PG Zugang, Struktur und Sicherheit im Netz

Handlungsempfehlungen zum Bereich Kritische Infrastrukturen und Internetkriminalität

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, …

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[1] sowie die TAB-Studie, Kap. IV[2] 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.

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.

---

1 „Risiken und Herausforderungen für die Öffentliche Sicherheit in Deutschland“, Grünbuch des Zukunftsforums Öffentliche Sicherheit, 1. Aufl., Sept. 2008.

2 „Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen Ausfalls der Stromversorgung“, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, November 2010.

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, S. 79 bis 81 des Zwischenberichtes der Projektgruppe Datenschutz, Persönlichkeitsrechte[3] 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)[4] 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[5]).

3 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.

4 * https://www.datenschutzzentrum.de/material/recht/audit.htm (Quelle: Stand 19.11.2012, 10.40 Uhr)

5 * 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.[6]

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.[7] Die Enquete-Kommission bekräftigt ihre dort gemachten Ausführungen und fordert die Bundesregierung auf, bei

---

6

7 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.

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 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.

IPv6

Die nach dem neuen Internetprotokoll IPv6 vergebenen Internetadressen haben das Potential, 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 die 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 allgemeinverständlicher 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 IPv-Adress-Prefixen (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 einzuräumen, zumindest aber ohne zusätzliche 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 ggfs. auch gesetzlich zu verankern.

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 Bereich Internetkriminalität

Evaluierung von Eingriffsbefugnissen

In einem Sondervotum des Berichtes „Datenschutz, Persönlichkeitsrechte“ der Enquete-Kommission Internet und digitale Gesellschaft[8] 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 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.[9] 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

8 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.

9 * Vgl. Stellungnahme Manske, S. 1.

fortschreitenden Technisierung der Gesellschaft auch in den kommenden Jahren immer mehr Erscheinungsformen von Kriminalität ins Internet verlagern oder dort entstehen werden.[10]

- 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“[11]

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 der IT-Sicherheitsbranche haben vor, während und nach der Änderung der Norm auf ihre gravierenden Bedenken hingewiesen.[12]

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.[13]

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

10 * Vgl. Stellungnahme Manske, S. 3.

11 Siehe hierzu auch den Vorschlag „Streichung von §202c StGB („Hackertoolverbot“)“ aus der Online-Beteiligungsplattform. Siehe hierzu: Kapitel V

12 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.

13 * 2 BvR 2233/07, 1151/08 und 1524/08: http://www.bundesverfassungsgericht.de/entscheidungen/rk20090518_2bvr223307.html

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 verfassungsgemäß vorgenommen werden.[14] Solange aber die Einzelheiten einer Maßnahme nicht geregelt sind, kann § 20 1 II BKAG nicht als Vorbild dienen.[15]

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

14 * Vgl. dazu K&R 11/2011.

15 * Vgl. dazu K&R 11/2011.

Ausfuhrbeschränkungen sicherzustellen, dass derartige Techniken nicht 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.