netzbetreiber voraus. Dies muss durch die Regulierung ebenso sichergestellt werden, wie effektiver Wettbewerb, der sowohl den Ausbau befördert, als auch für attraktive Endkundenprodukte sorgt. Dies gilt umso mehr, als verschiedene Marktstudien eine bislang nur gering ausgeprägte Bereitschaft der Kunden belegen, für leistungsfähige Anschlüsse auch mehr zu bezahlen. In einem solchem Marktumfeld müssen Ausbau- und damit Investitionsentscheidungen besonders sorgfältig auf ihre Wirtschaftlichkeit geprüft werden. Entscheidende Stellschraube für die Steigerung der Kundennachfrage sind aber insbesondere die über die Netze realisierten Dienste und Anwendungen. Ein Vorangehen der öffentlichen Hand in diesem Bereich, etwa durch einen verstärkten Einsatz von E-

Government-[813], E-Learning-[814] oder E-Health-Angeboten[815] kann daher zu einer steigenden Nachfrage nach Breitbanddiensten und damit von Hochgeschwindigkeitsanschlüssen führen.

Streitig gestellt von den Fraktionen BÜNDNIS 90/DIE GRÜNEN und DIE LINKE.

Vorrang von Marktlösungen beim Breitbandausbau

Mit Blick auf den flächendeckenden Ausbau können Marktlösungen bei Kooperationen und freiwillige Angebote Vorrang vor staatlichen Regulierungseingriffen haben. Sie sind zu unterstützen, solange sie letztendlich zu einer Öffnung für alle Marktteilnehmer führen. Wenn jedoch bestehende oder entstandene Monopole von einzelnen Unternehmen verteidigt werden, bedarf es einer regulierten Öffnung des Marktes durch die staatlichen Aufsichtsbehörden.

Hinsichtlich des Konzeptes eines Open Access, das auf den Prinzipien der Freiwilligkeit und Diskriminierungsfreiheit basiert, muss zwischen allen betroffenen Akteuren zunächst ein gemeinsames Grundverständnis hergestellt werden. Kern dieses Grundverständnisses sollte sein, dass Open Access letztlich zu weniger und nicht zu mehr Regulierung führen soll. Es entspricht beispielsweise nicht einer symmetrischen Regulierung. Gelingt hierüber eine wettbewerbliche Marktöffnung, besteht auch kein weiterer Bedarf mehr für Regulierungseingriffe.

Streitig gestellt von der Fraktion DIE LINKE.

Breitbandausbau im Technologiemix

Eine zeitnahe flächendeckende Versorgung mit leistungsfähigen Breitbandanschlüssen gelingt nur durch die Nutzung aller geeigneten Technologien wie Glasfaser, Kabel, Funk oder Satellit. Diese Mischung stärkt auch den aus Gründen der Wahlfreiheit und Vielfaltsicherung anzustrebenden Infrastrukturwettbewerb. Eine politische Priorisierung einer bestimmten Technologie würde den weiteren Breitbandausbau in dieser Vielfältigkeit gefährden.

---

[813] E-Government wird laut Duden bezeichnet als die „Durchführung von Prozessen, die zwischen staatlichen Institutionen oder zwischen staatlicher Institution und Bürger ablaufen, mithilfe der Informationstechnologie".

[814] E-Learning wird laut Duden bezeichnet als „computergestütztes Lernen, bei dem Schüler und Lehrer räumlich getrennt voneinander sind und vor allem über das Internet in Kontakt stehen".

[815] E-Health wird laut Duden bezeichnet als „Einsatz von Computern und Internet im Gesundheitswesen".

Ergänzende Handlungsempfehlungen der Fraktionen der SPD und BÜNDNIS 90/DIE GRÜNEN und der Sachverständigen Alvar Freude, Constanze Kurz, Prof. Dr. Wolfgang Schulz, Lothar Schröder und Cornelia Tausch

zum Kapitel „Zugang zum Internet und Infrastruktur des Internets“

Thema Breitband

Die Enquete-Kommission empfiehlt angesichts der herausragenden gesellschaftlichen Bedeutung der Breitbandversorgung in Deutschland dem Deutschen Bundestag, dafür einzutreten, dass

1. kurzfristig eine flächendeckende Grundversorgung mit schnellen Internetverbindungen realisiert und diese durch eine Universaldienstverpflichtung abgesichert wird. Zur Erfüllung der staatlichen Gewährleistungsverantwortung für die telekommunikative Grundversorgung (Artikel 87 Absatz 1 GG) sollte ein Breitband-Universaldienst mit einer zu Verfügung zu stellenden Bandbreite, die der Mehrheit der Nutzer zur Verfügung steht, implementiert werden. Dies sollte über eine wettbewerbs- und investitionsfreundliche Rahmenregulierung geschehen, um den Aufbau einer gemeinsamen, hochleistungsfähigen Infrastruktur zu beschleunigen. Die gesetzlich festzulegende Bandbreite sollte entsprechend den EU-Vorgaben ermittelt und gesetzlich verankert werden, damit derzeit mindestens die Nutzung klassischer Internetanwendungen bei zwei MBit/s für alle ermöglicht wird;

2. schnellstmöglich eine Qualitätsentwicklung mit Geschwindigkeiten von mindestens sechs MBit/s realisiert wird;

3. der schrittweise Ausbau von Hochgeschwindigkeitsnetzen vorangetrieben wird, die deutlich höhere Bandbreiten von 50 Mbit/s und mehr ermöglichen und auch den zukünftigen Anforderungen an eine moderne Breitbandinfrastruktur gerecht werden.

4. Weiterhin empfiehlt die Enquete-Kommission in regelmäßigen Abständen zu prüfen, welche Übertragungsgeschwindigkeiten der Mehrheit der Teilnehmer mit Internetanschluss mittlerweile zur Verfügung stehen und der Breitband-Universaldienst unter Berücksichtigung der Investitionssicherheit der ausbauenden Unternehmen durch den Gesetzgeber dementsprechend anzupassen. Die Finanzierung dieses Universaldienstes sollte über eine Fondslösung realisiert werden. Mittels eines Fonds wird die Finanzierung des Breitbandausbaus auf alle Telekommunikationsunternehmen ab einem relevanten Marktanteil entsprechend ihren Marktanteilen umgelegt.

5. Außerdem sollte der in Deutschland stockende, geografisch weit zerstreute Glasfaserausbau durch klare regulatorische Maßnahmen deutlich beschleunigt und gezielte Anreize für die Öffnung von Glasfasernetzen für andere Wettbewerber gesetzt werden. Leerrohre müssen bei Tiefbauarbeiten verpflichtend verlegt werden, der vorbildliche Open Access anderer Anbieter zu Glasfasernetzen finanziell gefördert und Synergieeffekte zwischen kommunalen Versorgungsunternehmen und Telekommunikationsanbietern genutzt werden. Hilfreich dabei ist die Erstellung eines Baustellenatlasses für relevante Tiefbauvorhaben, die einen Mehrwert für den Breitbandausbau mit sich bringen.

Zur Erreichung dieser Ziele empfiehlt die Enquete-Kommission dem Deutschen Bundestag

1. angesichts eines Marktes mit gewaltigen Investitionskosten und regional sehr unterschiedlichen Rahmenbedingungen die richtige Balance zwischen Wettbewerbs- und Investitionsförderung herzustellen;

2. alle Schritte auch mit Blick auf Planungs- und Rechtssicherheit aller Beteiligten durchzuführen;

3. die Bundesnetzagentur in die Lage zu versetzen, bei Diskriminierungen oder Marktmachtmissbrauch schnell einzugreifen;

4. durch gesetzliche Regelungen einheitliche und bessere Rahmenbedingungen zu schaffen, um alle sinnvollen Synergiepotenziale zu heben, damit die Verlege- und Aufbaukosten der Telekommunikationsunternehmen für moderne Breitbandnetze innerhalb und außerhalb der Häuser gesenkt werden können.

Investierende Unternehmen und Kommunen sind auf gute Informationen über vorhandene und geplante Infrastrukturen sowie Fördermöglichkeiten angewiesen.

Die Enquete-Kommission empfiehlt deshalb, die Informationserhebung und die Informationsangebote des Bundes und der Länder weiter zu verbessern. Die Kommunen müssen konsequenter in die Infrastrukturplanungen eingebunden werden.

Im Sinne einer besseren Abstimmung der unterschiedlichen Akteure empfiehlt die Enquete-Kommission dem Deutschen Bundestag,

1. die Bundesregierung anzuhalten, eine stärkere Koordinierungsfunktion als bisher wahrzunehmen und regelmäßig einen nationalen Breitbandgipfel mit Bund, Ländern, den kommunalen Spitzenverbänden sowie TK-Unternehmen durchzuführen.

2. die Bundesregierung anzuhalten, weitere etwaige Breitbandziele und Maßnahmen mit der Europäischer Kommission enger miteinander zu verzahnen, um deren Wirksamkeit sowie die Planungs- und Investitionssicherheit für Unternehmen zu erhöhen.

Die Gewährleistung von Netzneutralität ist mit Blick auf den Datentransfer im Internet von zentraler Bedeutung. Daher empfiehlt die Enquete-Kommission dem Deutschen Bundestag, dafür Sorge zu tragen, dass

1. die grundsätzliche Gleichbehandlung aller Datenpakete unabhängig von Inhalt, Dienst, Anwendung, Herkunft oder Ziel gewahrt bleibt;
2. der Charakter des Internets als freies und offenes Medium bewahrt und gestärkt wird. Jeglicher Form der Diskriminierung im Netz ist entschieden entgegenzutreten;
3. der faire Wettbewerb als Voraussetzung für eine dynamische Entwicklung des Internets und dort genutzter Dienste gewährleistet wird.

Ergänzende Handlungsempfehlungen der Fraktion DIE LINKE.

zum Kapitel „Zugang zum Internet und Infrastruktur des Internets“

Thema Breitband

Weil sich in vielen ländlichen Gebieten nicht genug Gewinn erwirtschaften lässt, bauen die Telekommunikations-Unternehmen die notwendige Infrastruktur nicht aus. Deshalb müssen immer noch über eine Million Menschen in Deutschland ohne schnellen Internetzugang leben. Während in Großstädten schon Internetanschlüsse mit einer Übertragungsgeschwindigkeit von 200 Megabit pro Sekunde (Mbit/s) angeboten werden, kriechen viele Dorfbewohner über ein Modem ins Internet.

Doch nicht nur die Grundversorgung ist ein Problem, auch der schnelle Ausbau der Glasfaser-Hochleistungsnetze muss in Schwung kommen. Glasfasernetze sind die Netze der Zukunft, denn Glasfaser ist das physikalisch schnellste Übertragungsmedium der Welt. Die Übertragungsgeschwindigkeit bleibt außerdem über lange Strecken erhalten und ist nicht störanfällig gegenüber elektromagnetischen Feldern. Daher bedarf es klarer Weichenstellungen für den Glasfaserausbau. Das Ziel der Bundesregierung, bis 2014 drei Viertel der Haushalte mit Übertragungsraten von mindestens 50 Mbit/s zu versorgen, greift jedoch zu kurz. Diese Geschwindigkeit ist mit dem herkömmlichen kupferkabelbasierten VDSL zu erreichen. Außerdem genügt zum Erreichen dieser Quote der Ausbau in dicht besiedelten Gebieten. Das vertieft die Digitale Spaltung zwischen Stadt und Land weiter.

Die Enquetekommission empfiehlt,

- Breitband-Anschlüsse als Universaldienstleistung gesetzlich festschreiben, damit jeder einen gesetzlichen Anspruch auf schnelles Internet hat. Die zu gewährende Mindestbandbreite sollte sich dabei nach den von der Mehrzahl der Teilnehmern vorherrschend verwendeten Technologien richten. Gegenwärtig wäre das ein Breitbandanschluss mit 6 Mbit/s Übertragungsgeschwindigkeit.
- die Anforderung an die Mindestübertragungsgeschwindigkeit im Rahmen einer Universaldienstleistung dynamisch zu konkretisieren, so dass das Mindestangebot in regelmäßigen Abständen überprüft und den aktuellen Entwicklungen angepasst werden muss. Bei den Anforderungen an ein Mindestangebot müssen neben der Bandbreite (Download und Upload) auch qualitative Merkmale wie Latenz und Verfügbarkeit berücksichtigt werden.

– dass die Bundesregierung sich auf der Ebene der EU für die unverzügliche Einbeziehung von Breitband-Internet in den EU-Universaldienstkatalog einsetzt.

Handlungsempfehlungen zum Kapitel „Zugang zum Internet und Infrastruktur des Internets“

Empfehlungen hinsichtlich der Einführung des Internetprotokolls in der Version 6 (IPv6)

Streitig gestellt von der Fraktion DIE LINKE.

Sensibilisierung der Endnutzer[816]

Die Enquete-Kommission empfiehlt der Bundesregierung und der deutschen Wirtschaft bei der Einführung des neuen Standards IPv6, die Bürgerinnen und Bürger ausführlich über die technischen Folgen und Neuerungen des Standards zu informieren. Ihnen sollte die Wahl gelassen werden, ob sie anhand ihrer IP-Adresse von Diensteanbietern (beispielsweise Betreibern beliebiger Webseiten) bei erneuter Nutzung eines Angebotes wiedererkannt werden können (statische IP-Adresse) oder ob dies aufgrund einer beispielsweise täglich wechselnden IP-Adresse nicht möglich sein soll. Die Entscheidung darüber, welche technische Variante letztlich zur Anwendung kommen sollte, sollte immer beim Endnutzer liegen.

Streitig gestellt von den Fraktionen der SPD und DIE LINKE.

Stiftung Datenschutz

Die Enquete-Kommission begrüßt die von der Bundesregierung gegründete Stiftung Datenschutz. Sie kann durch die Aufklärung der Bürgerinnen und Bürger, aber auch der Unternehmen und durch die Entwicklung eines Datenschutzaudits und eines Datenschutzauditverfahrens zur Prüfung von Produkten und Dienstleistungen auf ihre Datenschutzfreundlichkeit (zum Beispiel im Rahmen der Einführung von IPv6) einen wesentlichen Beitrag zu mehr Datenschutz und auch zu mehr Datensicherheit in Deutschland leisten.

[816] Siehe hierzu auch die gemeinsamen Leitlinien „IPv6 und Datenschutz“ des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, und des Deutschen IPv6-Rates. Online abrufbar unter: http://www.ipv6council.de/documents/leitlinien_ipv6_und_datenschutz.html

Ergänzende Handlungsempfehlungen der Fraktionen der SPD, BÜNDNIS 90/DIE GRÜNEN und der Sachverständigen Alvar Freude, Constanze Kurz, Prof. Dr. Wolfgang Schulz, Lothar Schröder und Cornelia Tausch

zum Kapitel „Zugang zum Internet und Infrastruktur des Internets“

Empfehlungen hinsichtlich der Einführung des Internetprotokolls in der Version 6 (IPv6)

Die nach dem neuen Internetprotokoll IPv6 vergebenen Internetadressen haben das Potenzial, zu Personenkennzeichen für jeden Internetnutzer zu werden und zwar unabhängig davon, wie viele Geräte der Einzelne im Internet verwendet. Umso wichtiger ist es, dass bei der Umsetzung des neuen Standards mit der notwendigen Sorgfalt vorgegangen und der Datenschutz berücksichtigt wird.

Vor diesem Hintergrund empfiehlt die Enquete-Kommission Internet und digitale Gesellschaft:

1. Bei der Umsetzung ist den Empfehlungen des Deutschen IPv6-Rats und den Entschließungen nationaler und internationaler Datenschutzkonferenzen zum Schutz der Privatsphäre bei IPv6 Rechnung zu tragen.
2. Ebenfalls ist dafür Sorge zu tragen, dass die Datenschutzbeauftragten über die nötigen Mittel verfügen, um eine datenschutzgerechte Ausgestaltung und Implementierung von IPv6 sicherzustellen.
3. Internet-Service-Provider sind darauf zu verpflichten, im Rahmen der Umsetzung von IPv6 verbindlich vorzugebende Datenschutz- und Sicherheitsvorschriften umzusetzen.
4. Die Endnutzer sollten von den Internet-Service-Providern in allgemein verständlicher Weise über die Möglichkeiten anonymer und pseudonymer Nutzung von IPv6-Diensten aufgeklärt werden. Insbesondere sollte ihnen die Wahl gelassen werden, ob sie anhand ihrer IP-Adresse von Diensteanbietern (beispielsweise Betreibern beliebiger Webseiten) bei erneuter Nutzung eines Angebotes wiedererkannt werden können (statische IP-Adresse) oder ob dies aufgrund einer beispielsweise täglich wechselnden IP-Adresse nicht möglich sein soll.
5. Endkunden sollten daher die Wahl zwischen festen und dynamischen IPv6-Adress-Präfixen (Adressbereichen) haben. Dynamische und statische Adressen sollten aus dem gleichen Adressbereich vergeben werden, damit für Dritte nicht ohne Weiteres ersichtlich

ist, ob eine Adresse dynamisch oder statisch ist, ob ein Nutzer also anhand der IP-Adresse wiedererkannt werden kann. Die Anbieter sollten verpflichtet werden, ihren Kunden beide Optionen einräumen, zumindest aber ohne zustätzliche Kosten die Möglichkeit einer dynamischen anstelle einer statischen Zuteilung von Präfixen anzubieten. Da der Adressraum bei IPv6 groß genug ist, wäre es auch möglich, auf Wunsch sowohl einen statischen als auch einen dynamischen Präfix zu vergeben.

6. Gerätehersteller sollten die Privacy Extensions nach RFC 4941 bei Endkunden-Systemen standardmäßig aktivieren. Der Gesetzgeber wird aufgefordert, diese Entwicklung aufmerksam zu beobachten und diese Verpflichtung gegebenenfalls auch gesetzlich zu verankern.

Ergänzende Handlungsempfehlungen der Fraktion DIE LINKE.

zum Kapitel „Zugang zum Internet und Infrastruktur des Internets“

Empfehlungen hinsichtlich der Einführung des Internetprotokolls in der Version 6 (IPv6)

Die Enquetekommission empfiehlt:

- gesetzgeberisch dafür Sorge zu tragen, dass die Datenschutzbeauftragten über die nötigen Mittel verfügen, um eine datenschutzgerechte Ausgestaltung und Implementierung von IPv6 sicherzustellen
- Internet-Service-Provider sind darauf zu verpflichten, im Rahmen der Umsetzung von IPv6 verbindlich vorzugebende Datenschutz- und Sicherheitsvorschriften umzusetzen
- Die Endnutzer sollten von den Internet-Service-Providern in allgemeinverständlicher Weise über die Möglichkeiten anonymer und pseudonymer Nutzung von IPv6-Diensten aufgeklärt werden. Insbesondere sollte ihnen die Wahl gelassen werden, ob sie im Rahmen ihrer Internetnutzung anonym bleiben oder identifizierbar sein möchten.
- Um Rechtsunsicherheit zu vermeiden, sollte im Rahmen einer gesetzlichen Norm zweifelsfrei festgeschrieben werden, dass es sich bei IP-Adressen um personenbezogene Daten handelt.
- Es sollte eine Regelung geben, die Anbieter dazu verpflichtet, dem Kunden ohne Aufpreis die Möglichkeit einer dynamischen anstelle einer statischen Zuteilung von Präfixen anzubieten. Es ist derzeit nicht absehbar, dass einem solchen Wunsch auf rein marktwirtschaftlicher Basis entsprochen werden wird.
- Anbieter sollten verpflichtet werden, ihren Kunden die Möglichkeit einzuräumen, ein anonymisierendes Netzwerk (Multi-hop-Proxy-Routing) zu betreiben.
- Im Sinne einer größtmöglichen Privacy by default sollten Anbieter verpflichtet werden, die im Rahmen von IPv6 möglichen Privacy Extensions in allen Endnutzergeräten standardmäßig zu aktivieren, damit ungewünschte Identifizierung und Profilbildung erschwert werden. Geräte, die diese Anforderung nicht erfüllen, sollten auf dem deutschen Markt nicht zugelassen werden.
- Um die im Telekommunikationsgesetz ausdrücklich vorgesehene Möglichkeit der anonymen Nutzung nicht zu unterlaufen, sollten die Hersteller darauf verpflichtet werden, nur solche Endgeräte auf den Markt zu bringen, die dem Kunden die freie Wahl zwischen anonymer oder identifizierbarer Netznutzung lassen. Die jeweilige Option sollte einfach

und leicht wählbar sein, etwa durch einen leicht zugänglichen Button. Die Grundeinstellung sollte verpflichtend ein anonymes Surfen vorsehen.

– Die Hersteller sollten dazu verpflichtet werden, regelmäßig Updates zur Verfügung zu stellen. Interessierten Kunden sollte dabei stets auch die Möglichkeit eingeräumt werden, die Wartung des eigenen Geräts selbst vorzunehmen.

Handlungsempfehlungen zum Kapitel „Schutz kritischer Infrastrukturen im Internet“

Nur Staat, Wirtschaft und Gesellschaft gemeinsam können einen ausreichenden Schutz der Kritischen Infrastrukturen gewährleisten. „Ein ausdrücklicher Verfassungsauftrag für die Sicherung kritischer Infrastrukturen fehlt im Grundgesetz. Ein Sicherungsauftrag folgt jedoch aus der staatlichen Pflicht, sich schützend vor die Grundrechte zu stellen und diese auch vor Angriffen Privater – etwa Terroristen – und sonstigen Gefahren zu schützen.“ [817] Darüber hinaus ist der Staat grundgesetzlich zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung verpflichtet.

Die meisten Kritischen Infrastrukturen sind in privater Hand. Daraus folgt eine besonders wichtige Rolle für die Privatwirtschaft. Es ist eine gesellschaftliche Aufgabe, die Bürgerinnen und Bürger für die Tatsache zu sensibilisieren, dass sie privat und beruflich (wiederum als Teil von Wirtschaft und Behörden) zentrale Mitgestalter der IT-Sicherheit sind.

Das Sicherheitsniveau der Kritischen Infrastrukturen kann entweder allgemein betrachtet werden, im Hinblick auf die sicherheitspolitische Lage (siehe Kapitel II.1.2) oder für jeden spezifischen Sektor, dann hinsichtlich der Art der Infrastruktur und ihrer Kritikalität. Eine detaillierte Analyse jedes Sektors ist im Rahmen der Arbeit der Projektgruppe nicht möglich, deshalb werden an dieser Stelle allgemeine Schutzmaßnahmen vorgeschlagen. Die Gesamtlage zu betrachten ist bei kritischen Infrastrukturen besonders wichtig, da es oft nicht um einzelne Anlagen, sondern um das Zusammenspiel verschiedener Branchen geht.

Auf nationaler, europäischer und internationaler Ebene existieren bereits eine Vielzahl von unterschiedlichen Maßnahmen. Die Maßnahmen lassen sich dabei in verschiedene Handlungsfelder wie beispielsweise zur Prävention und Abwehrbereitschaft, zum Erkennen und zur Reaktion, zur Folgeminderung und Wiederherstellung sowie zur Nachhaltigkeit unterteilen. Eine weitere Unterscheidung der Maßnahmen kann nach ihrer Art und Weise vorgenommen werden (zum Beispiel personell, technisch, organisatorisch, gesetzgeberisch und wissenschaftlich).

1. Empfehlungen an die Gesellschaft

Stärkere Konzentration auf Prävention bedeutet an erster Stelle die Kompetenz („Faktor Mensch“) in Gesellschaft, Wirtschaft und Staat zu verbessern. Die Enquete-Kommission empfiehlt Bund und Ländern, gegebenenfalls gemeinsam mit der Wirtschaft, mehr und besser

[817] „Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen“, BSI 2005

ausgestattete interdisziplinäre Lehrstühle für IT-Sicherheit an deutschen Universitäten schaffen.

IT-Sicherheit soll bei Schaffung und Ausgestaltung neuer und bestehender Berufsbilder in entsprechenden Berufsfeldern stärker beachtet werden. IT-Sicherheit muss raus aus den Fachgremien und in die Öffentlichkeit. Der mündige und kompetente Bürger kann durch mehr Selbstschutz sehr viel Schaden verhindern. Hier leisten das BSI mit seiner Website „BSI für Bürger“, die Verbraucherzentralen sowie gemeinsame Initiativen von Staat und IT-Wirtschaft wie „Deutschland sicher im Netz“ oder die Anti-Botnetz-Initiative bereits wertvolle Beiträge. Diese sollten daher weiter ausgebaut werden.

Notwendig ist auch die Stärkung der Sensibilität für die Datensicherheit. Unter der Prämisse der Datensparsamkeit sollten persönliche Daten erst gar nicht an Dritte, insbesondere im Internet, weitergegeben werden, sodass sie nicht kompromittiert oder missbraucht werden können. Die Enquete-Kommission empfiehlt der Bundesregierung zu prüfen, ob und inwieweit Einwirkungsmöglichkeiten bestehen, das Thema „sicheres Internet“ bei der Ausbildung von Medienkompetenz bereits in den Schulalltag zu integrieren. Hinsichtlich der Umsetzung, Ausführung etc. wird auf die Handlungsempfehlungen und weitergehenden Leitfragen der Projektgruppe Medienkompentenz[818] verwiesen.

2. Empfehlungen an die Wirtschaft

Die Enquete-Kommission betont, dass insbesondere die Sensibilisierung von Betreibern Kritischer Infrastrukturen für Gefahren und Maßnahmen besonders wichtig ist.

Die Enquete-Kommission begrüßt daher die im Jahr 2012 durchgeführten Fachgespräche zum IT-Schutz Kritischer Infrastrukturen durch das Bundesministerium des Innern. Sie haben dazu beigetragen, dass auf geschäftsführender Ebene bei Unternehmen und Verbänden das Bewusstsein für notwendige Sicherheitsmaßnahmen geschaffen und weiter geschärft wurde.

Alternativtext der Fraktion der SPD

Die Enquete-Kommission begrüßt, dass das Bundesministerium mit den im Jahr 2012 durchgeführten Fachgesprächen zum IT-Schutz Kritischer Infrastrukturen einen ersten Schritt

[818] Siehe hierzu Kapitel 5 und 6 des zweiten Zwischenberichts der Enquete-Kommission Internet und digtale Gesellschaft. Medienkompetenz. BT-Drucksache 17/7286. 21. Oktober 2011. Online abrufbar unter: http://dipbt.bundestag.de/dip21/btd/17/072/1707286.pdf

getan hat, , um auf geschäftsführender Ebene bei Unternehmen und Verbänden das Bewusstsein für notwendige Sicherheitsmaßnahmen zu schaffen und zu schärfen.

Auf geschäftsführender Ebene müssen die notwendigen Sicherheitsmaßnahmen eingesetzt und unterstützt werden.

Die Enquete-Kommission weist auf die Bedeutung von IT-Sicherheits-Schulungen für Mitarbeiter bei der Risikominimierung, gerade im Bereich von kleinen und mittleren Unternehmen (KMU) hin. Investitionen in die Mitarbeiterkompetenz lohnen sich für Unternehmen, weil durch sie schwere Schäden vermieden werden können. „Endnutzer Bildung“ nützt der Einzelperson und gleichzeitig dem ganzen Unternehmen. Auch ein an der Kompetenz der Mitarbeiter orientiertes Führungsmanagement leistet einen wichtigen Beitrag. Die Tarifpartner sollten darauf hinwirken, ausgebildete IT-Administratoren als hoch spezialisierte Fachkräfte einzuordnen und adäquat zu bezahlen.

Die Enquete-Kommission regt an, dass alle Unternehmen einen Ansprechpartner benennen, der für die IT-Sicherheit verantwortlich ist. Derzeit verfügt gerade bei den KMU nur jedes zweite Unternehmen über einen entsprechenden Ansprechpartner. Auch die unternehmensinternen Abstimmungsabläufe und Verantwortlichkeiten sind noch verbesserungsfähig. Hier wäre Sensibilität dafür zu schaffen, dass in allen Unternehmen klare Verantwortlichkeiten und eindeutige Abstimmungsabläufe zwischen IT-Verantwortlichen und Geschäftsführung erforderlich sind. Die Enquete-Kommission unterstützt die Maßnahmen der Bundesregierung in diesem Bereich, die u. a. eine Beratung von Unternehmen durch das BSI beinhalten. Diese ist fortzuführen und in Zusammenarbeitzum Beispiel mit den Kammern auszubauen.

Die Enquete-Kommission regt darüber hinaus an, die Zusammenarbeit mit der Task Force IT-Sicherheit des BMWi als zentralem Ansprechpartner und Impulsgeber für den Mittelstand zu stärken.

a) Rolle von Internet- und TK-Providern

Die Enquete-Kommission weist darauf hin, dass Providern für die „Querschnittsinfrastruktur“ Internet eine besondere Rolle und Bedeutung bei der Mitwirkung zur Aufklärung von Beeinträchtigungen und Angriffen zukommt.

Aus Sicht der Enquete-Kommission sollten die Provider daher insbesondere im eigenen Interesse generierte Erkenntnisse über aktuelle Internetsicherheitsentwicklungen schnell an die zuständigen Behörden (zum Beispiel das BSI) weitergeben (Frühwarnungen). Sie sollten

auch entsprechend der Vorgaben des Telekommunikationsgesetzes Maßnahmen zum Schutz vor unerlaubten Eingriffen in die Infrastruktur ergreifen und über erhebliche Störungen der Verfügbarkeit unverzüglich informieren.

b) Bereitstellung von Information für die Nutzerinnen und Nutzer über bekannte Schadprogramme und Verfügbarkeit von Sicherheitswerkzeugen

Schon heute stehen den Nutzerinnen und Nutzern zahlreiche Informationsmöglichkeiten über Sicherheitsgefahren und Schadprogramme zur Verfügung, die teils auf Initiative staatlicher Institutionen, teils von Unternehmen beruhen (zum Beispiel BSI für Bürger, Deutschland sicher im Netz, Anti-Botnetzinitiative). Kooperationen zwischen privaten und öffentlichen Stellen in diesem Bereich sollten aus Sicht der Enquete-Kommission weiter fortgeführt und ausgebaut werden, um möglichst hohe Standards in Bezug auf Qualität, Aktualität und auch Verständlichkeit der Information zu erreichen. Die bereitgehaltenen Informationen sollen die Nutzer in die Lage versetzen, selbst Maßnahmen gegen Schadsoftware zu ergreifen. Ergänzend sollte sichergestellt werden, dass den Nutzern einfach bedienbare Sicherheitswerkzeuge zur Verfügung stehen.

c) Rolle von Anbietern von Telemediendiensten

Die Enquete-Kommission empfiehlt auch gewerblichen Telemediendiensteanbietern, der IT-Sicherheit ein größeres Maß an Bedeutung beizumessen. Auch deren Angebote werden ausgenutzt, um Schadprogramme zu verbreiten. Sie sollten daher prüfen, ob sie nicht durch die Einrichtung von anerkannten Schutzmaßnahmen in ihren Diensten, ebenfalls einen Beitrag für mehr IT-Sicherheit leisten können. Ein entsprechendes, effektives Handeln würde zu mehr Vertrauen in die angebotenen Leistungen bei den betroffenen Nutzerinnen und Nutzern führen. Ein mögliches Einschreiten des Gesetzgebers wäre dann entbehrlich.

3. Zusammenarbeit zwischen Staat und Wirtschaft im Bereich der IT-Sicherheit

Die Enquete-Kommission Internet und digitale Gesellschaft empfiehlt dem Deutschen Bundestag, die Bundesregierung aufzufordern, eine umfassende Bestandsaufnahme der Kritischen digitalen Infrastruktur vorzulegen und hierbei neben den technischen Fragestellungen insbesondere auch die intersektorielle Abhängigkeit von Anbietern proprietärer Systeme zu untersuchen.

Behörden sind ebenfalls Kritische Infrastrukturen. Sie müssen deshalb ihre Systeme technisch nach dem Stand der Wissenschaft sichern und ihre Mitarbeiter angemessen schulen. Die Enquete-Kommission regt an, die IT-Kompetenz der Sicherheitsbehörden in Bund und

Ländern fortlaufend zu verbessern, um so sicherzustellen, dass geltendes Recht durchgesetzt und umgesetzt werden kann.

Streitig gestellt von der Fraktion DIE LINKE.

a) Stärkere Berücksichtigung der Wirtschaft bei der Cybersicherheitsstrategie

Die Enquete-Kommission empfiehlt, die *Cybersicherheitsstrategie der Bundesregierung* konsequent weiterzuverfolgen. Dabei sollte die Wirtschaft stärker in strategische Überlegungen und Strukturen einbezogen werden, weil insbesondere auch internationales Know-how der Unternehmen für die Gewährleistung der Sicherheit unerlässlich ist. Das bedeutet, dass beide Seiten, also BSI und Unternehmen, verstärkt zusammenarbeiten müssen. So genannte Single Points of Contact (SPOC) in Unternehmen und Verbänden sollten weiter etabliert werden.

Streitig gestellt von den Fraktionen der SPD, BÜNDNIS 90/DIE GRÜNEN und DIE LINKE.

b) Rolle von CERTs und Zusammenarbeit mit dem BSI

Die Enquete-Kommission stellt fest, dass Deutschland mit dem Deutschen CERT-Verbund (Computer Emergency Response Teams) eine national gut vernetzte CERT-Community besitzt. Das BSI ist auch international in Europa mit RegierungsCERTs und auf globaler Ebene sehr gut vernetzt, sodass ein kontinuierlicher Informationsaustausch gegeben ist.

Darüber hinaus steht das BSI mit den großen Software-Herstellern und Antivirensoftwareherstellern im intensiven Dialog. Informationen zu Angriffen und Schwachstellen, die das BSI auf diesen und anderen Wegen erreichen, werden über die Initiativen des UP KRITIS, der Allianz für Cybersicherheit und des Bürger-CERT, den in den jeweiligen organisierten Unternehmen oder auch der Öffentlichkeit in Form von Warnmeldungen zur Verfügung gestellt.

Streitig gestellt von der Fraktion der SPD

c) Verbesserung des Lagebilds zur Cybersicherheit am Standort Deutschland

Das Nationale Cyberabwehrzentrum fasst, in Zusammenarbeit mit dem 24-Stunden Lagezentrum, die Erkenntnisse verschiedener Sicherheitsbehörden zusammen und kann bei konkreten Vorfällen schnell ein ganzheitliches Lagebild aus Behördensicht entwickeln.

Die Enquete-Kommission hat festgestellt, dass viele Internet-Service-Provider auf Basis eigener Sicherungsmaßnahmen einen wichtigen eigenen Beitrag bei der Abwehr beziehungsweise Eingrenzung von Cyber-Attacken wahrnehmen.

Sie bedauert aber, dass bisher noch nicht alle Unternehmen an diesem Austausch teilnehmen und daher nur teilweise auf Informationen aus der Wirtschaft zurückgegriffen werden kann.

Schließlich steht über die Allianz für Cyber-Sicherheit grundsätzlich allen deutschen Unternehmen der Zugang zu Warnmeldungen des BSI offen. Nur ein gegenseitiger Informationsaustausch kann auch zu einer Verbesserung der Informationsbasis führen.

Nur anhand eines vollständigen und aktuellen Lagebildes ist es möglich, vorhandene Zusammenhänge zwischen IT-Attacken auf verschiedene Infrastrukturen aufzudecken und die richtigen Bewertungen, Handlungsoptionen und gegebenenfalls Abwehrmaßnahmen abzuleiten.

Auch können nur dann die staatlichen Sicherheitsbehörden ihrem gesetzlichen Auftrag hinsichtlich der Sicherstellung der öffentlichen und staatlichen Sicherheit vollumfänglich nachkommen, wenn Informationen über schadensauslösende oder gefährdende IT-Angriffe vorliegen.

Im Interesse einer noch effizienteren Gefahrenabwehr empfiehlt die Enquete-Kommission, Strukturen zu schaffen, die unter Wahrung von Vertraulichkeit einen stärkeren Austausch über konkrete Sicherheitsbedrohungen, Abwehrmaßnahmen und Erfahrungen zwischen Providern und staatlichen Stellen ermöglichen. Dabei sollten auch Betreiber anderer Kritischer Infrastrukturen eingebunden werden. Staatlichen Stellen kann eine wichtige Rolle als Ermöglicher und Moderator eines solchen Austauschs zukommen, der die tatsächlichen Bedürfnisse der Unternehmen berücksichtigen kann.

Die Enquete-Kommission bittet die Bundesregierung zu prüfen, ob eine gesetzliche Verpflichtung von Betreibern Kritischer Infrastrukturen in diesem Zusammenhang erforderlich ist.

Streitig gestellt von den Fraktionen der SPD und DIE LINKE.

d) Beidseitiger Austausch von Informationen

Es ist sicherzustellen, dass jedem Unternehmen ein nachvollziehbarer Meldeweg eines sicherheitsrelevanten Ereignisses zur Verfügung steht. Dieser Meldeweg sollte immer auch Vertraulichkeit und auf Wunsch auch Anonymität gewährleisten.

In einem weiteren Schritt müssen die eingegangenen Informationen zusammengestellt und in einer Form aufbereitet werden, sodass auch eine qualitativ hochwertige Information an die Wirtschaft zeitnah über mögliche Gefährdungen und Risiken übermittelt werden kann. Dies muss aus Sicht der Enquete-Kommission flächendeckend und nicht nur punktuell erfolgen. Ein schneller Informationsfluss zwischen Bund und Ländern stellt die Grundlage dafür dar.

Es sollte auch auf bestehende regionale Partnerschaften zwischen der Wirtschaft und den Sicherheitsbehörden zurückgegriffen werden. Cybersicherheit wurde in diesem institutionalisierten Austausch bisher zwar nur in Einzelfällen berücksichtigt. Aufgrund der gestiegenen Bedeutung von Cybersicherheit für die Gesamtwirtschaft sollte der Austausch hierzu jedoch intensiviert werden. Hierbei ist vor allem auf eine verbesserte Transparenz zum Zweck der Kontrolle und Nachvollziehbarkeit zu achten. Auch die Task Force „IT-Sicherheit in der Wirtschaft“ des BMWi sollte hier mit einbezogen werden.

Aus Sicht der Enquete-Kommission wird der bessere Informationsaustausch die Beurteilung der IT-Sicherheitslage verbessern und nicht nur bei der Prävention helfen, sondern auch die Reaktionsfähigkeit stärken. Wichtig ist dabei, dass das Cyberabwehrzentrum einen reinen Informationsaustausch anbietet, keine neuen Kompetenzen verteilt und das Trennungsgebot für Polizeien, Bundeswehr und Geheimdienste eingehalten bleibt.

e) Gesetzliche Verankerung des IT-Grundschutzes des BSI als Standard für die öffentliche Verwaltung

Die bisherige Grundlage für einen standardisierten IT-Grundschutz stellt zwar ein Beschluss[819] des Bundeskabinetts dar. Hierdurch werden jedoch unabhängige Institutionen (wie zum Beispiel der BfDI oder aber die Bundesbank) nicht verpflichtet. Eine gesetzliche Regelung könnte dies beseitigen. Auch könnte diese sicherstellen, dass auch in Zukunft der

[819] Beschluss der Bundesregierung zur Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung vom 16. Januar 2002. Online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/kab160102_pdf.pdf?__blob=publicationFile

Staat seiner Verantwortung für das Thema IT-Sicherheit nachkommen wird. Eine gesetzliche Regelung könnte festlegen, welche Schutzniveaus jeweils erreicht werden müssen und entsprechende Standards definieren. Darüber hinaus sollte ein verpflichtendes Minimalpaket auf Basis des Standards definiert werden. Da die bisherigen Anweisungen und Prüfmaßnahmen im Standard nur zu einem sehr kleinen Teil, und dann nur implizit, den Umgang mit Cloud-Diensten behandeln, ist durch die Bundesregierung eine mögliche Fortschreibung des Standards „IT-Grundschutz“ zu prüfen.

Die Enquete-Kommission empfiehlt darüber hinaus der Bundesregierung und dem Deutschen Bundestag sicherzustellen, dass das BSI aufgrund der zunehmenden Bedeutung des Themas Cybersicherheit mit ausreichenden Mitteln ausgestattet ist.

4. Sicherstellung des technischen Schutzes

a) Grundschutz

Bei Cyberangriffen sind Angreifer, Ziel und Motivation am Anfang oft schwer zu erkennen. Deswegen sind Abschreckungsmaßnahmen nicht sehr effektiv und es ist besser, die Widerstandsfähigkeiten den Kritischen Infrastrukturen zu verstärken, um ein robustes System zu sichern.[820]

Dies bedeutet zuerst, durch hohe Standards in den Kritischen Infrastrukturen ein grundsätzlich hohes IT-Sicherheitsniveau zu gewährleisten. Diese Standards sollen auf System-/Architekturebene stattfinden, damit zum Beispiel Isolierungen dafür sorgen können, dass Viren sich nicht überall ausbreiten. Aus Sicht der Enquete-Kommission sollen die Standards gemeinsam mit Wirtschaft, Wissenschaft und öffentlicher Verwaltung in Gremien wie der Koordinierungsstelle IT-Sicherheit (KITS) des Deutschen Instituts für Normung e.V. (DIN) und möglichst international entwickelt werden. Standards sind besonders wichtig für Verfahren und Methoden, weil die Produktzyklen immer kürzer werden. Sie sollten möglichst in den Produktentwicklungsprozess implementiert werden.

Software und Hardware sollten bereits von Anfang an möglichst sicher entwickelt werden. Insbesondere Hardwaredefekte sind oft schwierig festzustellen und können dann zu einem späteren Zeitpunkt durch eine Fernsteuerung ausgenutzt werden. Das System ist in einem solchen Fall auch nicht schnell wiederherstellbar.

[820] OECD „Reducing Systemic Cybersecurity Risk“ 14.01.2011

Die Empfehlung der Enquete-Kommission für den Bereich Datenschutz und Persönlichkeitsrechte, den Grundsatz Privacy by Design/by Default als verpflichtende Vorgaben bei der Entwickelung und dem Einsatz neuer Technologien festzuschreiben, kann auch auf den Sicherheitsbereich übertragen werden.

Für den Hochsicherheitsbereich sollten möglicherweise neue Modelle von Hardware und Software konzipiert und kontinuierlich weiterentwickelt werden.[821] Produkte sollten vor ihrer Verbreitung auch für diesen Bereich von einer unabhängigen Stelle geprüft werden.[822]

Die Enquete-Kommission bittet die Bundesregierung zudem zu prüfen, ob die Verpflichtung von Betreibern Kritischer Infrastrukturen zur Erfüllung von Mindestanforderungen (Stand der Technik) an IT-Sicherheit durch eine abstrakte gesetzliche Regelung sinnvoll ist.

b) SCADA- und PLC-Systeme

Gerade bei SCADA- und Programmable Logic Controller(PLC)[823]-Systemen, die bei Kritischen Infrastrukturen angewendet werden, sollten aus Sicht der Enquete-Kommission Sicherheitsaspekte stärker als bisher berücksichtigt werden. Grundsätzlich gibt es zwei Prinzipien, nämlich das „Security through Obscurity“ Prinzip[824] und das Kerckhoff-Prinzip[825]. Security through Obscurity bedeutet, dass die Funktionsweise der Software technisch verdeckt oder verschleiert wird, um es dem Angreifer zu erschweren, ausnutzbare Sicherheitslücken zu entdecken. Die Methoden der Absicherung – aber auch die Absicherung selbst – sind geheim. Falls der Angreifer im Vorfeld Informationen über das System erlangt, ist keine Sicherheit mehr gegeben, da das Prinzip nur solange Sicherheit garantiert, wie der Angreifer die Sicherheitslücken nicht kennt. Der Personenkreis, der in die Methoden der Absicherung „eingeweiht“ werden muss, ist sehr groß, weil das Prinzip jedem Zulieferer sowie jeder Firma, die solche Anlagen oder Teile davon installiert, bekannt sein muss. Damit ist die Gefahr des Geheimnisverrats enorm hoch, weil die Personengruppe, die Zugang zu dem Geheimwissen hat, unkontrollierbar groß wird.

---

[821] Stellungnahme Expertengespräch PG ZStrSi von Dr. Sandro Gaycken (FU), 28. November 2011

[822] Siehe hierzu auch die Kapitel 2.3.5 sowie 3.6 des Berichtes der Projektgruppe Datenschutz, Persönlichkeitsrechte der Enquete-Kommission Internet und digitale Gesellschaft. 15. März 2012. Drucksache 17/8999. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zwischenberichte/Zwischenbericht_Datenschutz_1708999.pdf

[823] http://en.wikipedia.org/wiki/Programmable_logic_controller

[824] http://de.wikipedia.org/wiki/Security_through_obscurity

[825] http://de.wikipedia.org/wiki/kerckhoffs_Prinzip

Kritische Infrastrukturen benötigen stattdessen Systeme, deren technische Funktionsweise prinzipiell vollständig offengelegt werden kann (das so genannte Kerckhoff-Prinzip), ohne das ein Sicherheitsrisiko entstehen kann. Notwendige Zugangsbeschränkungen, wiezum Beispiel Zugangsschlüssel oder Passwörter, müssen selbstverständlich absolut geheim bleiben und dürfen nur einer kleinstmöglichen Personengruppe zur Verfügung gestellt werden.

Die Funktionsweise der Systeme selbst sollte prinzipiell so sicher sein, dass auch bei Kenntnis der genauen Funktionsweise keine Gefahr eines Angriffs besteht. Einmal an diesem Punkt angelangt, ist die Offenlegung nur förderlich für das Auffinden möglicher weiterer Sicherheitslücken. Dieser sich positiv verstärkende Kreislauf aus Offenlegung und Bugfixes aufgrund von Meldungen interessierter Bürgerinnen und Bürger, die nun jeder Fachkundige abgeben kann, führt zu den denkbar sichersten Systemen. Die Gefahr, dass die Zugangsschlüssel durch menschliche Fehler zu dem Angreifer gelangen, stellt dann das größte Risiko dar.

Aus Sicht der Enquete-Kommission ist ein weiterer bekannter möglicher Problempunkt, dass zwischen dem Bekanntwerden einer Sicherheitslücke und den Sicherheitsupdates immer ein Zeitraum liegt, der möglicherweise von Angreifern genutzt werden kann. Die Enquete-Kommission empfiehlt daher Bund, Ländern und der Wirtschaft eine schnelle Handlungsfähigkeit bei Auftreten entsprechender Sicherheitslücken sicherzustellen (zum Beispiel durch ausreichend geschultes Personal). Gerade bei Anlagen zur Maschinensteuerung sind Updates schwierig und können nur selten geschehen, weil dazu in einigen Fällen die Anlage vollständig heruntergefahren werden muss.[826] Der Open-Source-Weg, also das Kerckhoff-Prinzip, ist daher für Kritische Infrastrukturen ein geeigneter Weg.

Die Enquete-Kommission empfiehlt Unternehmen, die Software für bestimmte Kritische Infrastrukturen entwickeln, diese vor der Verwendung durch einen zertifizierten unabhängigen Dritten (zum Beispiel BSI oder TÜV) prüfen zu lassen (IT-Security Audit) und die Prüfberichte zu veröffentlichen.

Wie in der Wirtschaft üblich, sollte gerade gegenüber Herstellern von Software für bestimmte Kritische Infrastrukturen zwingend darauf geachtet werden, dass der Source Code zur Überprüfung zugänglich gemacht wird.

[826] „Schwierige Hackerabwehr“ Dipl. Ing Maik G. Seewald, Spektrum der Wissenschaft, 10/2011

IT-Sicherheitsaspekte sollen bereits in der fachlichen wie auch in der allgemeinen technischen Auslegung zukünftiger Kritischer Infrastrukturen von Anfang an ausreichend mit berücksichtigt werden.[827]

c) Neue Technologien

Die Enquete-Kommission hat die Entwicklung der Wirtschaft hin zu mehr Cloud Computing aufmerksam verfolgt. Sie stellt fest, dass gerade für viele alltägliche IT-Nutzungen Cloud Computing ein Mehr an Sicherheit bewirken kann, da auch private und kleine gewerbliche Nutzer damit Zugang zu Speicher- und Anwendungssystemen mit professionellem Sicherheitsmanagement erhalten, ohne hierfür selbst mit eigener Expertise tätig werden zu müssen. Auf der anderen Seite können gerade bei der Nutzung für sicherheitskritische Daten und Anwendungen aus Sicht der Enquete-Kommission auch Sicherheitsprobleme entstehen, zum Beispiel wenn die Authentifizierung nicht sicher oder die Verfügbarkeit nicht umfassend gewährleistet ist. Sie regt daher eine vertiefte Diskussion darüber an, welche kritischen Daten und Geschäfte in der Cloud stattfinden können. Diese grundsätzliche Diskussion sollte bei allen anderen zugangsgesicherten Services geführt werden, da sie sich auch dort stellen.[828]

Die Enquete-Kommission hat auch die zunehmende Einführung von Smart Meters bei Kritischen Infrastrukturen aufmerksam verfolgt. Sie sieht auch in diesem Bereich technische und datenschutzrechtliche Risiken, die noch nicht vollständig ausgeräumt sind. Aus ihrer Sicht muss sichergestellt werden, dass die Verbraucherdaten nicht beliebig oft abgefragt werden können. Dies kann durch keine oder eine reduzierte Datenspeicherung erreicht werden. Weiterhin muss die Verbindung zwischen Smart Meter und Anbieter besonders gesichert sein, um ein Mithören oder eine Man-in-the-middle-Attacke durch Hacker auszuschließen. Auch auf Seiten des Anbieters müssen Daten gegen den Zugriff von unberechtigten Personen geschützt werden. Zudem muss die Software beim Anbieter, die Firmware auf dem Smart Meter sowie die Verschlüsselung und Authentifizierung regelmäßig auf den neuesten Stand gebracht werden. Dass dies erfolgt, kann nur durch unabhängige Dritte geprüft werden, mit transparent für jeden Bürger einsehbaren Prüfberichten. Ergänzend

---

[827] Stellungnahme Expertengespräch PG ZStrSi von Andreas Könen (BSI) 28. November 2011

[828] Die datenschutzrechtlichen Fragen des Cloud Computing wurden in der Projektgruppe Datenschutz, Persönlichkeitsrechte behandelt. Vgl. hierzu den fünften Zwischenbericht der Enquete-Kommission Internet und digitale Gesellschaft, Bundestagsdrucksache 17/8999. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zwischenberichte/Zwischenbericht_Datenschutz_1708999.pdf

weist die Enquete-Kommission darauf hin, dass neue neue Technologien auch zum Ausbau der Speicherkapazitäten und zur Reduktion der Komplexität benutzt werden können.[829]

d) Trennung von Systemen

Die Enquete-Kommission weist darauf hin, dass die steigende Vernetzung von Steuerung und Information mit einer wachsenden Anzahl von Schnittstellen zu einer erheblichen Skalierbarkeit von Störungen führt. Die dabei entstehenden Kaskadeneffekte können über die ursprünglich gestörte oder angegriffene Struktur erheblich hinausgehen und zu weitflächiger Dysfunktionalität führen. Das Einziehen von technischen „Brandmauern“ wird mit steigender Komplexität der Informationsstrukturen zunehmend schwieriger, da kaum mehr ein vollständiger Überblick über die wachsende Vielfalt möglicher Dominoeffekte und Übersprungstellen zu gewinnen ist.

Eine mögliche Gegenstrategie liegt in der Reduktion von Komplexität. Diese kann in einerTrennung von Systemen komplexer Informationsstrukturen, der physischen Trennung von eindeutig identifizierten „Kritischen“ und „weniger Kritischen“ Informationsstrukturen oder dem teilweisen Rückgriff auf einfachere Steuerungs- und Informationsstrukturen geschehen. Teil dieser Strategie kann auch das Einziehen getrennter und abgesicherter Redundanzen für zentrale Prozesse sein. Wichtig ist dabei deren verifizierte Entkoppelung von Skalen- und Dominoeffekten.

Die Enquete-Kommission regt daher an, dass die Bundesregierung das BSI beauftragt zu prüfen, welche Kritischen Infrastrukturen jetzt und auf welche Weise ans Netz angeschlossen sind. Zwei Beispiele von Kritischen Strukturen mit nahezu ungeschützten Internetzugängen sind einige Steuerungen von Schleusentoren und einige Notrufnummern.[830]

Die Enquete-Kommission weist darüber hinaus darauf hin, dass es zusätzlich die Möglichkeit gibt, eine vom Internet unabhängige Kommunikationsplattform zur Vernetzung von KRITIS zu entwickeln. Dies hat beispielsweise die USA mit ihrem „Global Information Grid Bandwidth Expansion“ gemacht.[831]

---

[829] „State of the Art der Forschung zur Verwundbarkeit kritischer Infrastrukturen am Beispiel Strom/Stromausfall“, Schriftenreihe Forschungsforum Öffentliche Sicherheit

[830] Stellungnahme Expertengespräch PG ZStrSi von Dr. Sandro Gaycken (FU), 28. November 2011

[831] „State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall“, Schriftenreihe Forschungsforum Öffentliche Sicherheit, Oktober 2010

Obwohl die Trennung von Systemen eine Option sein kann, bestehen aus Sicht der Enquete-Kommission auch erhebliche Bedenken.

Alternativtext der Fraktion DIE LINKE.

Obwohl die Trennung von Systemen eine Option sein kann, bestehen aus Sicht der Enquete-Kommission erhebliche Bedenken gegen eine komplette Trennung vom Netz

Die Abschottung vom Internet sichert Systeme dennoch nicht gegen Innentäter.

Ergänzungstext der Fraktion DIE LINKE.

Die Abschottung *vom öffentlich zugänglichen* Internet sichert Systeme dennoch nicht gegen Innentäter

Weiterhin kann sie auch zu einem falschen Sicherheitsbewusstsein innerhalb eines Unternehmens führen.

Auch das Aktualisieren von Komponenten mit neuen Patches gegen Sicherheitslücken wird durch eine zuvor erfolgte Trennung von Systemen deutlich schwieriger – ein Ingenieur muss beispielsweise mit einem Datenträger die neue Software von Hand aufspielen.

Ergänzungstext der Fraktion DIE LINKE.

Auch das Aktualisieren von Komponenten mit neuen Patches gegen Sicherheitslücken wird durch eine zuvor erfolgte Trennung von Systemen und *ihre Abkoppelung vom Netz* deutlich schwieriger – ein Ingenieur muss beispielsweise mit einem Datenträger die neue Software von Hand aufspielen.

Bestechung, Manipulation oder Erpressung von außen können zudem dazu führen, dass die Viren von einem Datenträger auf alle Geräte in ganzen Netzwerk verteilt werden, ohne dass dies festgestellt oder verhindert werden kann. Besonders gefährlich ist es, wenn die Hauptkomponenten vom Internet abgetrennt, und die Sicherheitsmaßnahmen darauf ausgerichtet sind, aber trotzdem weniger beachtete Komponenten (deren Zugangsmöglichkeit vielleicht gar nicht bekannt ist) doch Zugang zum Internet haben.

Streitig gestellt von der Fraktion DIE LINKE.

e) KRITIS

Wie im Umsetzungsplan KRITIS[832] explizit erwähnt, sollte die KRITIS-Strategie[833] entsprechend der veränderten IT-Sicherheitslage laufend angepasst werden.

Für Betreiber Kritischer Infrastrukturen (Unternehmen und Behörden) sollen IT-Sicherheit, Datensicherheit und Datenschutz eine Selbstverständlichkeit sein. Sie sind prioritär zu erfüllen und stellen damit auch einen wichtigen Wirtschaftsfaktor dar. In der Praxis haben sich oft marktwirtschaftliche Lösungen entwickelt. Zum Beispiel konnte Spam bereits deswegen erfolgreich bekämpft werden, weil es für die Unternehmen lukrativ war und einen zusätzlichen Service gegenüber den Nutzern darstellte.

Marktwirtschaftliche Lösungen haben sich somit aus Sicht der Enquete-Kommission bewährt und sind somit zunächst anzustreben. Sollten sie jedoch nicht zustande kommen und Instrumente auf freiwilliger Basis nicht mehr ausreichend sein, empfiehlt die Enquete-Kommission der Bundesregierung zu überlegen, ob für besonders schutzbedürftige Bereiche eine gesetzliche Pflicht zu einer unabhängigen Sicherheitsüberprüfung und zugleich Zertifizierung –zum Beispiel durch den TÜV angeordnet werden könnte. Die durchzuführenden Überprüfungen wären in regelmäßigen Zeitabständen zu wiederholen und würden einen hohen Standard sichern.

5. Forschung

Die Enquete-Kommission ist aufgrund der durchgeführten Expertengespräche zu dem Ergebnis gekommen, dass es auch weiterhin einen erhöhten Forschungsbedarf zu IT-Angriffen gibt. Insbesondere im Hinblick auf die Anzahl und Motivation von Innentätern wären aussagekräftigere Daten beziehungsweise Statistiken wünschenswert. Eine fortlaufende Aktualisierung der Statistiken würde zu einer besseren Einschätzung der Sicherheitslage beitragen.

Die Enquete-Kommission weist zudem auf die bisherigen Forschungsergebnisse des Fraunhofer Instituts hin. Demnach sollten insbesondere intersektorielle Abhängigkeiten

[832] Bundesministerium des Innern (Hrsg.): Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen (UP KRITIS). September 2007. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2007/Kritis.pdf?__blob=publicationFile

[833] Bundesministerium des Innern (Hrsg.): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Juni 2009. Online abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?__blob=publicationFile

Kritischer Infrastrukturen und die Möglichkeit von kaskadierenden Effekten genauer untersucht werden. Kaskaden verursachen 30 Prozent der KRITIS-Ausfälle.[834]

Die Enquete-Kommission regt darüber hinaus eine bessere Zusammenarbeit zwischen Herstellern, Providern, Sicherheitsexperten und Anwendern an. Insbesondere eine enge Kooperation der Hersteller von mobilen Geräten, von Betriebssystemen und von Schutzsoftware ist dringend erforderlich. Dabei dürfen aber Verantwortlichkeiten und Haftungsfragen nicht verwischt oder unzulässig ausgeweitet werden.

Die Enquete-Kommission spricht sich dafür aus, vorhandene Kompetenzen in Forschung und Industrie („Security made in Germany/Europe“) noch besser zu nutzen und auszubauen. Forschungsprojekte an Universitäten sollten verstärkt initiiert werden und deren Ergebnisse in Produkte des Alltags einfließen. Das würde zu einer besseren Ausstattung der IT-Infrastrukturen in Deutschland und Europa führen. Das gilt sowohl für Hardware (zum Beispiel eingebettete Chips) als auch für Software (Betriebssysteme). Es sollte das Ziel verfolgt werden, die komplette Lieferkette sicherer zu gestalten. Dazu gehört auch die physische Infrastruktur. Die Förderung von kleinen Unternehmen durch den Bund und die Länder wirkt innovationsfördernd und stellt daher einen wichtigen Bestandteil zur Erreichung des vorgenannten Ziels dar.

Streitig gestellt von der Fraktion DIE LINKE.

6. International

Die Enquete-Kommission stellt fest, dass Sicherheit nur durch abgestimmte Maßnahmen auf nationaler und internationaler Ebene erreicht werden kann. Zusätzlich zu Deutschlands aktuell schon sehr guter Unterstützung von ENISA, der Europäischen Agentur für Netz- und Informationssicherheit, muss die Kommunikation zwischen ENISA und den zuständigen deutschen Behörden durch die Bundesregierung kontinuierlich weiter verbessert werden. Die internationale Zusammenarbeit auf allen Ebenen – Europäische Union, NATO, G8-Staaten, G20-Staaten, Internet Governance Forum (IGF) und Vereinte Nationen – ist unverzichtbar.

Genauso wie auf nationaler Ebene sollten auch auf europäischer und internationaler Ebene Abhängigkeiten zwischen Kritischen Infrastrukturen untersucht werden. Die Enquete-Kommission regt daher die Durchführung einer Studie durch die Bundesregierung zur internationalen Abhängigkeit von Kritischen Infrastrukturen an.

[834] http://www.zukunftsforum-oeffentliche-sicherheit.de/downloads/ZOES-12-Rome.pdf

Dann kann definiert werden, in welchen Bereichen gemeinsame Aktionen (zunächst auf europäischer Ebene) notwendig sind.[835] Momentan existieren in den europäischen Ländern im Hinblick auf den Schutz Kritischer Infrastrukturen unterschiedliche Schutzlevel. Weil sich Störungen von Kritischen Infrastrukturen auch grenzüberschreitend auswirken können, ist es sinnvoll, Schutzmaßnahmen, wie zum Beispiel Standards, Bildung, Informationsaustausch, gemeinsamen Kriterien für Risikoanalyse usw., auf europäischer Ebene zu koordinieren. Gremien, wie zum Beispiel das European Public-Private Partnership for Resilience (EP3R), können hierzu einen wertvollen Beitrag leisten. Planspiele und Simulationen auf nationaler, europäischer und internationaler Ebene sind sinnvolle Maßnahmen und sollten daher von der Bundesregierung und den Ländern auch in Zukunft unterstützt werden.

Die Enquete-Kommission unterstützt das Vorhaben der Bundesregierung unter dem Dach der Vereinten Nationen einen Cyber-Kodex für gutes Verhalten von Staaten im Netz zu schaffen (Norms of State Behaviour in Cyberspace). Die Unterzeichnung eines solchen Kodexes durch eine Vielzahl von Staaten wäre nicht nur eine starke vertrauens- und sicherheitsbildende Maßnahme, sondern auch ein erster Schritt hin zu einer gemeinsamen Abwehr von Bedrohungen.

[835] "Protecting Critical Infrastructure in the EU", CEPS 2010

Ergänzende Handlungsempfehlungen der Fraktionen der SPD und BÜNDNIS 90/DIE GRÜNEN und der Sachverständigen Alvar Freude, Constanze Kurz, Prof. Dr. Wolfgang Schulz, Lothar Schröder, Cornelia Tausch

zum Kapitel „Schutz Kritischer Infrastrukturen im Internet“

Die Fraktionen der SPD und BÜNDNIS 90/DIE GRÜNEN sowie die Sachverständigen Alvar Freude, Constanze Kurz, Prof. Dr. Wolfgang Schulz, Lothar Schröder, Cornelia Tausch … begrüßen es ausdrücklich, dass es der Enquete-Kommission gelungen ist, zu einigen grundsätzlichen Fragestellungen zum „Schutz kritischer Infrastrukturen“ eine gemeinsame Position zu erarbeiten und gemeinsame Handlungsempfehlungen vorzuschlagen. Leider sind diese gerade mit Blick auf die Stabilität und Sicherheit der Infrastruktur und die Schaffung eines Immunsystems der digitalen Gesellschaft nicht weitgehend genug, nicht zuletzt deswegen, weil damit das Lagebild zur Cybersicherheit und zu konkreten Angriffen nicht wirksam verbessert wird. Vor diesem Hintergrund werden folgende über die mehrheitlich beschlossenen Handlungsempfehlungen hinausgehende Handlungsempfehlungen gegeben:

Stabilität und Sicherheit der Infrastruktur

Die Enquete-Kommission hat in einer Zustandsanalyse herausgearbeitet, wie abhängig usnere moderne Gesellschaft von Informations- und Kommunikationstechnologien heute ist und hat diese als eine zentrale Kritische Infrastruktur (KRITIS) identifiziert. Bei großflächigen IT-Störungen und –Ausfällen, die als Folge unter Umständen sogar einen längeren Stromausfall von mehreren Tagen oder Wochen nach sich ziehen können, sind nicht nur Privatpersonen und deren Haushalte betroffen, sondern auch Behörden und Organisationen mit Sicherheitsaufgaben, Krankenhäuser und Pflegeeinrichtungen, der Handel sowie zahlreiche weitere Wirtschaftszweige betroffen. Der Ausfall oder die schwerwiegende Beeinträchtigung einer sogenannten Kritischen Infrastruktur, also auch der IT, kann kaskadierende Folgen für die gesamte Versorgungssicherheit (Wasser, Energie, Transport und Verkehr etc.) nach sich ziehen. Die Enquete-Kommission hat in ihrem Bericht auch dargelegt, wo und wodurch in diesen digital vernetzten Strukturen Sicherheitslücken entstehen können und welche Folgen ein längerer Ausfall einer entsprechenden Netzinfrastruktur nach sich ziehen kann. Desweiteren wurde dargelegt, wo Kritikalität identifiziert und welche Schutz- und Abwehrstrukturen bereits national- und international etabliert sind. Zudem wurden bestehende Defizite identifiziert und künftige Herausforderungen beschrieben.

Die digitale Vernetzung bietet viele Chancen, die auch im Bereich digital vernetzter Infrastrukturen zum Tragen kommen. Nichtsdestotrotz dürfen die in Kapitel II.1.2

dargestellten Risiken nicht unterschätzt werden. Die Enquête-Kommission Internet und digitale Gesellschaft empfiehlt deshalb dem Deutschen Bundestag,

1. die Bundesregierung aufzufordern, eine umfassende Bestandsaufnahme der kritischen digitalen Infrastruktur vorzulegen und hierbei neben den technischen Fragestellungen insbesondere auch die intersektorielle Abhängigkeit von Anbietern proprietärer Systeme zu untersuchen.

2. die Bundesregierung aufzufordern, zu überprüfen, ob und inwieweit eine verstärkte Nutzung der Möglichkeit einer Trennung von Systemen einen Beitrag zum Schutz Kritischer Infrastrukturen zu leisten vermag,

3. in Gesetzgebungsverfahren, in denen Kritische Infrastrukturen angelegt werden oder betroffen sind, die Regelungen so auszugestalten, dass eine Trennung von Systemen möglich beziehungsweise unterstützt wird, soweit diese sich als notwendig erweist. Damit kann die autarke Stellung einer Kritischen Infrastruktur gefestigt und Kaskadeneffekten entgegenwirkt werden. Sie soll nicht durch immer weitere Vernetzungen mit anderen Infrastrukturen anfälliger für Angriffe von außen werden.

4. die besondere Stellung von Energienetzen, dem Internet sowie von zentralen IT-Steuerungsnetzen als Kritische Infrastrukturen (KRITIS) hervorzuheben und eine verbindliche Definition festzulegen, zum Beispiel durch Festschreibung in der einschlägigen Gesetzgebung etc. Hinsichtlich konkreter Auswirkungen und Folgen sowie Möglichkeiten für deren Bewältigung wird auf das Grünbuch des Zukunftsforums Öffentliche Sicherheit, Kapitel 3[836] sowie die TAB-Studie, Kap. IV[837] verwiesen.

5. die Sicherheitsstrategie für KRITIS weiterzuentwickeln und mit einer zivilen Cybersicherheitsstrategie zu einer integrierten Gesamtstrategie zusammenzuführen, so dass auch die im Bundesdatenschutzgesetz (BDSG) vorhandenen Lücken etwa im Hinblick auf generelle Informationspflichten sowie eine Mithaftung des Datenverarbeiters bei unrechtmäßiger Datenerlangung durch Dritte im Falle von unzureichenden Sicherheitsvorkehrungen, geschlossen werden.

836 „Risiken und Herausforderungen für die Öffentliche Sicherheit in Deutschland“, Grünbuch des Zukunftsforums Öffentliche Sicherheit, 1. Aufl., Sept. 2008.

837 „Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen Ausfalls der Stromversorgung“, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, November 2010.

6. die Schaffung eines allgemeinen IT-Sicherheits-Rahmengesetzes unter Einbeziehung der bestehenden beziehungsweise Ersetzung der veralteten Vorschriften, in dem auch die neue Definition von KRITIS sowie die entsprechenden Melde- und Veröffentlichungspflichten für bekannt gewordene Angriffe oder über Sicherheitslücken enthalten sein sollen.

7. Aus Sicht der Enquete-Kommission muss der Informationsaustausch zwischen den Sicherheitsbehörden für die Beurteilung der IT-Sicherheitslage verbessert werden. Dies kann nicht nur bei der Prävention helfen, sondern auch die Reaktionsfähigkeit erheblich beschleunigen. Dabei ist es wichtig, dass das Cyberabwehrzentrum einen reinen Informationsaustausch anbietet, darüber hinaus jedoch keine neuen Kompetenzen zusätzlich verteilt und das strikte Trennungsgebot eingehalten wird. Darüber hinaus sollte das Cyberabwehrzentrum weiterentwickelt werden, um der Komplexität der Cyber-Bedrohungen gerecht zu werden. Hierbei sollte neben dem technischen Sachverstand verstärkt auf die interdisziplinäre Zusammensetzung gedrängt werden. So sollten beispielsweise auch Juristen, Sozialwissenschaftler und die Datenschutzbehörden beteiligt werden.

IT-Sicherheit: Schaffung eines Immunsystems der digitalen Gesellschaft

Sicherheitslücken in Soft- und Hardware können nie gänzlich ausgeschlossen werden. Mit geeigneten modernen Methoden der Software-Entwicklung und Qualitätskontrolle können diese aber hinsichtlich Anzahl und Schwere durchaus eingeschränkt werden. Dies kostet allerdings Zeit und Geld, ohne dass der Kunde direkt neue Funktionen in der Software bemerkt. Der Anreiz, in Sicherheit zu investieren, ist daher für viele Hersteller gering.

In den vergangenen Jahrzehnten hat sich der Trend durchgesetzt, den zunehmenden Bedrohungen mit Verschärfungen des Strafrechts zu begegnen. Die stetig wachsende Zahl an Angriffen zeigt jedoch, dass die Bedrohung damit nicht reduziert werden konnte.

Vor diesem Hintergrund hält es die Enquete-Kommission für geboten, ein „Immunsystem der digitalen Gesellschaft“ aufzubauen. Dazu gehört sowohl Anreize für die Erstellung sicherer Software zu schaffen als auch den Druck zur schnellen Behebung von Sicherheitslücken weiter zu erhöhen. Angriffe und Lücken müssen daher schnellstmöglich identifiziert sowie gegenüber potenziell Betroffenen kommuniziert und behoben werden. Zugleich muss gegenüber staatlichen Stellen - deren Aufgabe die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung ist -, angezeigt werden, wenn Kritische Infrastrukturen betroffen sein könnten.

Viele Angriffe auf informationstechnische Systeme oder Sicherheitslücken werden nicht bekannt. Dadurch können andere Nutzer der gleichen Software ihre Systeme nicht vor Angriffen schützen. Von zunehmender Bedeutung ist zudem der Schutz von Cloud-Diensten, denn diese stellen für Angreifer attraktive Ziele dar, da hier oft eine Vielzahl von unterschiedlichsten Daten gespeichert werden. Um so wichtiger ist es, dass die Betroffenen über IT-Sicherheitsprobleme des jeweiligen Dienstleisters informiert werden, um ihren IT-Sicherheitsschutz enstsprechend anpassen zu können. Die Enquete-Kommission empfiehlt dem Deutschen Bundestag deshalb

1. eine Regelung zu schaffen, die eine grundsätzliche Meldepflicht von bekanntgewordenen und hinsichtlich ihres Gefahrenpotentials näher zu definierenden und differenzierenden Angriffen auf staatliche und private Stellen an das Bundesamt für Sicherheit in der Informationstechnik (im folgenden BSI genannt) beinhaltet – eine solche Meldepflicht ist zwingend zur Verbesserung des Lagebildes erforderlich.

2. das BSI gesetzlich zur Veröffentlichung dieser Angriffe zu verpflichten. Dabei kann eine Veröffentlichung grundsätzlich anonym erfolgen; eine anonyme Nutzung ist angezeigt, um zu verhindern, dass angegriffene Unternehmen durch diese Meldungen einen erheblichen Vertrauensverlust erleiden und aus diesem Grunde die Meldepflicht zu umgehen versuchen.

3. zu den Ausführungen unter Punkt 2 sind schnellstmöglich Erhebungen über weitere erforderliche personelle und finanzielle Ressourcen im BSI erforderlich .

4. Anbieter von Cloud-Diensten sollten darüber hinaus verpflichtet werden, ihre Kunden über erkannte Angriffe zu informieren, damit diese ihren Schutz entsprechend anpassen können.

5. eine gesetzliche Regelung zu schaffen, die Soft- und Hardware-Hersteller verpflichtet, ihnen bekannt gewordene Sicherheitslücken ihrer Software gegenüber dem BSI unmittelbar nach Bekanntwerden anzuzeigen.

6. eine gesetzliche Regelung zu schaffen, nach der alle öffentlichen Stellen und Behörden verpflichtet werden, ihnen bekannt gewordene Sicherheitslücken unmittelbar an das BSI zu melden.

7. den verstärkten Einsatz freier Software und offener Formate fördert, die nachweislich eine verminderte Vulnerabilität gegenüber IT-Angriffen mit sich bringt

Entdecker von Sicherheitslücken stehen oftmals vor dem Problem, dass sie entweder gänzlich ignoriert oder mit zivil- oder strafrechtlichen Verfahren bedroht werden, wenn sie ihre Entdeckung beispielsweise an den Hersteller einer Software oder Betreiber einer Internet-Anwendung melden. Daher unterlassen viele solche Meldungen. Dies sorgt dafür, dass bestehende Sicherheitslücken nicht gestopft und von Kriminellen ausgenutzt werden können, beispielsweise wenn Informationen über Lücken auf dem Schwarzmarkt gehandelt werden.

Vor diesem Hintergrund empfiehlt die Enquête-Kommission dem Deutschen Bundestag

8. eine beim BSI angegliederte Meldestelle einzurichten, bei der jeder (auf Wunsch anonym oder pseudonymisiert) Meldungen über Sicherheitslücken einreichen kann, ohne Konsequenzen befürchten zu müssen.

9. Zu prüfen, ob und in welchem Umfang die zur Bearbeitung der Meldungen entsprechenden personellen und finanziellen Ressourcen des BSI aufgestockt werden müssen.

10. eine Weiterleitung der Meldungen an die jeweils verantwortlichen Hersteller durch die Meldestelle festzuschreiben und die Behebung der Sicherheitslücken zu überprüfen.

11. eine gesetzliche Regelung zu schaffen, die Sicherheitsforscher und Entdecker von Sicherheitslücken vor straf- und zivilrechtlicher Verfolgung schützt, wenn diese sich verantwortungsvoll verhalten.

12. eine gesetzliche Regelung zu schaffen, die interne und externe Personen schützt, die Sicherheitslücken offenlegen (Whistleblowerschutz).

Es gibt immer wieder Fälle, in denen die Hersteller von Betriebssystemen, Anwendungsprogrammen oder weiterer Software auch Jahre nach Kenntnis von Sicherheitslücken diese weder beheben noch veröffentlichen. Während dieser Zeit können diese Lücken von Kriminellen ausgenutzt werden, ohne dass die betroffenen Anwender die Möglichkeit zur Umgehung des Problems haben. Es ist daher für die Gesellschaft nützlich, wenn Sicherheitslücken der Allgemeinheit bekannt werden: Jeder hat dann die Möglichkeit, Schutzmaßnahmen zu ergreifen. Zudem steigt der Druck auf den Hersteller, das Problem tatsächlich zu beheben.

Daher empfiehlt die Enquête-Kommission dem Deutschen Bundestag

13. eine gesetzliche Regelung zu schaffen, nach der das BSI verpflichtet wird, nach einer Frist von 30 Tagen nach Meldung an den Hersteller, die Lücke, Details dazu und

Möglichkeiten zur Beseitigung oder Umgehung des Problems zu veröffentlichen („Full Disclosure“). Diese Frist kann in schwierig zu behebenden Fällen auf Antrag bis zu zwei mal um jeweils 30 Tage verlängert werden.

Für viele Hersteller ist Sicherheit nur ein Kostenfaktor, der sich nicht in einem höheren Umsatz niederschlägt. Um den ökonomischen Anreiz für sichere Software zu steigern empfiehlt die Enquête-Kommission dem Bundestag

14. zu prüfen, wie Anbieter gegebenfalls auch gesetzlich verpflichtet werden könnten, IT-Sicherheit stärker in die Produkte zu implementieren. Dies kann beispielsweise durch Produkthaftungsregelungen oder eine Beweislastregelung befördert werden.

Des Weiteren empfiehlt die Enquête-Kommission dem Bundestag

15. eine gesetzliche Regelung zu schaffen, die seitens der Provider ab einer relevanten Größe eine Erreichbarkeit gegenüber dem BSI an sieben Tagen in der Woche für 24 Stunden gewährleistet.

16. eine Regelung zu schaffen, die sicherstellt, dass für IT-Projekte der öffentlichen Hand von Beginn an Risiko- und Bedrohungsmodelle (Thread Model) erstellt werden. Dazu gehört ein effizientes Konzept zur sicheren Entwicklung sowie eines sicheren Lebenszyklus für die Software. Diese sollen öffentlich zugänglich sein, so dass sie von unabhängiger Seite begutachtet werden können. Dadurch fallen potentielle Risiken frühzeitig auf und durch die Öffentlichkeit wird es erschwert, angebrachte Maßnahmen nicht durchzuführen.

17. unter dem IT-Sicherheitsaspekt ist auch das „Dilemma“ zwischen Wettbewerb und Sicherheit zu prüfen: Einige Anbieter schotten ihre Produkte oder Marktplätze ab und errichten hohe Barrieren, während andere Anbieter ihre Produkte und Marktplätze für den Wettbewerb öffnen,. Sicherheitsaspekte dürfen nicht Vorwand für die Abschottung gegenüber dem Wettbewerb sein. Darum sind Initiativen zu fördern, die IT-Sicherheit mit offenen Plattformen und offener Software verbinden.

Darüber hinaus empfiehlt die Enquête-Kommission:

18. im Bereich des Informatik-Studiums und der Ausbildung verstärkt den Bereich der Sicherheit und sicherer Software-Entwicklung zu beachten.

Die bei Mobiltelefonen genutzte GSM-Verschlüsselung kann nicht mehr als sicher angesehen werden, seit sie 2009 kompromittiert und erfolgreiche Angriffe dokumentiert wurden.

Mittlerweile steht für Wirtschaftsspionage oder den Bruch der Privatsphäre der Nutzerinnen und Nutzer von Mobiltelefonen einfach einzusetzende Software zur Verfügung.

Die Enquete-Kommission fordert die Bundesregierung daher auf,

19. bei den deutschen Unternehmen und insbesondere bei den Mitgliedern der GSM Association darauf zu drängen, dass im Rahmen der GSM Association schnellstmöglich ein neuen Standard für ein sicheres Verschlüsselungsverfahren auf den Weg gebracht wird.

Auditierung

Die Enquete-Kommission nimmt Bezug auf das Kapitel 4.2.2.6, Seite 79 bis 81 des Zwischenberichtes der Projektgruppe Datenschutz, Persönlichkeitsrechte[838] und verweist auf die dort gemachten Ausführungen und Handlungsempfehlungen zum Thema Regulierte Selbstregulierung und Auditierung. Sie stellt fest, dass Datenschutzaudits und Datenschutzgütesiegel ein wesentliche Instrumente zur Vertrauensbildung im gegenseitigen Verhältnis von Bürgern, Unternehmen und Staat darstellen können.

Deshalb wird dem Deutschen Bundestag empfohlen,

1. ein Datenschutzauditgesetz gemäß § 9a BDSG zu verabschieden, welches den Unternehmen die Möglichkeit eines Audits auf freiwilliger Basis bietet und dessen Verfahren unbürokratisch, aber verbindlich ausgestaltet sein muss. Hierbei sind folgende Punkte – angelehnt an das Datenschutz-Behördenaudit des Unabhängigen Landeszentrums für den Datenschutz Schleswig-Holstein (ULD)[839] nach § 43 Abs. Landesdatenschutzgesetzes Schleswig-Holstein (LDSG SH) – bei der Schaffung eines Datenschutzaudit-Gesetzes im Besonderen zu beachten:

a) Zunächst sind Begrifflichkeiten und Gegenstand des Datenschutz-Behördenaudits zu klären. Gleichzeitig muss das Datenschutzaudit-Zeichen festgelegt werden. Es sollten ebenso Audits bereits für Verfahren, die erst in der Planung und Entwicklung sind vergeben werden können (sogenanntes Konzept-Audit[840]).

---

[838] Bericht der Projektgruppe Datenschutz, Persönlichkeitsrechte der Enquete-Kommission Internet und digitale Gesellschaft. 15. März 2012. Drucksache 17/8999. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zwischenberichte/Zwischenbericht_Datenschutz_1708999.pdf.

[839] https://www.datenschutzzentrum.de/material/recht/audit.htm (Quelle: Stand 19.11.2012, 10.40 Uhr)

[840] vgl. https://www.datenschutzzentrum.de/material/recht/audit.htm - Punkt 2.2 (Quelle: Stand 19.11.2012, 10.40 Uhr)

b) Ebenso bedarf es einer Regelung über die Vereinbarung über die Durchführung des Auditierungsverfahrens. Diese Regelung sollte u. a. die Schriftform voraussetzen und den Audit-Gegenstand, die Auditierungs-Art, die einzelnen Verfahrensschritte, den Ablauf des Verfahrens, den zeitlichen Rahmen sowie die damit befassten Personen und Funktionen beinhalten.[841]

c) In das Auditierungsgesetz muss ebenfalls aufgenommen werden, ob und inwieweit ein Voraudit erfolgt und welche Verfahrensschritten hierfür erforderlich sind sowie welche einzelnen Schritte für die Durchführung des Behörden-Audits notwendig sind.

d) Ebenso bedarf es weiterer Voraussetzungen für die Erteilung des Audits, wie zum Beispiel die Festlegung von Datenschutzzielen, die Einrichtung eines Datenschutzmanagementsystems und die Ausarbeitung eines Datenschutzkonzeptes. Entsprechende Regelungen, die Art und Weise und Umfang beinhalten sind in den Gesetzentwurf aufzunehmen.

e) Der Gesetzentwurf muss desweiteren Regelungen enthalten, unter welchen Voraussetzungen genau eine Zertifizierung und eine Erteilung des Auditzeichens zu erfolgen hat. Hierbei schlägt die Enquete-Kommission die Erteilung der Zertifizierung sowie des Auditzeichens für einen begrenzten Zeitraum, z. B. für drei Jahre, vor.

f) Gleichzeitig muss sich auch eine Regelung in dem Gesetz wiederfinden, aus der sich ergibt, wann und unter welchen Umständen eine Zertifizierung zurückzuziehen ist bzw. zurückgezogen werden kann.

g) im Rahmen von Vergabegesetzen ist eine Verpflichtung öffentlicher Stellen zu verankern, solche auditierten beziehungsweise zertifizierten Produkte bevorzugt einzusetzen. Soweit keine Vergabegesetze bestehen, ist im Rahmen der Ausschreibungen zu berücksichtigen, dass besonders datenschutzfreundliche Produkte bevorzugt eingekauft oder genutzt werden.

Stiftung Datenschutz

Die Enquete-Kommission stellt fest, dass die geplante Stiftung Datenschutz, wenn die richtigen Vorgaben für die inhaltliche Ausgestaltung gefunden werden, als wirkungsvolle Plattform vorhandene Angebote zusammenführen und so ihrem geplanten Auftrag für

Aufklärung und Information gerecht werden kann. Die von der Bundesregierung auf den Weg gebrachte Stiftung Datenschutz ist deshalb im Grundsatz zu begrüßen. Die Enquete-Kommission verweist in ihren Ausführungen und Handlungsempfehlungen insoweit auf Kapitel 4.2.2.6, S. 80-81 des Zwischenberichtes zur Projektgruppe Datenschutz, Persönlichkeitsrechte.[842] Die Enquete-Kommission bekräftigt ihre dort gemachten Ausführungen und fordert die Bundesregierung auf, bei Einsetzung der Stiftung folgende Punkte – die für eine wirkungsvolle Arbeit einer Bundesstiftung Datenschutz mit vorstehendem Auftrag unabdinglich sind – zu berücksichtigen:

1. Die Stiftung ist wirtschaftlich und organisatorisch, also finanziell und personell, unabhängig von den zu bewertenden Unternehmen und der Exekutive zu organisieren. Insbesondere ist

a. die Besetzung der Stiftungsgremien so zu konzipieren, dass die Freiheit der Stiftungsorgane bei der Willensbildung gewährleistet ist. Der Beirat der Stiftung muss hierzu paritätisch mit Vertretern der unabhängigen Datenschutzbeauftragten des Bundes und der Länder, Verbrauchervertretern sowie Vertretern aus Politik, Wissenschaft und Wirtschaft besetzt sein.
b. zu gewährleisten, dass die Stiftung ihre Aufgaben unabhängig von der datenverarbeitenden Wirtschaft ausführen kann.
c. die Stiftung so zu konzipieren, dass sie nicht finanziell von den privaten datenverarbeitenden Unternehmen abhängig wird, welche die zu entwickelnden Standards und Zertifizierung später nutzen.
d. den Datenschutzbeauftragten des Bundes und der Länder bei der Entwicklung der Aufgabenstellung der Stiftung entscheidenden Einfluss einzuräumen;

2. In der Satzung ist das Verhältnis zu den Datenschutzbehörden zu klären. Es ist festzuhalten, dass diesen allein die Kontrolle über die Einhaltung der Gesetze obliegt und die Aufsichtstätigkeit nicht durch die Arbeit der Stiftung beeinflusst werden darf. Ebenso dürfen die von der Stiftung Datenschutz erteilten Audits und Gütesiegel keine rechtliche Bindungswirkung gegenüber den Datenschutzbehörden entfalten, das heißt

[842] Bericht der Projektgruppe Datenschutz, Persönlichkeitsrechte der Enquete-Kommission Internet und digitale Gesellschaft. 15. März 2012. Drucksache 17/8999. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zwischenberichte/Zwischenbericht_Datenschutz_1708999.pdf

die Aufsichtsbehörden müssen die entsprechenden Unternehmen dennoch anlassbezogen überprüfen dürfen.

3. Es ist in der Satzung zu regeln, wer die materiellen Standards für Zertifizierungsverfahren setzt. Dabei sind ein Höchstmaß an Transparenz sowie eine enge Kooperation mit den Datenschutzbehörden unabdingbar.

4. Die Vergabe von Audits kann durch die Stiftung Datenschutz aufgrund eines bundeseinheitlich gesetzlich festgelegten Auditierungsverfahrens erfolgen. Hierfür bedarf es eines Gesetzes im Sinne von § 9a BDSG. Dabei ist zu beachten, dass bereits existierende Auditverfahren (wie zum Beispiel in Bremen oder Schleswig-Holstein) in die Ausgestaltung und Vergabe eingebunden werden.

5. Bei der Vergabe von Gütesiegeln durch die Stiftung ist darauf zu achten, dass ein einheitliches Gütesiegel entwickelt wird und eine inflationäre Handhabung bei der Vergabe vermieden wird. Ebenso ist das Verfahren für die Vergabe transparent zu gestalten. Die Gütesiegel sind nur für eine bestimmte Zeit (zum Beispiel für zwei Jahre) zu erteilen und müssen turnusgemäß geprüft werden.

6. Es ist dafür Sorge zu tragen, dass die Stiftung bei der Entwicklung von Standards und Prüfparametern für die Vergabe von Gütesiegeln die Weiterentwicklung des Datenschutzrechts auf Europäischer Ebene berücksichtigt

7. Im Bereich der Bildung darf die Stiftung Datenschutz nicht die Zuständigkeit der Länder verletzen. Die Länder sind deshalb mitentscheidend einzubeziehen. Schwerpunkt der Stiftungstätigkeit sollte deshalb allenfalls die außerschulische Bildung sein.

8. Im Bereich der Aufklärung wird der Stiftung empfohlen, ein zentrales Informationsportal oder ein virtuelles Datenschutzbüro (wie derzeit beim ULD Schleswig-Holstein praktiziert) zu schaffen.

9. Die Stiftung Datenschutz sollte perspektivisch auch im Bereich der Datenschutzforschung, insbesondere der Entwicklung und dem Ausbau von Instrumenten des technischen Datenschutzes, tätig werden. Mögliche Tätigkeitsfelder eröffnen sich sowohl im Bereich der Koordination der Forschungsmittelvergabe als auch für den Bereich eigener Forschungsanstrengungen.

Die Fraktion BÜNDNIS 90/DIE GRÜNEN trägt diese Empfehlung nicht mit

Einrichtung eines Digitalen Hilfswerks

Dass nicht jede digitale Sicherheitslücke sofort entdeckt wird, kann mitunter am fehlenden Know-how oder an der Organisation der betreibenden Stelle einer KRITIS liegen. Hier bedarf es der Unterstützung von Experten, die zum Beispiel ihr Wissen und ihre Kenntnis in einer freiwillig tätigen Organisation zur Verfügung stellen. So empfiehlt die Enquete-Kommission dem Deutschen Bundestag

1. die gegebenenfalls notwendigen gesetzgeberischen Voraussetzungen zu schaffen und finanzielle Möglichkeiten in den Haushalt einzustellen, die die Gründung eines sogenannten Digitalen Hilfswerks (DHW) ermöglichen. Dabei kann eine Gründung ähnlich der Bundesanstalt des Technischen Hilfswerks erfolgen beziehungsweise eine Angliederung an dieses nachgedacht werden. Der Vorteil eines solchen, die bestehenden Sicherheitsstrukturen ergänzenden DHW liegt u. a. darin, dass dieses im Gegensatz zu bereits bestehenden ehrenamtlichen Strukturen, grundsätzlich weder zeit- noch ortsgebunden agieren kann.
2. Dieses DHW soll helfen, Sicherheitslücken bei zentralen Infrastrukturen ausfindig zu machen, diese zu analysieren und an das BSI melden. Es soll eine zusätzliche Unterstützung für Unternehmen und Behörden bieten, die kritische Infrastrukturen bereitstellen. Es soll sie im Krisen und Notfall (etwa bei erheblichen Angriffen) durch Personal und Expertise unterstützen. Darüber hinaus könnte es für eine gegenseitige Fort- und Weiterbildung sorgen und mit Aktionen zur Aufklärung der Bürgerinnen und Bürger zu Sicherheitsfragen im Netz sowie für Aktionen zur Sensibilisierung für Gefahren tätig sein.

Haftung bei Sicherheitsproblemen, Produkthaftung

Unternehmen die u. a. ihr Geschäftsmodell auf Closed Source Software ausrichten oder öffentliche Internet-Angebote bereitstellen sollen auch bei Sicherheitslücken und daraus resultierenden Schadensfällen entsprechend haften. Darüber hinaus besteht Bedarf für mehr Rechtssicherheit der Anpassung der Haftungstatbestände für Produkt- und Gewährleistungshaftung. Deshalb empfiehlt die Enquete-Kommission dem Deutschen Bundestag

1. die gesetzliche Anpassung der Haftungsregelungen auf digitale Tatbestände. Dabei sollte in die Haftungstatbestände aufgenommen werden, dass dem entwickelnden Unternehmen bei der Entwicklung eines Software- oder Hardware-Produkts eine gewisse Sorgfalt hinsichtlich der Genauigkeit und Anfälligkeit in Bezug auf Sicherheitslücken abverlangt werden kann.

2. zu prüfen, ob und inwieweit eine Beweislastumkehr im Rahmen dieser Anpassungen zugunsten des Nutzers geschaffen werden kann, da der Betroffene im Zweifelsfall die Zusammenhänge oft nicht richtig darlegen kann.

Ebenso wurde einheitlich von den Experten in dem Fachgespräch festgestellt, dass es den Internet-Nutzern oft an einer Sensibilisierung für die Gefahren bei der sicheren Internetnutzung fehlt. Die Enquete-Kommission schließt sich den Experten an und empfiehlt deshalb dem Deutschen Bundestag,

3. den Bedarf für weitere finanzielle Mittel für aufklärende Projekte und Aktionen hinsichtlich bereits vorhandener Gütesiegel und Vergleiche hinsichtlich ihrer Aussagekraft und Qualität gegenüber den Bürgerinnen und Bürgern zu klären und zu prüfen, inwieweit Anreize geschaffen werden können, bestehende Angebote zur Vermittlung von Medienkompetenz um IT-Sicherheitsaspekte zu ergänzen.

Handlungsempfehlungen zum Kapitel „Kriminalität im Internet“

Der Modus Operandi im Bereich Internetkriminalität ist größtenteils schon aus konventionellen Kommunikationsmitteln bekannt: Straftaten, die man aus der realen Welt kennt, begegnet man auch im Netz. Ausnahmen stellen spezifische Cybercrime-Delikte wie etwa Identitätsdiebstahl oder Phishing dar, doch auch diese werden größtenteils durch die Strafrechtsnormen im Bereich der Datendelikte bereits erfasst. Eine valide Darstellung der Steigerungsraten dieser Delikte ist jedoch aufgrund des zum Teil großen Dunkelfeldes schwierig.

Das Internet ist ein Teil unserer Gesellschaft, die eine fortschreitende Digitalisierung erlebt. Damit werden sich auch in den kommenden Jahren Erscheinungsformen von Kriminalität ins Internet verlagern oder dort entstehen.

Dabei ist zu berücksichtigen, dass es sich im Bereich der Internetkriminalität bereits heute oft um grenzüberschreitende Ermittlungsverfahren handelt, die nur mittels nationaler Aktivitäten und Informationsquellen erfolgreich durchgeführt werden können. Auslandsermittlungen bedingen in aller Regel justizielle Rechtshilfeersuchen, die den Ermittlern die benötigten Informationen nur mit erheblichen Zeitverzögerungen zur Verfügung stellen. Problematisch ist dieser Zeitverzug insbesondere vor dem Hintergrund der Flüchtigkeit der Daten.

Streitig gestellt von der Fraktion DIE LINKE.

1. Vor dem Hintergrund langwieriger Rechtshilfeersuchen empfiehlt die Enquete-Kommission der Bundesregierung und den Ländern dringend, die Rechtshilfewege zu beschleunigen und sich auf internationaler oder zumindest bilateraler Ebene dafür einzusetzen, dass Rechtshilfeersuchen in kürzerer Laufzeit nachgekommen wird. Dies könnte beispielsweise durch die Erweiterung bestehender Rechtshilfeabkommen oder aber durch einen stärkeren personellen Austausch (beispielsweise durch gemeinsame Tagungen, Fortbildungsveranstaltungen und gegenseitige Hospitationen) mit den betroffenen Staaten erreicht werden. Hierbei müssen aber auch weiterhin bestehende Grundrechte gewahrt bleiben.

2. Die Enquete-Kommission empfiehlt vor dem Hintergrund der Überlastung der notwendigen Spezialdienststellen und der weiterhin zunehmenden Bedeutung des Internet eine personelle und technische Aufstockung sowohl bei den Polizei- als auch bei den Justizbehörden des Bundes und der Länder.

3. Die Enquete-Kommission empfiehlt dem Deutschen Bundestag und der Bundesregierung, kontinuierlich (zum Beispiel wiederkehrend alle 4 Jahre) den Straftatenkatalog des §100 a Absatz 2 StPO auf seinen rechtstatsächlichen Bedarf und die Wirksamkeit des Kernbereichschutzes hin zu überprüfen.

Streitig gestellt von den Fraktionen der SPD und DIE LINKE.

4. Die Enquete-Kommission hält einen strafrechtlichen Schutz nicht-körperlicher Daten in der Informationsgesellschaft für ebenso geboten wie den strafrechtlichen Schutz von Sachen. Sofern Daten weder dem Schutzbereich der Diebstahlsdelikte gemäß §§ 242 ff. StGB noch der Hehlerei gemäß §§ 259 ff. StGB unterfallen, können gesetzliche Klarstellungen erforderlich sein.
   Das unbefugte Abgreifen fremder Daten und der missbräuchliche Einsatz fremder Daten ist derzeit nur in Teilbereichen strafrechtlich erfasst. Betrachtet man beispielsweise den florierenden Handel auf den weltweiten virtuellen Schwarzmärkten der Cyberkriminellen, sind die Verkäufer/Käufer missbräuchlich erlangter Daten häufig weder die Täter, die die Daten zuvor ausgespäht haben, noch diejenigen, die sie später betrügerisch einsetzen (beziehungsweise dies ist ihnen nicht nachzuweisen). Diese Weitergabe rechtswidrig erlangter Daten ist jedoch bisher nicht strafbar.
   Die Enquete-Kommission fordert daher die Bundesregierung auf, etwa bestehende Strafbarkeitslücken in diesem Bereich zu schließen.

5. Die Enquete-Kommission begrüßt die bisher bei Banken und Kreditkarten-unternehmen und im Online-Banking vorgenommenen Maßnahmen zur Eigensicherung, die im Falle eines (unbemerkten) Ausspähens von Kreditkarten- oder aber Bankdaten eine unmittelbare Überprüfung von vorgenommenen Buchungen beim Inhaber erlauben. Sie tragen in erheblicher Weise zur Begrenzung von volkswirtschaftlichen Schäden und zur Reduzierung der Attraktivität eines Diebstahls von Bank- und/oder Kreditkartendaten sowie bei der Sicherheit des Onlinebanking bei und sollten daher weiter ausgebaut und verfeinert werden. Angesichts der aktuellen Warnungen vor Angriffen beim mobilen Onlinebanking empfiehlt die Enquete-Kommission der Bundesregierung, vergleichbare Initiativen wie beispielsweise zum Cloud Computing durchzuführen, um eine deutliche Stärkung und Sensibilisierung der Öffentlichkeit zu erreichen und um auf mögliche Risiken und entsprechende Schutzmöglichkeiten aufmerksam zu machen.

6. Die Enquete-Kommission empfiehlt der Bundesregierung im Dialog mit der betroffenen Wirtschaftsbranche zu prüfen, ob es negative Auswirkungen aufgrund des §202c StGB für die Überprüfung von Sicherheitslücken in Computersystemen gibt und die Vorschrift entsprechend gegebenenfalls anzupassen.[843]

[843] Siehe hierzu auch den Vorschlag „Streichung von §202c StGB („Hackertoolverbot“)“ aus der Online-Beteiligungsplattform. Siehe hierzu: Kapitel V

Ergänzende Handlungsempfehlungen der Fraktionen der SPD und BÜNDNIS 90/DIE GRÜNEN und der Sachverständigen Alvar Freude, Constanze Kurz, Prof. Dr. Wolfgang Schulz, Lothar Schröder, Cornelia Tausch

zum Kapitel „Kriminalität im Internet“

Evaluierung von Eingriffsbefugnissen

In einem Sondervotum des Berichtes „Datenschutz, Persönlichkeitsrechte“ der Enquete-Kommission Internet und digitale Gesellschaft[844] haben die Oppositionsfraktionen und einige der von ihnen benannten Sachverständigen dem Deutschen Bundestag empfohlen, „die bestehenden Aufgaben und Befugnisse von Sicherheitsbehörden und Diensten, die mit Grundrechtseingriffen verbunden sind, umfassend hinsichtlich ihrer Notwendigkeit, Wirksamkeit und Effizienz sowie ihrer grundrechtswahrenden Funktion unabhängig, auf wissenschaftlicher Grundlage und ergebnisoffen zu evaluieren.“ Dies ist insbesondere mit Blick auf die verdeckten Ermittlungsmaßnahmen und auf so weitreichende Eingriffe wie Quellen-Telekommunikationsüberwachung und Online-Durchsuchung zwingend geboten. Zwar bestehen in zahlreichen Gesetzen, beispielsweise im BKA-Gesetz in Bezug auf die Online-Durchsuchung, bereits Evaluierungsvorschriften, die jedoch in der Umsetzung diesen Ansprüchen zumeist nicht genügen.

– Die Enquete-Kommission bekräftigt diese Empfehlung und empfiehlt dem Bundestag, eine diesen Ansprüchen genügende Evaluation zur Notwendigkeit, Wirksamkeit und Effizienz insbesondere der Online-Durchsuchung und der Quellen-Telekommunikationsüberwachung vorzunehmen.

– Die Enquete-Kommission empfiehlt darüber hinaus im Rahmen dieser Evaluation, zu prüfen, ob – angesichts der technischen wie auch der rechtlichen Entwicklungen - der Kernbereich privater Lebensgestaltung unter den digitalen Bedingungen noch ausreichend geschützt ist oder ob es hier weiterer gesetzlicher Absicherungen bedarf.

– Die Enquete-Kommission fordert darüber hinaus, sicherzustellen, dass das verfassungsrechtliche Trennungsgebot zwischen Polizeien und Nachrichtendiensten

[844] [844] Bericht der Projektgruppe Datenschutz, Persönlichkeitsrechte der Enquete-Kommission Internet und digitale Gesellschaft. 15. März 2012. Drucksache 17/8999. Online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zwischenberichte/Zwischenbericht_Datenschutz_1708999.pdf.

zwingend gewahrt bleibt. Dies muss auch bei Kooperationen zwischen Behörden sichergestellt sein.

Evaluation der bestehenden Straftatbestände

Im Bereich der Internetkriminalität kann festgestellt werden, dass der Modus Operandi größtenteils schon aus konventionellen Kommunikationsmitteln bekannt ist. So haben sich die Straftaten- vornehmlich aus dem Betrugsbereich- nicht wesentlich geändert.[845] Spezifische Cybercrime-Delikte, beispielsweise Identitätsdiebstahl oder digitale Schutzgelderpressung werden heute größtenteils durch die Strafrechtsnormen im Bereich der Datendelikte (§§ 202 a bis c, 303, 303 b, 263 a, 261 a StGB) erfasst. Eine valide Darstellung der Steigerungsraten dieser Delikte ist aufgrund des zum Teil großen Dunkelfeldes, der zum Teil nicht entdeckten Taten sowie der häufig vorhandenen Verkettung von Straftaten (siehe „Phishing“) schwierig und oftmals fehlerbehaftet. Dennoch kann prognostiziert werden, dass sich mit der weiter fortschreitenden Technisierung der Gesellschaft auch in den kommenden Jahren immer mehr Erscheinungsformen von Kriminalität ins Internet verlagern oder dort entstehen werden.[846]

- Die Enquete-Kommission empfiehlt vor dem Hintergrund der Dynamisierung der Technik Evaluationen der bestehenden Straftatbestände und des entsprechenden Anpassungsbedarfs im weiteren gesetzgeberischen Verfahren.

Evaluation des „Hackerparagraphen“[847]

Bei der Verabschiedung des Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität und der Neufassung des § 202 StGB gab es erhebliche Bedenken dahingehend, dass es hierdurch zukünftig sehr problematisch sein werde, Sicherheitslücken in IT-Systemen von Unternehmen aufzuspüren, ohne sich dabei strafbar zu machen oder zumindest in die Gefahr geraten, das Gesetz zu übertreten. Der Umgang mit sogenannten "Dual use"-Programmen wurde als nicht hinreichend klar geregelt gesehen. In diesem Zusammenhang wurde eine erhebliche Beeinträchtigung der Sicherheit von Computersystemen befürchtet. Da sich ein Antrag auf Erlass eines Durchsuchungsbeschlusses leicht auf die Strafnorm stützen lässt, wurde weiterhin befürchtet, dass es vermehrt zu Durchsuchungen in der IT-Branche kommen könnte. Verbände, Vereine sowie Unternehmen

[845] Vgl. Stellungnahme Manske, S. 1.

[846] Vgl. Stellungnahme Manske, S. 3.

[847] Siehe hierzu auch den Vorschlag „Streichung von §202c StGB („Hackertoolverbot“)“ aus der Online-Beteiligungsplattform. Siehe hierzu: Kapitel V

der IT-Sicherheitsbranche haben vor, während und nach der Änderung der Norm auf ihre gravierenden Bedenken hingewiesen.[848]

Klärung brachte erst eine schriftliche Erörterung durch das Bundesverfassungsgericht, die deutlich macht, dass die Norm teilweise ihr Ziel verfehlt. Der Anwendungsbereich wird folglich durch das Gericht beschränkt.[849]

Die Strafrechtsänderung ist gesetzestechnisch problematisch und schafft durch den rechtlichen Wortlaut der weit auslegbar gefassten Rechtsnorm Unklarheit und dadurch Unsicherheit bei Unternehmen, Universtäten und Mitarbeiterinnen und Mitarbeitern im Bereich IT-Sicherheit. Es gilt für die Zukunft zu verhindern, dass die Strafnorm weiterhin als Risiko für IT-Firmen und deren Mitarbeiter, aber auch für Technikjournalisten gesehen wird. Ein Rechtfertigungszwang für den Einsatz und die Entwicklung von Software, nur weil sie auch von Kriminellen verwendet wird, sollte in Zukunft wegen der kontraproduktiven Wirkung auf die IT-Sicherheit vermieden werden. Dass IT-Sicherheitsexperten wegen der entstandenen gesetzlichen Unsicherheit Deutschland meiden, sollte durch eine präzisere Formulierung der Norm verhindert werden.

Die Enquete-Kommission empfiehlt daher,

– im Rahmen der Evaluation der Straftatbestände auch die Auswirkungen der Neufassung des § 202 a StGB auf die Überprüfungsmöglichkeiten von Sicherheitslücken in Computersystemen und gegebenfalls notwendige Änderungen zu überprüfen und bei der Überarbeitung der Norm auf die Bestrafung des bloßen Umgangs mit Computerprogrammen zu verzichten.

Quellen-Telekommunikationsüberwachung

Der Einsatz von Software zur Überwachung der Telekommunikation am Rechner (Quellen-Telekommunikationsüberwachung) stellt einen sehr weitgehenden Grundrechtseingriff dar, der aus datenschutzrechtlicher und bürgerrechtlicher Sicht überaus problematisch ist. Derart intensive Grundrechtseingriffe können angesichts mangelnder ausreichend klarer und eindeutig formulierter bereichsspezifischer Rechtsgrundlage, die den Anforderungen, die das Bundesverfassungsgericht zu den genannten Eingriffsmaßnahmen formuliert hat, nicht

[848] Stellungnahme des CCC Stellungnahme anläßlich der Verfassungsbeschwerde gegen den § 202c StGB: Derzeitige und zukünftige Auswirkungen der Strafrechtsänderung auf die Computersicherheit: https://erdgeist.org/archive/46halbe/202output.pdf.

[849] 2 BvR 2233/07, 1151/08 und 1524/08: http://www.bundesverfassungsgericht.de/entscheidungen/rk20090518_2bvr223307.html

verfassungsgemäß vorgenommen werden.[850] Solange aber die Einzelheiten einer Maßnahme nicht geregelt sind, kann § 20 1 II BKAG nicht als Vorbild dienen.[851]

– Unabhängig von der Frage, dass die Einsicht in den Quelltext entsprechender Überwachungssoftware unverzichtbar für die Überprüfung der Funktionalität ist und unabhängig von der Frage, ob es möglich ist, technischen und rechtlichen Absicherungen verfassungskonform sicherzustellen sowie die Funktionalitäten der Software für die Quellen-Telekommunikationsüberwachung auf allen Ebenen wirksam auf die Funktionalität einer Telekommunikationsüberwachung einzuschränken, ist die geltende Regelung des § 100 a StPO keine hinreichende Rechtsgrundlage, weil sie eine Beeinträchtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht ausreichend berücksichtigt. Zudem enthält diese Vorschrift keine Schutzvorkehrungen, um rechtlich und technisch sicherzustellen, dass die Überwachung nur die laufende Telekommunikation erfassen würde. Dazu müssten Bestimmungen in § 100 a StPO Eingang finden, die der erhöhten Eingriffsintensität und den technischen Besonderheiten der Quellen-TKÜ gerecht werden. Darüber hinaus müsste eine Überprüfung des Quellcodes vor, während und nach entsprechenden Einsätzen durch die berechtigten Stellen ermöglicht werden.

Export von Überwachungssoftware beschränken

Die Ausfuhr von Überwachungs- und Spähsoftware unterliegt nach derzeitigem Recht in Deutschland keiner Genehmigungspflicht. Sie ist nur dann ausfuhrgenehmigungspflichtig, wenn sie von den Vorgaben für „Güter mit doppeltem Verwendungszweck“ (Dual-Use) oder „als besonders entwickelt für militärische Zwecke“ entsprechend der Außenwirtschaftsverordnung erfasst werden. Exportgenehmigungen werden dann nur bei dem hinreichenden Verdacht des Missbrauchs zur inneren Repression oder zu sonstigen fortdauernden und systematischen Menschenrechtsverletzungen verweigert. In der Praxis laufen die bestehenden Regelungen jedoch leer.

Die Enquete-Kommission Internet und digitale Gesellschaft empfiehlt derm Deutschen Bundestag, die Ausfuhrmöglichkeiten für Überwachungssoftware- und Spähsoftware sowohl auf deutscher als auch auf europäischer und internationaler Ebene drastisch zu beschränken und durch gesetzliche Ausfuhrbeschränkungen sicherzustellen, dass derartige Techniken nicht

[850] Vgl. dazu K&R 11/2011.

[851] Vgl. dazu K&R 11/2011.

in Länder geliefert werden , in denen fortdauernd und systematisch Menschenrechtsverletzungen begangen werden. Dem Deutschen Bundestag ist regelmäßig über Veränderungen der Ausfuhrbeschränkungen und über entsprechende Ausfuhrgenehmigungen zu unterrichten.

Transparenz von Forschung und Entwicklung von Überwachungssoftware

Die Enquete-Kommission Internet und digitale Gesellschaft fordert die Bundesregierung auf, in Öffentlichkeit in geeigneter Weise über die Forschung und Entwicklung von Überwachungssoftware und mit dieser verwandte Technik, insbesondere mit Blick auf deren Zielsetzungen und die vorgesehenen Funktionalitäten, sowie die damit verbundenen Kosten zu informieren. Das Sicherheitsforschungsprogramm ist dahingehend zu evaluieren, ob und inwieweit die Zielsetzungen der Forschungs- und Entwicklungsvorhaben erreicht und welche Maßnahmen zum Grundrechtsschutz dabei getroffen wurden. Die Evaluation ist dem Deutschen Bundestag vorzulegen.

EU-Forschungsprogramm INDECT

Bei „INDECT“ handelt es sich um ein Forschungsprojekt im Rahmen des 7. Forschungsrahmenprogramms der EU, Fördergeber ist die Europäische Union, vertreten durch die Europäische Kommission. Ein zentrales Ziel des INDECT-Projektes ist die intelligente Verarbeitung von Informationen und das automatische Erkennen von Bedrohungen, abnormalen Verhaltens oder Gewalt. Dabei geht es um die Entwicklung einer Plattform zur Erfassung und zum Austausch operationeller Daten, das heißt von Aufnahmen intelligenter Videokameras zur Aufdeckung von Gefahren, die insbesondere von Terrorismus und Schwerverbrechen ausgehen. Der EU-Zuschuss für das INDECT-Projekt beträgt 10,9 Millionen Euro. Für die Gewährung der Finanzhilfen werden die zur Förderung ausgewählten Projekte einer ethischen Prüfung unterzogen. Diese ethische Prüfung auf europäischer Ebene kam zu dem Ergebnis, dass das Projekt förderfähig sei.

Die Enquete-Kommission stellt fest, dass diese Ziele des Forschungsprojektes kaum mit europäischen und deutschen Grundrechten in Einklang gebracht werden kann und auch den Datenschutzvorgaben auf deutscher und europäischer Ebene diametral zuwiderlaufen. Aus diesen Grund spricht sich die Enquete-Kommission Internet und digitale Gesellschaft in aller Deutlichkeit gegen die Entwicklung und den Einsatz derartiger Technologien aus und fordert die Bundesregierung auf,

1. dieses und ähnliche EU-Forschungsvorhaben nicht weiter zu unterstützen und eine deutsche Beteiligung daran auszuschließen;

2. sich auf europäischer Ebene dafür einzusetzen, dass derartige Forschungsprojekte nicht fortgeführt und auch nicht finanziell gefördert werden;

3. den Fortgang des Forschungsprojektes aufmerksam zu verfolgen und die Ergebnisse fortlaufend hinsichtlich ihrer Vereinbarkeit mit deutschen und europäischen Grundrechten zu überprüfen.

Sensibilisierungskampagnen starten

Angesichts der aktuellen Warnungen vor Angriffen beim mobilen Onlinebanking appelliert die Enquete-Kommission dringend an die Wirtschaft, die IT-Sicherheit entscheidend zu verbessern. Darüber hinaus empfiehlt die Enquete-Kommission dem Deutschen Bundestag, die Bundesregierung aufzufordern, neben der Überprüfung von rechtlichen Ergänzungen zur Verbesserung IT-Sicherheit – vergleichbar mit vergleichbaren Initiativen beispielsweise beim Cloud Computing - eine deutliche Stärkung von Sensibilisierungskampagnen der Öffentlichkeit, um auf diese Risiken und die entsprechenden Schutzmöglichkeiten aufmerksam zu machen.

Ergänzende Handlungsempfehlungen der Fraktion DIE LINKE.

zum Kapitel „Kriminalität im Internet“

Thema Staatstrojaner

Die Enquetekommission empfiehlt der Bundesregierung

- den Kernbereich privater Lebensgestaltung unter den digitalen Bedingungen stärker gesetzlich zu schützen,
- die Befugnis der Ermittlungsbehörden der Länder zu Online-Durchsuchungen aufzuheben und gänzlich darauf zu verzichten, informationstechnische Systeme mittels Infiltration zu durchsuchen,
- den Quellcode der Trojaner, die im Rahmen der Quellen-TKÜs verwendet wurden, zu veröffentlichen sowie für künftige Einsätze den Quellcode für die Prüfung vor, während und nach dem Einsatz durch die berechtigten Stellen zu ermöglichen,
- Infiltrationen von informationstechnischen Systemen ohne spezifische gesetzliche Grundlage und wirksame technische Prüfung zukünftig zu unterlassen,
- die Befugnis des Bundeskriminalamts zum verdeckten Eingriff in informationstechnische Systeme (§20k des Bundeskriminalamtgesetzes) und zur Verwendung und Übermittlung solcher Daten (§ 20v BKAG) aufzuheben,
- die Öffentlichkeit in transparenter Weise über die finanzielle Förderung und Erforschung und die Anschaffungskosten von Spionage- und Überwachungssoftware sowie verwandter Technik zu informieren. Zu diesem Zweck sollen auch das Sicherheitsforschungsprogramm der Bundesregierung und die Tätigkeit der neu geschaffenen, verfassungsrechtlich problematischen Gremien wie „Nationales Cyber-Abwehrzentrum“ und Nationaler Cyber-Sicherheitsrat transparenter gestaltet und einer wirksamen unabhängigen Kontrolle unterworfen werden.
- in wirksamer Weise dafür zu sorgen, dass deutsche Firmen keine Überwachungstechnik an autoritäre und undemokratische Regime verkaufen, entsprechende Überwachungstechnik Rüstungsgütern gleichzusetzen, ihre Ausfuhr entsprechend zu regeln und darüber dem Parlament zu berichten.

Thema Cybersicherheit

Der Begriff Sicherheit hat in den letzten Jahren einen schleichenden Bedeutungswandel erfahren. Traditionell ist die Schutzpflicht des Staates für seine Bürger im Sinne einer social security verstanden worden, also einer Schutzverpflichtung im Sinne existentieller, kultureller

und sozialer Existenzsicherung. Dieser bürgerzentrierte Schutzgedanke ist in den letzten Jahren jedoch zunehmend von einem militärischen Sicherheitsbegriff verdrängt worden. Seit es den „Krieg gegen den Terror“ gibt, ist die Gefahrenabwehr als Paradigma der Sicherheitspolitik auf immer weitere, zunehmend auch auf zivilgesellschaftliche Bereiche ausgedehnt worden. Im digitalen Zeitalter betrifft dieses Denken auch die Netze, also die zentrale Kommunikationsinfrastruktur der modernen Gesellschaft. Das ist umso erstaunlicher, als in vernetzten Strukturen die klassischen Abwehrmechanismen zunehmend versagen müssen.

Wenn Angriffe potenziell von jedem Internetcafé aus geführt werden können, kann man noch so viel Geld in Hochtechnologie zur Abwehr solcher Gefahren investieren: Wenn nur ein kleiner Prozentteil aller Angriffe erfolgreich ist, waren alle Gegenmaßnahmen umsonst. Man müsste, um sicherzugehen, die Kommunikation eines jeden einzelnen Bürgers überwachen, da jeder Einzelne eine potenzielle Gefahrenquelle ist, sofern er Zugang zu Informationstechnologie hat. Tatsächlich gehen staatliche Strategien zur Bekämpfung von Gefahren aus dem Cyberspace immer mehr in diese Richtung, wie der zunehmende Einsatz von Überwachungstechnologie gegen die eigene Bevölkerung in vielen autoritären Staaten zeigt. In Deutschland sind solche Maßnahmen bislang auf den Bereich der inneren Sicherheit beschränkt geblieben, zumindest was den Einsatz des sogenannten Staatstrojaners oder die massenhafte Abfrage der Handydaten von Demonstrationsteilnehmern in verschiedenen deutschen Städten angeht. Es gibt jedoch keinerlei Garantie dafür, dass solche schon im Hinblick auf die innere Sicherheit inakzeptable Maßnahmen nicht auch zu militärischen Zwecken eingesetzt werden. Hier ist dringend ein Umdenken gefordert.

Vor diesem Hintergrund empfiehlt die Enquete der Bundesregierung die Beachtung folgender Punkte:

- anzuerkennen, dass einer Bedrohung, die potenziell von jedem beliebigen Rechner der Welt ausgehen kann, nicht mit den klassischen Abwehrstrategien begegnet werden kann. Die Gründung von Cyberabwehrzentren verfehlt ihr Ziel ebenso wie der Versuch, das Angriffsverhalten durch Strafandrohung zu beeinflussen (präventive Abwehr).
- die Verteidigungsstrategie im Cyberspace an dessen reale Gegebenheiten anzupassen. Dies bedeutet, in erster Linie für einen verlässlichen Schutz kritischer Infrastruktur zu sorgen (Krankenhäuser, Energieversorgung etc.). Hierfür ist eine Entkoppelung der Systeme nötig, die es verunmöglicht, von beliebigen Punkten aus Angriffe durchzuführen, die potenziell die gesamte Struktur bedrohen. Insbesondere sollten kritische

Infrastrukturen nicht mit dem öffentlich zugänglichen Teil des Internets verbunden sein. Die Anforderungen an die Netzwerksicherheit müssen umso höher sein, je wichtiger der Schutz der Infrastruktur aus zivilgesellschaftlicher Sicht ist. Im Zweifel ist dem zivilgesellschaftlichen Sicherheitsbedürfnis Vorrang vor den Profitinteressen der Geräteindustrie einzuräumen, die derzeit eine zunehmende Vernetzung solcher Infrastrukturen anstrebt.

– Das verfassungsrechtliche Trennungsgebot zwischen Nachrichtendiensten, Polizei und Militär ist zwingend zu beachten. Dies muss auch für Kooperationen gelten, etwa im Rahmen eines Cyberabwehrzentrums und ähnlicher Einrichtungen.
– Die vom AK Kritis des Bundesministerium des Inneren gehandhabte Definition der Kritischen Infrastrukturen (KRITIS) sollte nicht in einer Weise ausgeweitet werden, die befürchten lässt, dass es durch eine solche Neudefinition zu einer unverhältnismäßigen Einschränkungen von Grundrechten kommen kann. Vielmehr sollte der Begriff der kritischen Infrastrukturen möglichst eng gefasst sein und sich an dem konkreten Schutzziel einer Sicherung der existenziellen Bedürfnisse der Bevölkerung orientieren.
– Auch im Rahmen einer Neudefinition kritischer Infrastrukturen darf es zu keiner Vermischung des Schutzes ziviler kritischer Infrastrukturen mit Strategien zur militärischen Cybersicherheit kommen. - Forschungsgelder, die für zivile Zwecke bestimmt sind, dürfen nicht unter der Hand für militärische Zwecke benutzt werden. Eine klare Trennung beider Bereiche ist hier geboten. Der Forschungsetat des Bundes darf nicht zur Förderung von High-Tech-Projekten eingesetzt werden, die letztlich primär militärischen Zwecken dienen.
– Der Kampf gegen den Terror darf nicht als Vorwand für die zunehmende Überwachung ziviler Infrastruktur missbraucht werden. Insbesondere ist eine militärische Überwachung der Kommunikationsinfrastruktur auszuschließen. Innere und äußere Sicherheit müssen klar getrennt bleiben.
– Forschungsprogramme wie INDECT, die darauf abzielen, möglicherweise kriminelles Verhalten von Individuen bereits im Vorfeld vorauszusagen und ggf. präventiv zu bekämpfen, sind als voraufklärerischer Gnostizismus zu verwerfen.
– Anbieter von Cloud-Diensten sollten verpflichtet werden, ihre Kunden über erkannte Angriffe umfassend zu informieren. Gerade Clouds stellen für Angreifer attraktive Ziele dar, da hier nicht nur die Daten eines einzelnen Unternehmens, sondern eine Vielzahl unterschiedlicher Informationen zu bekommen sind. Umso wichtiger ist es, dass die

Betroffenen über IT-Sicherheitsprobleme ihres jeweiligen Dienstleisters umfassend informiert werden.

- Die Bundesregierung sollte sich auf EU-Ebene dafür einsetzen, dass unzureichende IT-Sicherheit, die zu Cyberspionage führen kann, mit Sanktionen belegt wird. Zu denken ist hier beispielsweise an Haftungsregelungen und Strafzahlungen mit Bezug zum Schaden.
- Dem grauen Markt sollte das Geld entzogen werden: Die Kunden von Exploits, die unerkannte Schwachstellen ausnutzen, sind heutzutage überwiegend Staaten. Die Aufrüstung für staatsterroristische Akte hat zu einem erheblichen Anstieg der Preise geführt, die für Zero Day Exploits gezahlt werden. Dieses Geld sollte eher in die Entwicklung besserer IT-Sicherheit investiert werden.
- Die GSM-Verschlüsselung kann nicht mehr als sicher betrachtet werden, seit sie 2009 geknackt wurde. Mittlerweile steht für den Einbruch in die Privatsphäre der Nutzer von Mobiltelefonen einfache Software zur Verfügung. Die Bundesregierung sollte sich bei der GSM Association für ein sicheres Verschlüsselungsverfahren einsetzen.
- Für erkannte Angriffe auf die IT- Sicherheit von Unternehmen und staatlichen Einrichtungen sollte es eine Meldepflicht geben. Insbesondere Angriffe auf kritische Infrastruktur sind unverzüglich zu dokumentieren.
- Im Bereich der IT-Sicherheit herrscht ein Mangel an Fachkräften. Forschung und Ausbildung in den Bereichen Informatik, Mechatronik und Wirtschaftsinformatik müssen dringend verbessert werden.
- Hacking, das keine kriminellen Zwecke verfolgt, sondern darauf abzielt, die öffentliche Aufmerksamkeit für Gefahren mangelhafter IT-Sicherheit zu sensibilisieren, muss konsequent entkriminalisiert werden.

IV. Sondervoten

V. Dokumentation der Beteiligung der interessierten Öffentlichkeit an der Arbeit der Projektgruppe über die Online-Beteiligungsplattform enquetebeteiligung.de

Interessierte Bürgerinnen und Bürger konnten als „18. Sachverständige“ über die Online-Beteiligungsplattform *enquetebeteiligung.de* an der Arbeit der Projektgruppe Zugang, Struktur und Sicherheit im Netz mitwirken.

Mit Einrichtung der Projektgruppenseite[852] auf *enquetebeteiligung.de* im April 2011 hat der Vorsitzende dazu aufgerufen, über die Plattform handlungsorientierte Fragestellungen mit Erläuterung einzureichen, die von der Projektgruppe bearbeitet werden sollten. Zusätzlich hat er im August 2011 in einem Beitrag im Blog der Enquete-Kommission auf die Möglichkeit hingewiesen, sich an der Erstellung des Arbeitsprogrammes der Projektgruppe zu beteiligen.

Zur konstituierenden und ersten Sitzung am 5. September 2011 lagen den Mitgliedern neun Beiträge aus der interessierten Öffentlichkeit vor (3 Themenvorschläge für das Arbeitsprogramm, 6 Handlungsempfehlungen). Diese konnten in die sechs von der Projektgruppe identifizierten Themenfelder (für den Bereich Zugang und Struktur: Ausbau und Modernisierung der Netze, Wettbewerb; für den Bereich Sicherheit: Schutz kritischer Infrastrukturen im Internet, Kriminalität im Internet, Spionage, Sabotage) eingeordnet werden.

Im Anschluss an die erste Sitzung wurde auf der Online-Beteiligungsplattform das Arbeitsprogramm der Projektgruppe veröffentlicht. Die Bürgerinnen und Bürger waren nun aufgefordert, auf Basis des Arbeitsprogrammes eigene Ideen und Vorschläge zu den Themenfeldern einzubringen.

Vor der parlamentarischen Sommerpause 2012 lagen insgesamt 20 Beiträge aus der interessierten Öffentlichkeit vor (3 Themenvorschläge für das Arbeitsprogramm, 15 Handlungsempfehlungen, 1themenfremder Beitrag, 1 Textbeitrag einer Fraktion). Die Mitglieder haben die Beiträge in der Sitzung vom 11. Juni 2012 gesichtet und geprüft, ob alle darin angesprochenen Themen Eingang in den Bericht gefunden haben. Die Themen des Berichtes spiegeln sich in allen Beiträgen wider. Über die Sommerpause wurden die Bürgerinnen und Bürger aufgefordert, weitere Handlungsempfehlungen vorzuschlagen. Daraufhin kamen ein weiterer Themenvorschlag für das Arbeitsprogramm sowie eine weitere Handlungsempfehlung hinzu.

---

[852] Siehe hierzu: https://zugang.enquetebeteiligung.de/instance/zugang

Nachdem die Projektgruppe die Bestandsaufnahme im Oktober 2012 nahezu abgeschlossen hatte, wurden die bis dahin konsensualen Texte auf der Online-Beteiligungsplattform veröffentlicht.

Über den Zeitraum von Anfang November 2012 bis Ende Dezember 2012 waren die Bürgerinnen und Bürger noch einmal eingeladen, sich an der Formulierung von Handlungsempfehlungen auf *enquetebeteiligung.de* zu beteiligen. Innerhalb des genannten Zeitraumes sind keine weiteren Vorschläge aus der Öffentlichkeit eingegangen, wenngleich sich die Stimmenverteilung der bereits eingereichten Handlungsempfehlungen während dieser Zeitspanne leicht verändert hat.

Die Mitglieder der Projektgruppe haben in der Sitzung vom 22. Oktober 2012 einstimmig beschlossen, die eingegangenen Vorschläge der Bürgerinnen und Bürger inklusive der Stimmenverhältnisse im hier vorliegenden Bericht der Projektgruppe abzubilden. Lediglich der themenfremde Beitrag sowie der Textbeitrag einer Fraktion werden nicht aufgenommen. Im Vergleich zur Anzahl eingereichter Vorschläge der anderen Enquete-Projektgruppen kann die Beteiligung an der Arbeit der Projektgruppe Zugang, Struktur und Sicherheit im Netz mit 20 themenrelevanten Beiträgen zu der komplexen Themenstellung als durchaus positiv bewertet werden.

Zu den insgesamt 22 Vorschlägen sind 24 Kommentare eingegangen. Für den Bereich der Projektgruppe auf der Online-Beteiligungsplattform haben sich 113 Mitglieder registriert. Von diesen haben 8 Mitglieder Anregungen zum Arbeitsprogramm beziehungsweise Handlungsempfehlungen eingereicht. Die Beiträge haben 115 Bewertungen erhalten.

Über die Sitzungstermine der Projektgruppe wurden die Bürgerinnen und Bürger sowohl über die Terminfunktion der Online-Beteiligungsplattform als auch über die Internetseite der Enquete-Kommission[853] informiert. Hier wurde auch aus den stets öffentlichen Sitzungen der Projektgruppe berichtet. Auf die Veröffentlichung der Projektgruppenberichte wurde per Twitter hingewiesen.

Der Vorsitzende und die Mitglieder der Projektgruppe Zugang, Struktur und Sicherheit im Netz bedanken sich bei allen, die sich in die Projektgruppenarbeit eingebracht haben.

Die Vorschläge werden nach der größten Unterstützung sortiert. Sie wurden redaktionell nicht bearbeitet. Die hinzugefügten Kommentare werden nicht abgebildet.

---

[853] Siehe hierzu: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/index.jsp

Vorschlag	Ja : Nein
Anbieter zur Verwendung von sicheren Verbindungen verpflichten? Sollten Anbieter zur Verwendung von sicheren Verbindungen, beispielsweise bei der Übertragung von personenbezogenen Daten, verpflichtet werden, um das Ausspähen von sensiblen Daten zu verhindern? Grund: Viele Anbieter bieten momentan keine Möglichkeit sichere Verbindungen wie z.B. HTTPS zu Verwenden und zwingen die Nutzer so zur unsicheren Übertragung ihrer Daten. *Angelegt von mx880 am 15. Mai 2011* https://enquetebeteiligung.de/d/709 *Dieser Beitrag wurde als Themenvorschlag für das Arbeitsprogramm gewertet.*	14 : 1
Streichung von §202c StGB („Hackertoolverbot“) Vorschlag: Ersatzlose Streichung von §202c StGB. Begründung: Privatpersonen und Freiberufler oder mittelständische Unternehmen die nicht auf IT-Sicherheit spezialisiert sind können oft nur schwer glaubhaft machen, sich von §202c erfasste Hilfsmittel nicht zur Vorbereitung illegaler Handlungen beschafft/hergestellt zu haben - obwohl es hierfür viele andere legitime Gründe gibt (z.B. Sicherheitstests eigener Computersysteme/Websites, Weiterbildung im Bereich IT-Sicherheit, wissenschaftliches Interesse). Ohnehin ist dieses Gesetz zur Bekämpfung von Computerkriminalität unnötig, da Beihilfe zu Vergehen nach §§ 202a und 202b bereits strafbar ist (was sämtliche böswilligen/schädlichen Fälle von §202c abdeckt). *Angelegt von Autolykos am 27. Juni 2011* https://enquetebeteiligung.de/d/780 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	11 : 0
„Deep Packet Inspection“ verbieten Das Ablauschen von Kommunikationsinhalten sollte sowohl Internetunternehmen als auch dem Staat nicht erlaubt sein. Bilder, Texte oder Videos sollten nicht für einen Internetprovider voneinander unterscheidbar sein. Ein Mobilfunkunternehmen sollte kein VoIP verbieten dürfen, da es dazu den Inhalt mitlesen müsste, was technisch nicht ohne ein umfangreiches Überwachungssystem, welches VoIP-Verschleierungen erkennen würde,	8 : 0

Vorschlag	Ja : Nein
realisierbar wäre. *Angelegt von TAE am 8. Oktober 2011* https://enquetebeteiligung.de/d/943 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	
Universaldienst per Gesetz Förderprogramme und Technologie-Mix schaffen es nicht das Marktversagen aufzufangen. Der Bund hat jedoch nach Artikel 87f des Grundgesetzes zu gewährleisten, dass flächendeckend, angemessen und ausreichend Dienstleistungen der Telekommunikation angeboten werden. Das TKG bietet hier keine ausreichende Definition, der Bundesverband gegen digitale Spaltung -geteilt.de- e.V. hat hierzu bereits eine Stellungnahme in die Novellierung des TKG eingebacht. http://www.geteilt.de/forum/viewtopic.php?f=47&t=10531 Die Enquete Kommission sollte sich intensiv mit diesem Thema auseinandersetzen und hierbei die technische Entwicklung im Auge behalten, Begriffsdefinition und Anforderungsprofil an einen Breitbandanschluss müssen anhand folgender Merkmale bewertet diskutiert werden: -Download- und Uploadgeschwindigkeit, -Latenzzeit, -Verfügbarkeit, -Datenvolumen, -Drosselung, -sonstige Merkmale/Einschränkungen(Netzneutralität) *Angelegt von spokesman am 1. September 2011* https://enquetebeteiligung.de/d/889 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	7 : 0
Die Rolle des Staates als Internetnutzer Vorschlag: Die Enquete-Kommission möge ermitteln in welchem Umfang der Staat selbst Internetnutzer und -dienstleistungsanbieter ist. Welche behördlichen Vorgänge finden online statt, welche benötigen zwingend das Internet? Wie begegnet man den speziellen Schutzanforderungen dieser vertraulichen Systeme? Wie kann ein Mißbrauch ausgeschlossen werden? Mit welchen Veränderungen ist in der nahen Zukunft zu rechnen? *Angelegt von cschoen am 25. April 2011* https://enquetebeteiligung.de/d/609 *Dieser Beitrag wurde ald Themenvorschlag für das Arbeitsprogramm gewertet.*	6 : 0

Vorschlag	Ja : Nein
Keine generelle Vorratsdatenspeicherung Ein Überwachungs- und Polizeistaat sollte verhindert werden, Bürgerrechte müssen gewahrt werden. Der Staat sollte nur die notwendigsten Informationen über den Bürger erhalten. Darum ist das Konzept der Vorratsdatenspeicherung, wie sie in der EU-Richtlinie steht, abzulehnen. Internetstraftaten, sei es Datenschutzverletzungen, wie z.B. die Intimsphäre verletzende Bilder, oder Urheberrechtsverletzungen, wie z.B. die illegale Verbreitung teurer Unternehmenssoftware, sollten verfolgt werden können. Bei einer Kommunikation zwischen zwei Bürgern sollte die Anklage nur von einem der Beteiligten ausgehen dürfen. Eine schlichte Verkürzung der Dauer der Vorratsdatenspeicherung ist der falsche Weg eine goldene Mitte zu finden, vielmehr sollte differenziert betrachtet werden, welche Daten gespeichert werden sollten. Dies sind ausschließlich die unverzichtbaren Zuordnungsdaten von IP-Adresse und Anschluss. Auch sollte diese Zuordnung nicht nur live, sondern auch noch Monate nach der Tat möglich sein, da diese nicht unbedingt wiederholt werden muss. Bewegungs- und Anrufprofile sind dafür abzulehnen. *Angelegt von von TAE am 27. September 2011* https://enquetebeteiligung.de/d/935 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	6 : 0
Handlungsempfehlung - Keine Pflicht zum Einsatz von Providerhardware Provider zwingen oft ihre Kunden eine bereitgestellte Hardware einzusetzen (Blackbox-Zwang). Diese bietet jedoch oft nur einen eingeschränkten Funktionsumfang und das Vorgehen behindert alternative Hardware-Anbieter im Wettbewerb. Damit beschäftigt sich inzwischen auch die Bundesnetzagentur (siehe Heise News Artikel) Daher sollte es Providern verboten werden, Kunden den Einsatz von Providerhardware vorzuschreiben. Außerdem sollten die Provider verpflichtet werden die Zugangsdaten herauszugeben (einige machen das jetzt ja auch schon freiwillig). *Angelegt von mx880 am 9. September 2012* https://enquetebeteiligung.de/d/1426 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	6 : 0
Hochleistungsnetze	3 : 0

Vorschlag	Ja : Nein
Heute die Weichen für Morgen stellen, ohne Verpflichtung keine Zielerfüllung. FTTH Netze sind in Deutschland noch als Fremdwort gehandelt, damit dies nicht länger so bleibt sind enorme Investitionen nötig. Es stellt sich die Frage in welcher Form die am Markt tätigen Unternehmen künftig ein flächendeckendes Glasfasernetz zur Sicherung der Daseinsvorsorge errichten wollen und können. Da bis heute keine andere Technologie zur Absicherung von Bandbreiten mit wenigen Mbit/s flächendeckend zur Verfügung steht, ist klar, dass eine Wettbewerbslösung kein flächendeckendes Glasfasernetz hervorbringen wird. Der Bundesverband Initiative gegen digitale Spaltung -geteilt.de- e.V. hat auch hier entsprechende Ideen in die Diskussion gebracht. Eine breit angelegte Diskussion über mögliche Realisierungswege sollte bereits mit kurzfristigen Maßnahmen den langfristigen Erfolg sichern. Die Weiterentwicklung der Informations- und Wissensgesellschaft wird künftig auf diese Hochleistungsnetze nicht verzichten können, neue Anwendungen und Dienste werden abhängig von diesen Netzen sein, die Schlussfolgerung wird auch hier eine Grundversorgung mit Anschlüssen an Hochleistungsnetze sein. *Angelegt von von spokesman am 1. September 2011* https://enquetebeteiligung.de/d/887 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	
Grundversorgung mit Informationsaustausch Jeder Bürger sollte sich informieren und andere informieren können. Umsetzungsvorschlag: Jeder Bürger sollte Anspruch auf einen Internetanschluss mit stetigen 25 Mbit/s in Download und Upload-Richtung haben. Die Latenzzeit zu dem weitentferntesten Server in Deutschland sollte unter 50 Millisekunden liegen. Der Kostenpunkt für den Bürger sollte nicht höher als 30 Euro im Monat betragen. Diese Kosten sollten auch zur Berechnung derLeistungen für die Grundsicherung herangezogen werden. *Angelegt von TAE am 17. September 2011* https://enquetebeteiligung.de/d/911 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	3 : 0
Pseudonymer Websitenaufruf User-Tracking ist ein großes Problem im WWW. Anhand von IP-Adresse,	4 : 0

Vorschlag	Ja : Nein
Browser-Agent, Cookies, Schriftarten, Auflösung und vielen mehr kann ein Zugriff auf eine Webseite einer Person zugeordnet werden. Diese Daten werden auch zwischen verschiedenen Websiten ausgetauscht. Damit können komplette Persönlichkeitsprofile erstellt werden, die angeben, wer wann was wo kauft, sagt, anschaut, tut. Dies muss auf jeden Fall verhindert werden. *Angelegt von TAE am 17. September 2011* https://enquetebeteiligung.de/d/919 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	
Diskriminierungsfreier Datentransport Der Internetzugang sollte nicht bestimmte Adressen nur auf Aufpreis erreichen dürfen. Angebote wie YouTube sollen von einem Internetprovider nicht künstlich gesperrt werden, um nachher gegen Aufpreis wieder freigestaltet werden zu können. Ein solches Angebot steht keinem realen Gut gegenüber und würde nur der ungerechtfertigten Profisteigerung von Internetproviderun dienen, die Lebensqualität der Menschen senken und große Anbieter wie YouTube unnötig diskriminieren und damit den Wettbewerb unnötig verzerren. Ebenfalls sollte ein bekannter Inhalte-Anbieter für den gleichen Internetzugang nicht mehr bezahlen müssen, nur weil er ein bekannter Inhalte-Anbieter ist. Er sollte die gleiche Leistung zu dem gleichen Preis erhalten, wie andere Inhalte-Anbieter auch. *Angelegt von TAE am 8. Oktober 2011* https://enquetebeteiligung.de/d/945 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	4 : 0
Systemische IT-Infrastrukturen, z.B. in der Finanzwelt, erfordern zeitgemäßere Analyseanforderungen bzgl. des Risikofaktors "Ausland" Alle Länder mit einer volumenstarken Finanzindustrie verfügen über systemische Kandidaten, die dem Risiko "Too Big To Fail" oder besonderen Gefahren wie "Spionage"- oder "Cyber War"-Relevanz unterliegen. Ein IT-Ausfall bei nur einem einzigen wichtigen Player, z.B. in der aktuellen heißen Phase der Euro-Krise, könnte das gesamte Euro- oder Welt-Finanzsystem zum Kollabieren bringen. Man könnte verführt sein zu sagen, dass deren IT für die Sicherheit des Landes schon wichtiger und ausfallkritischer ist als die des Militärs. Die laufende Risikoanalyse der IT ist sehr komplex geworden, insbesondere wenn	2 : 0

Vorschlag	Ja : Nein
besonders sicherheitskritische operationelle IT-Abläufe durch Outsourcing-Dienstleister faktisch im Ausland betrieben werden. Eine Beschränkung auf formelle IT-Compliance verdrängt zu leicht die wahren Gefahren, und reicht in Zeiten so nachhaltiger Interessenskonflikte zwischen den Ländern nicht mehr aus. Eine objektive und wirksame IT-Risikoanalyse systemischer IT erfordert die Einbindung des Risikofaktors "Ausland", z.B. durch die Einbindung des Korruptionswahrnehmungsindex. Eine zeitgemäße Inspiration für das Thema findet sich unter http://www.kes.info/archiv/online/EPIS2.html sowie http://www.kes.info/archiv/online/EPIS.html Vielleicht inspiriert Sie dies in Ihrer wichtigen staatlichen Aufgabe, den Bürgern IT-bezogen Sicherheit zu bieten. *Angelegt von DrFedtke am 1. Juli 2012* https://enquetebeteiligung.de/d/1394 *Dieser Beitrag wurde als Themenvorschlag für das Arbeitsprogramm gewertet.*	
Anonymität im Internet Anonyme Nutzer können im Internet Schaden anrichten, ohne zur Verantwortung gezogen zu werden, z.B. mit Vireneinspeisung oder Hacking. Anonyme Nutzung des Internets ist in manchen Bereichen eine wertvolle Methode, z.B. wenn gesellschaftlich relevante Positionen eingebracht werden sollen, aber der Nutzer Angst vor Repressionen hat. Die Frage lautet, wie einerseits berechtigte Interessen an Anonymität erfüllt werden können, anderseits aber das Internet vor anonymen Raudies geschützt werden kann. Kann die (internationale) Internet-Gemeinschaft dies selbst in die Hand nehmen oder müssen hier staatliche Kontrollen vorgesehen werden? *Angelegt von gschwtbg am 31. Mai 2011* https://enquetebeteiligung.de/d/742 *Dieser Beitrag wurde als Themenvorschlag für das Arbeitsprogramm gewertet.*	3 : 2
Meinungsfreiheit sichern Es sollte im Internet ein freies Meinungsforum geben, indem jeder anonym seine	1 : 0

Vorschlag	Ja : Nein
Meinung posten kann. Dieses wird von zufällig aus der Bevölkerung gewählten Freiwilligengruppe kontrolliert. Entscheidend, ob eine Meinung gegen z.B. das Persönlichkeitsrecht verstößt, tut nur die Gruppe. Die Freiwilligengruppe arbeitet vollkommen anonym. D.h. die einzelnen Kontroll-Bürger kennen sich nicht gegenseitig. Außerdem kann niemand sie kontrollieren. Sie sind nur ihrem Gewissen unterworfen. In dem öffentlichen Meinungsforum sollen ausschließlich Texte gepostet werden können. Jemand, der im Meinungsforum postet, kann in keinem Fall bestraft werden. Es ist aber möglich, einzuschränken wieviele Beiträge pro Internetanschluss am Tag gestellt werden können. Dies sollte aber nicht einfach zu verändern sein. Daneben sollte es noch ein Offline-Meinungsforum geben, in dem alle hier beschriebenen Vorgänge mit mechanischen Schreibmaschinen und Papier stattfinden. *Angelegt von TAE am 17. September 2011* https://enquetebeteiligung.de/d/909 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	
Wettbewerb bei Internetnetzen statt Wettbewerbsverhinderung durch anbietereigene TAL-Leitungen Der Wettbewerb sollte gefördert werden, indem die Teilnehmeranschlussleitung vom keinen Unternehmen, sondern vom Staat gelegt wird. Selbstverständlich bleibt es aber jedem Bürger frei neben dem staatlichen Angebot. *Angelegt von TAE am 17. September 2011* https://enquetebeteiligung.de/d/917 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	1 : 0
Pseudonymer Zugang zum Internet Im Internet sollten sich wieder Rechte durchsetzen lassen. Absolute Meinungsfreiheit sollte dabei jedoch auf jeden Fall gegeben sein. Verstöße gegen Datenschutz, Persönlichkeitsrechte, Verbraucherschutz, Marken- und Urheberrechte sollten sich aber durchsetzen lassen. Auch Denial-of-Service-Angriffe und andere Hackerangriffe sollten nachvollziehbar sein. Eine Überwachung von Inhalten wird dabei auf jeden Fall abgelehnt. Stattdessen geht der Beginn einer Ermittlung immer von einem Kläger aus, der freiwillig den Inhalt	1 : 0

der Nachricht vorlegt, welcher signiert sein sollte, sodass seine Echtheit überprüft werden kann. Dazu sollten alle IP-Pakete signiert werden.

Angelegt von TAE am 30. August 2011

https://enquetebeteiligung.de/d/881

Dieser Beitrag wurde als Handlungsempfehlunggewertet.

Textvorschlag:

Um Kriminalität im Internet zu bekämpfen, müssen zwei Dinge geklärt werden: 1. Die Täter müssen identifizierbar sein, 2. Die Täter müssen in Europa oder Partnerländern greifbar sein.

Jeder Internetbenutzer muss durch eine pseudonyme Adresse identifizierbar sein. Alle Pakete werden verschlüsselt. Dazu hat der Nutzer eine Identifikationskarte, ähnlich einer SIM-Karte. Auf dieser ist ein privater Schlüssel gespeichert, der staatlich signiert und entweder einer Person oder einer Wohnung zuordbar ist. Mit diesem wird in regelmäßigen Abständen, z.B. täglich, aus datenschutzrechtlichen Gründen eine neue pseudonyme Adresse samt einem für diesen zeitlichen Abstand und diese Adresse gültigen privaten Schlüssel beantragt. Über diese Adresse werden alle ausgehenden Pakete geschickt. Für eingehende Pakete oder für Server können auch statische Adressen genutzt werden.

Die Überwachung der Internetkommunikation sollte verboten werden und technisch nicht möglich sein, da die privaten Schlüssel der Kommunikation dem Staat nicht bekannt sein werden. Es sollte jedem Bürger freistehen, eine eigene Verschlüsselung zusätzlich zu verwenden.

Erhält der Empfänger nun Inhalte, welche dem Urheberrecht oder anderen Rechten widersprechen, kann er dies einfach nachweisen. Dazu klickt er beispielsweise mit der rechten Maustaste auf den Inhalt z.B. einer E-Mail, eines Dateitransfers oder einer Webseite und wählt im Kontextmenü "Beweis ausdrucken" aus. Anschließend wird ein Papier ausgedruckt, auf dem der Inhalt und eine kryptographische Signierung dieses Inhalts mit der pseudonymen Absenderadresse zu finden ist.

Dieses Papier legt er dem Richter vor, welcher eine Identitätsoffenlegung beschließt und das Beweis-Papier von einem Sachverständigen prüfen lässt. Anschließend ist mit der Person gemäß den geltenden Rechten zu verfahren. Alternativ könnte der Beweis natürlich auch auf CD oder per verschlüsselter E-

Vorschlag	Ja : Nein
Mail an das Gericht übergeben werden. Disziplinierungsmaßnahmen wie Sperren des Internetanschlusses sollten nur von einem Richter getroffen werden dürfen. Normalerweise sollte dieser aber Geldstrafen verhängen. Falls nun Personen miteinander kommunizieren, welche sich nicht gegenseitig anzeigen, entsteht eine vertrauliche Kommunikation welche auch illegale Inhalte beinhalten kann. Sobald allerdings zu viele Personen dieser beitreten könnte einer die anderen verraten. Daher werden diese Gruppen akzeptiert. Um eine Hemmschwelle für die Begehung von Urheberrechtsverletzungen im Internet zu setzen, sollte eine staatliche digitale Rechteverwaltung eingeführt werden. Diese stellt eine freiwillige Erweiterung des Computers mit speziellen Chips und kompatibler Software dar, welche geschützte Inhalte entschlüsseln und eine Weitergabe nur innerhalb der Familie, nicht aber gegenüber weiteren Personen, erlauben. Um dieses zu umgehen, müsste beispielsweise der Bildschirm abgefilmt werden. Ein Herunterladen von Tools, die dieses System knacken könnten, sollte auf keinen Fall verboten werden, da dass System sich nicht softwaremäßig knacken lassen wird, sodass dies gar nicht nötig sein wird. Inhalte aus dem Ausland sollten unter der Angabe von IP-Adressen gesperrt werden können. Der gesperrte Anbieter sollte darüber, falls möglich, benachrichtigt werden. Die Sperrung darf auf keinen Fall für Angebote innerhalb der europäischen Union erfolgen. Es sollte ein Proxy bereitgestellt werden, über den Inhalte des Auslands aufgerufen werden können, bei denen die Inhalte selber zensiert worden sind, sodass eine feinere Zensur von Auslandsinhalten möglich ist. Die Strafen dürfen nicht allzu hoch sein, da zu beachten ist, dass Computer auch gehackt werden können ohne, dass der Hacker Spuren hinterlässt. Allerdings sollte ein Anreiz gesetzt werden, den Computer gut zu sichern. Auch kann ein ungesicherter Computer möglicherweise schnell von einem Nachbar oder Gast des Hauses missbraucht werden. Auch sollte ein Anreiz gesetzt werden, seinen Computer ein wenig vor fremden Personen zu sichern.	
OpenCrypt Die mafiösen Verquickungen der Zertifizierungsindustrie mit den Browser-Anbietern führen zu einem Marktversagen bei der Durchsetzung sicherer Verbindungsdienste im Web. Den Behörden sollen deshalb die Möglichkeit	1 : 0

Vorschlag	Ja : Nein
erhalten den Import von Root-Zertifikaten durch Browser-Anbieter anzuordnen, wobei mindestens ein offene Zertifizierung von allen unterstützt werden sollte. Derzeit ist der Zertifikatemarkt durch Marktversagen gekennzeichnet, das sich darin ausdrückt, dass entweder Wucherpreise für Zertifikate gezahlt werden müssen oder gar keine Verschlüsselung vom Dienstanbieter bereitgehalten wird wo sie möglich wäre. Das liegt daran, dass Rootzertifikate der freien Zertifikatdienste nicht von den Browserherstellern importiert werden. Das Ziel sollte sein, dass https insgesamt http ablöst. Technisch kein Problem, aber das geht nur, wenn von allen Browserherstellern konzertiert auf offene Zertifikate gesetzt wird. *Angelegt von rebentisch am 30. November 2012* https://enquetebeteiligung.de/d/1562 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	
Belastung des Netzes durch Denial-of-Service-Angriffe verhindern Belastung des Netzes durch Denial-of-Service-Angriffe sollten technisch verhindert werden. *Angelegt von TAE am 17. September 2011* https://enquetebeteiligung.de/d/915 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	1 : 1
Kommunikationsmanipulation verhindern Es sollte gesichert sein, dass wenn jemand an jemanden eine Nachricht schickt, dass diese nicht von einem Kommunikationsdienstleister oder einen anderen Person verändert werden kann. Vorschlag Version A: Jeder Internetverkehr von und zu einer Anschlusskennung (z.B. IP-Adresse) sollte kryptographisch verschlüsselt sein, damit ein Abhören des Inhalts verhindert wird. Vorschlag Version B: Jeder Internetverkehr von und zu einer Anschlusskennung (z.B. IP-Adresse) muss kryptographisch signiert sein, damit Manipulationen des Inhalts verhindert werden. *Angelegt von TAE am 17. September 2011*	1 : 1

Vorschlag	Ja : Nein
https://enquetebeteiligung.de/d/913 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	
Ertüchtigung des Artefakttransports im Internet Dieser Vorschlag will erreichen, dass im Internet zu transportierende Artefakte so ertüchtigt werden, dass aus ihnen selbst, d.h. aus dem Inhalt eines Artefakts, ihre (Nicht-)Korrektheit, Bedeutung und Eigenschaft erkannt werden können. Hintergrund: Die Zuverlässigkeit des Internet ist heute so desolat, dass ich frage, ob das Prinzip, auf dem das Internet aufbaut, leistungsfähig genug ist für ein Internet gemäß unseren heutigen und kommenden Anforderungen. Vielleicht befinden sich die heutigen Erbauer des Internet in einer ähnlichen Lage wie die Dombaumeister des Mittelalters, als denen die immer höher aufzutürmenden Dome zusammenbrachen., weil die Grundlagen der Steinbautechnik nicht leistungsfähig genug waren. Erst mit neuen Prinzipien und neuen Technologien wurden ein paar hundert Jahre später der Eifelturm, die Müngstener Brücke und riesige Hochhäuser gebaut. Handlungsempfehlung: Die Enquete-Kommission könnte durch Fachleute, z.B. durch das BSI, prüfen lassen, welche Schwächen in den Prinzipien, auf denen das Internet sich heute gründet, zu dessen Mängeln führen und ob es leistungsfähigere Prinzipien für Schaffung von Artefakttransporten im Netz, wie oben als Ziel beschrieben, gibt. *Angelegt von pauleduard am 10. Mai 2011* https://enquetebeteiligung.de/d/701 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	1 :5
Einrichtung einer unabhängigen Sicherheitskontrolle Vorschlag: Es soll eine Einrichtung geschaffen werden, deren Aufgabe es ist, unangekündigt unterschiedliche Angriffe auf Behörden und Anbieter kritische Infrastruktur (Strom, Kommunikation,...) auszuführen und die davon betroffenen dann zu informieren und beraten. Hintergrund: Solche simulierten Angriffe sind die einzige Möglichkeit, verläßliche Informationen über die Sicherheitsstandards der betroffenen Stellen zu gewinnen. Darüber hinaus kann so ein Problembewußtsein geschaffen werden, was wohl noch fehlt.	2 : 10

Vorschlag	Ja : Nein
Wo man solch eine Einrichtung eingliedert (Polizei, Katastrophenschutz, BSI) weiß ich nicht. Man kann davon ausgehen, daß andere Staaten bereits Angriffseinheiten haben. Deshalb ist ein solcher Selbstschutz für Deutschland unverzichtbar. *Angelegt von cschoen am 21. April 2012* https://enquetebeteiligung.de/d/607 *Dieser Beitrag wurde als Handlungsempfehlung gewertet.*	

5593

VI. Anlagen

Im Rahmen der Arbeit der Projektgruppe fanden mehrere Expertengespräches statt. Die Mitglieder danken den sachverständigen Anhörpersonen für ihre zahlreichen Hinweise und Anregungen sowohl während der Expertengespräche als auch in ihren schriftlichen Stellungnahmen.

VI.1. Öffentliches Expertengespräch zum Thema „Sicherheit im Netz“

Die Projektgruppe hörte in dem am 28. November 2011 durchgeführten öffentlichen Expertengespräch[854] zum Thema „Sicherheit im Netz“ folgende externe Sachverständige an:

Gaycken, Dr. Sandro
(Freie Universität Berlin)

Heckmann, Univ.-Prof. Dr. jur. Dirk
(Institut für IT-Sicherheit und Sicherheitsrecht; Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht; Forschungsstelle für IT-Recht und Netzpolitik; Universität Passau)

Könen, Andreas
(Leiter des Fachbereiches Sicherheit in Anwendungen und Kritischen Infrastrukturen Koordination und Steuerung, Bundesamt für Sicherheit in der Informationstechnik)

Manske, Mirko
(Erster Kriminalhauptkommissar; Sachgebietsleiter des Bereiches der Operativen Auswertung Cybercrime; Bundeskriminalamt)

Schiller, Prof. Dr.-ing. habil. Jochen H.
(CIO der Freien Universität Berlin; Projektleiter des Forschungsforums Öffentliche Sicherheit Institute of Computer Science; Freie Universität Berlin)

Schröder, Thorsten
(IT Security Analyst)

---

[854] Sämtlich Unterlagen zum öffentlichen Expertengespräch sind online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZustrSi_2011-11-28_oeffentliches_Expertengespraech/index.jsp

VI.2. Öffentliches Expertengespräch zum Thema „IPv6 – Sicherheitsaspekte“

Die Projektgruppe hörte in dem am 21. Mai 2012 durchgeführten öffentlichen Expertengespräch[855] zum Thema „IPv6 – Sicherheitsaspekte“ folgende externe Sachverständige an:

Döring, Gert
(IPv6-Spezialist bei der SpaceNet AG)

Fritsche, Wolfgang
(Leiter des Internet Competence Center der IABG; IPv6-Berater mit dem Schwerpunkt „IPv6 Sicherheit“; Mitglied im globalen IPv6-Forum; Mitglied im deutschen IPv6 Rat und Initiator der Arbeitsgruppe „IPv6 Security und Privacy“)

Kühn, Ulrich
(Leiter des Referats für Technikangelegenheiten beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit; Mitglied der Arbeitsgruppe IPv6 des AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder)

Turba, Martin
(Gruppenleiter Netzinfrastruktur & Projekte; Stellv. Leiter Fraunhofer Competence Center LAN Fraunhofer-Institut für Graphische Datenverarbeitung IGD)

Weber, Christoph
(Netzwerk und Security Spezialist)

Zeeb, Björn A.
(Entwickler und Mitglied des IPv6- und Security-Teams beim FreeBSD Projekt)

[855] Sämtlich Unterlagen zum öffentlichen Expertengespräch sind online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-05-21_oeffentliches_Expertengespraech/index.jsp

VI.3. Nicht öffentliches Expertengespräch zum Thema „Internetkriminalität“

Auf Einladung des Vorsitzenden Harald Lemke sowie des Abgeordneten Jerzy Montag (BÜNDNIS 90/DIE GRÜNEN) fand am 5. März 2012 ein nicht öffentliches Expertengespräch zum Thema „Internetkriminalität“ mit **Oberstaatsanwalt Rainer Franosch**, Leitung der hessischen Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT), Generalstaatsanwaltschaft Frankfurt am Main, statt. [856]

[856] Die schriftliche Stellungnahme von Oberstaatsanwalt Rainer Franosch ist online abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZuStrSi_2012-03-05/PGZuStrSi_2012-03-05_Stellungnahme_OStA_Franosch.pdf

Abkürzungsverzeichnis

ADSL	Assymmetric Digital Subscriber Line
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
B2B	Business-to-Business
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BHG	Bundesgerichtshof
BIT	Bundesstelle für Informationstechnik
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BKA	Bundeskriminalamt
BMJ	Bundesministerium der Justiz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BYOD	Bring Your Own Device
CC	Cybercrime Convention
CCITT	Comité Consultatif International Téléphonique et Télégraphique
CD-ROM	Compact Disc- Read Only Memory
CERT	Computer Emergency Response Team
CTW-Projekt	Check the Web-Projekt
DAF	Deutsches Advisory Format
DDoS-Angriff	Distributed Denial of Service-Angriff
DIN	Deutsches Institut für Normung e.V.
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
ECCP	European Cybercrime Platform
EDV	Elektronische Datenverarbeitung

EG	Europäische Gemeinschaft
EJN	European Judicial Network/Europäisches Justizielles Netz
ENISA	European Network and Information Security Agency/Europäische Agentur für Netz- und Informationssicherheit
EPG	Electronic Program Guide
EU	Europäische Union
EuroDOCSIS 3.0	Data Over Cable Service Interface Specification 3.0
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
FTTB	Fiber-to-the-Building
FTTC	Fiber-to-the-Curb
FTTH	Fiber-to-the-Home
G8	Gruppe der sieben führenden westlichen Industriestaaten einschließlich Russlands
GAK	Gemeinschaftsaufgabe zur Verbesserung der Agrarstruktur und des Küstenschutzes
GG	Grundgesetz
GHZ	Gigahertz
GKI	Gemeinsame Kontrollinstanz von Europol
GPSG	Geräte- und Produktsicherheitsgesetz
HD-TV	High Definition Television
HFC-Netzwerk	Hybrid Fiber Coax-Netzwerk
HTCN	G8 24/7 High Tech Crime Network
HTCSG	G8 Subgroup on High Tech Crome
HTML	Hypertext Markup Language
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum

5704	IKT	Informations- und Kommunikationstechnologie
5705	IPv6	Internetprotokolls Version 6
5706	ISO	International Organization for Standardization
5707	ISP	Internet-Service-Provider
5708	IT	Informationstechnik
5709	iTAN-Verfahren	indizierte Transaktionsnummern-Verfahren
5710	ITU	International Telecommunication Union
5711 5712	ITU-T	International Telecommunication Union - TelecommunicationStandardization Sector
5713	JGG	Jugendgerichtsgesetz
5714	Kbit/s	Kilobit pro Sekunde
5715	LTE	Long Term Evolution
5716	Mbit/s	Megabit pro Sekunde
5717	MPG	Gesetz über Medizinprodukte
5718	ms	Millisekunde
5719	NGA-Netz	Next Generation Access-Netz
5720	OSI	Open Systems Interconnection
5721	OWiG	Gesetz über Ordnungswidrigkeiten
5722	PC	Personal Computer
5723	PKS	Polizeiliche Kriminalstatistik
5724	PPP	Public-Private-Partnership
5725	ProdHaftG	Produkthaftungsgesetz
5726	ProdSG	Produktsicherheitsgesetz
5727	RFC	Request for Comments
5728	SDSL	Symmetric Digital Subscriber Line
5729	StGB	Strafgesetzbuch
5730	StPO	Strafprozessordnung
5731	TCP/IP	Transmission Control Protocol/Internet Protocol

TK	Telekommunikation
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UMTS	Universial Mobile Telecommunications System
UN	United Nations/Vereinte Nationen
UNODC	United Nations Office on Drugs and Crime
USB-Stick	Universal Serial Bus-Stick
UWG	Gesetz gegen den unlauteren Wettbewerb
VDSL	Very High Speed Digital Subscriber Line
W3C	World Wide Web Consortium
WIK	Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste
WLAN	Wireless Local Area Network

Literatur- und Quellenverzeichnis

Mitglieder der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft

Vorsitzender: Harald Lemke (Sachverständiger)

Wissenschaftliche Mitarbeiterin: Silvia Saupe

Stimmberechtigt:

Brandl, Dr. Reinhard (MdB, CDU/CSU)

Freude, Alvar (Sachverständiger)

Jarzombek, Thomas (MdB, CDU/CSU)

Kurz, Constanze (Sachverständige)

Lemke, Harald (Sachverständiger)

Montag, Jerzy (MdB, stellv. Mitglied der Enquete-Kommission, BÜNDNIS 90/DIE GRÜNEN)

Reichenbach, Gerold (MdB, SPD)

Schön, Nadine (MdB, stellv. Mitglied der Enquete-Kommission, CDU/CSU)

Schulz, Jimmy (MdB, FDP)

weitere Mitglieder:

Beckedahl, Markus (Sachverständiger)

Canel, Sylvia (MdB, FDP)

Gersdorf, Prof. Dr. Hubertus (Sachverständiger)

Gorny, Prof. Dieter (Sachverständiger)

Heveling, Ansgar (MdB, CDU/CSU)

Höferlin, Manuel (MdB, FDP)

Hofmann, Dr. Jeanette (Sachverständige)

Koeppen, Jens (MdB, CDU/CSU)

Mühlberg, Annette (Sachverständige)

Notz, Dr. Konstantin von (MdB, BÜNDNIS 90/DIE GRÜNEN)

Osthaus, Dr. Wolf (Sachverständiger)

padeluun (Sachverständiger)

Ring, Prof. Dr. Wolf-Dieter (Sachverständiger)

Rohleder, Dr. Bernhard (Sachverständiger)

Rößner, Tabea (MdB, BÜNDNIS 90/DIE GRÜNEN)

Sager, Krista (MdB, stellv. Mitglied der Enquete-Kommission, BÜNDNIS 90/DIE GRÜNEN)

Schwarzelühr-Sutter, Rita (MdB, SPD)

Tausch, Cornelia (Sachverständige)

Wawzyniak, Halina (MdB, DIE LINKE.)

Zypries, Brigitte (MdB, SPD)