Claudia Eckert
Heinz Thielmann

Herausgeber

Sicher im Internet

Wie unsere Zukunft von Sicherheit, Vertrauen und Datenschutz abhängt

MÜNCHNER KREIS
Übernationale Vereinigung für Kommunikationsforschung
Supranational Association for Communications Reseach

Claudia Eckert
Heinz Thielmann

Herausgeber

Sicher im Internet

Wie unsere Zukunft von Sicherheit, Vertrauen und Datenschutz abhängt

MÜNCHNER KREIS
Übernationale Vereinigung für Kommunikationsforschung
Supranational Association for Communications Reseach

Impressum

Herausgeber:

Prof. Dr. Claudia Eckert
Fraunhofer Institut AISEC
Parkring 4
85748 Garching
claudia.eckert@aisec.fraunhofer.de

Prof. Dr.-Ing. Heinz Thielmann
Emphasys GmbH
Eichenstr. 11
90562 Heroldsberg
heinz.thielmann@t-online.de

Reihenherausgeber:
Münchner Kreis – Übernationale Vereinigung für Kommunikationsforschung e.V.
Tal 16
80331 München
www.muenchner-kreis.de
office@muenchner-kreis.de

Redaktion:
Dipl.-Phys. Volker Gehrling
Münchner Kreis – Übernationale Vereinigung für Kommunikationsforschung e.V.
v.gehrling@muenchner-kreis.de

Druck:
Knecht-Druck, München

ISBN 978-3-9813733-6-3

Vorwort

Das Internet hat sich zu einem empfindlichen Nervensystem der Wirtschaft, der öffentlichen und privaten Organisationen und der kommunikativen globalen Gesellschaft entwickelt. Verfügbare Bandbreiten in Festnetzen und Mobilfunknetzen stellen eine globale Infrastruktur für einen fast unbegrenzten Datenverkehr dar. Die überwiegende Zahl der Nutzer bewegt sich in dieser offenen Infrastruktur so, als gäbe es keine Gefahren und Bedrohungen für schützenswerte Daten und Identitäten. Die kriminelle Energie für Datendiebstahl, Daten- und Transaktionsmanipulation nimmt allerdings ebenso rasant zu wie die Nutzung des Internet. Für den physischen Verkehr (Straße, Luft, Wasser) haben wir weltweit anerkannte Verkehrsordnungen.

Um Schäden und möglichen Katastrophen im Internet vorzubeugen, gibt es nach Meinung vieler Fachleute sowie der breiten Öffentlichkeit noch nicht in genügender Qualität wirksame Regeln und Lösungen. In der Geschäftswelt haben große Unternehmen ihr Bewusstsein für Sicherheit und Datenschutz weitgehend geschärft und begonnen, entsprechende Regeln (Policies, Governance) zu entwickeln, die regelmäßig auditiert und angepasst werden. Kleine Unternehmen (Mittelstand), Freiberufler und Privatpersonen sind dagegen in der Regel viel unbekümmerter, solange sie nicht direkt merkbar geschädigt werden.

In der vom Münchner Kreis durchgeführten Konferenz haben die Teilnehmer Bedrohungen identifiziert und diskutiert, Handlungsbedarfe herausarbeitet und Lösungswege entwickelt. Damit sollte jeder Teilnehmer die Bedeutung des Themas für sich selbst erkennen und Ansatzpunkte zur praktischen Handhabung mitnehmen können. In den drei parallelen Themen-Workshops:

- Sichere Identitäten im Internet
- Sichere Dienste und Prozesse im Internet
- Herausforderungen bei der Erfüllung von Complianceanforderungen

wurden darüber hinaus spezifische Themen vertieft bearbeitet.

Der vorliegende Tagungsband enthält die Workshop-Ergebnisse sowie die Vorträge und die durchgesehenen Mitschriften der Diskussionen. Allen Referenten und Diskutanten sowie allen, die zum Gelingen der Konferenz und zur Erstellung dieses Buches beigetragen haben, gilt unser herzlicher Dank!

Claudia Eckert Heinz Thielmann

Inhalt

1 Begrüßung und Einführung

Prof. Dr. Arnold Picot, Ludwig-Maximilians-Universität München

Meine sehr verehrten Damen und Herren, herzlich Willkommen zu unserer Fachkonferenz „Sicherheit im Internet – wie unsere Zukunft von Sicherheit, Vertrauen und Datenschutz abhängt“. Wir freuen uns, dass Sie zu früher Stunde so zahlreich und, wie mir scheint, vollzählig hier sind. Unser heutiges Thema hat in der Tat strategische Bedeutung für die Informations- und Wissensgesellschaft.

Der Münchner Kreis bemüht sich seit Beginn seiner Existenz, also seit fast 40 Jahren, darum, das Verhältnis zwischen neuen Technologien und dem, was die Gesellschaft, die Wirtschaft, die Bürger davon zu erwarten können bzw. wie sie darauf reagieren, in eine produktive und tragfähige Balance zu bringen. Das wird auch durch den Ausschnitt des Selbstverständnisses des Münchner Kreis, der hier projiziert ist, zum Ausdruck gebracht (Bild 1).

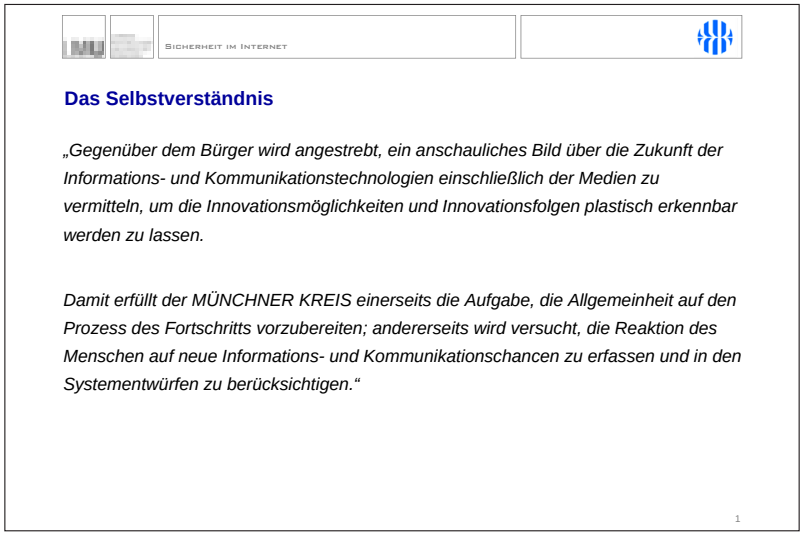


Bild 1

Letztlich geht es darum, mit Hilfe unserer Initiativen und Aktivitäten darauf hinzuwirken, dass die Reaktionen, die Wahrnehmungen und Wünsche des Menschen in Bezug auf neue IuK-Systeme realistisch erfasst und in den Systementwürfen auch berücksichtigt werden. Diese wichtige Herausforderung stellt sich auch beim Thema Sicherheit.

Ehe ich darauf etwas näher eingehe, ganz kurz ein kleiner Blick auf die derzeitigen Aktivitäten des Münchner Kreises (Bild 2).

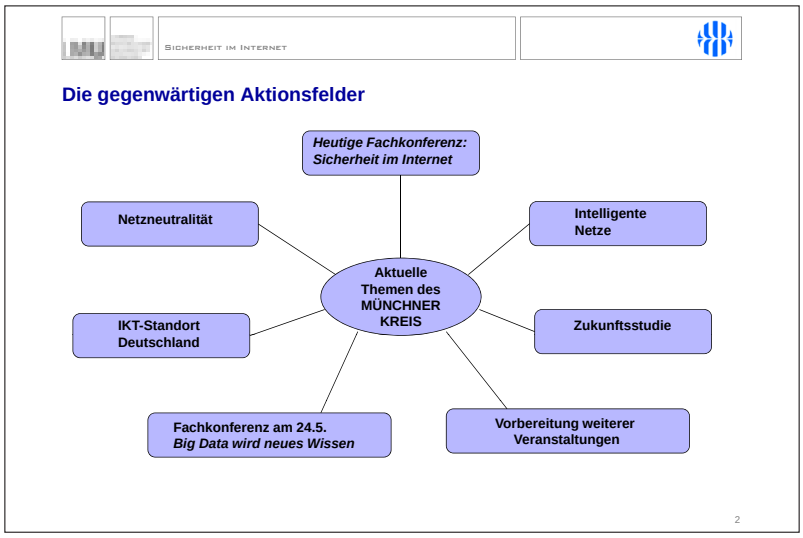


Bild 2

Heute haben wir diese Konferenz zur Sicherheit. Wir werden dann bald eine Konferenz zu Big Data haben, die sich in bestimmten Teilen an die heutige Thematik anschließt. Daneben befassen wir uns mit intelligenten Netzen und mit Netzneutralität in Arbeitsgruppen und Workshops, in einem Arbeitskreis mit Standortfragen der IKT-Wirtschaft in Deutschland und Europa. Die Zukunftsstudie wird auch weiter geführt, da sind wir gerade in intensiver Vorbereitung. Zudem bereiten wir weitere Veranstaltungen vor. Wir sind also auf vielen Gebieten unterwegs, um uns alle noch besser auszustatten für den Weg in und durch die Informationsgesellschaft und Internetwelt.

Der Ausgangspunkt der heutigen Fachkonferenz hat natürlich mit dem Internet ganz zentral zu tun (Bild 3).

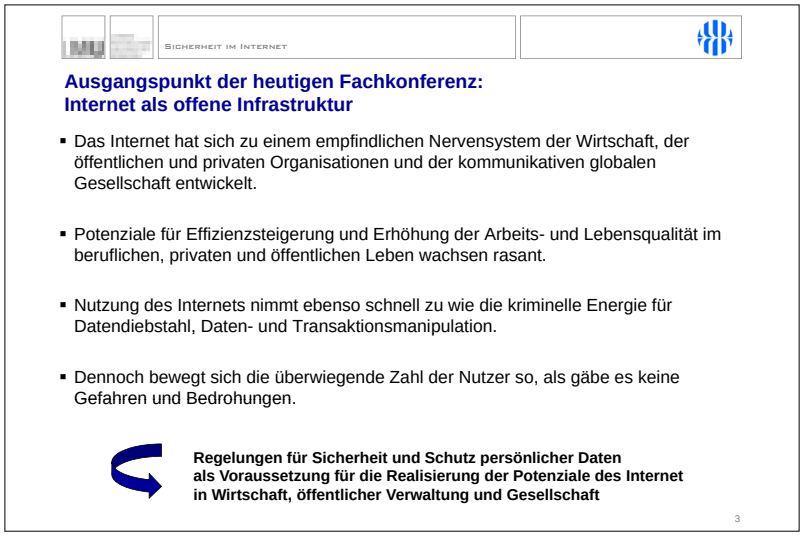


Bild 3

Das Internet und die damit zusammenhängenden benachbarten Systeme und Anwendungen ermöglichen eine hohe Effizienz- und Qualitätssteigerung unser aller Leben, unser aller Arbeitsverhältnisse und der gesellschaftlichen Zusammenhänge. Allerdings nimmt mit der Ausbreitung des Internet leider auch die kriminelle Energie zu; neue Chancen der kriminellen Nutzung des Internets werden ausprobiert. Darüber werden wir auf dieser Tagung noch einiges hören.

Viele Nutzer, vielleicht sogar die allermeisten alltäglichen Nutzer bewegen sich allerdings durch das Internet so, als ob es diese Gefahren kaum gäbe. Dennoch sind sie im Bewusstsein von sehr vielen irgendwo im Hintergrund verankert. Deswegen brauchen wir Regeln, Tools und auch andere Maßnahmen, um den Schutz persönlicher Daten und die Sicherheit der im Internet gespeicherten und übertragenen Daten zu gewährleisten. Nur dann lässt sich das, was das Internet uns an Nutzen stiften kann, auch tatsächlich ausschöpfen. Das ist nicht einfach, aber zugleich auch sehr relevant.

In den Studien des Münchner Kreises der letzten Jahre ist das Thema immer wieder behandelt worden, gerade in den Zukunftsstudien I bis IV (Bild 4).

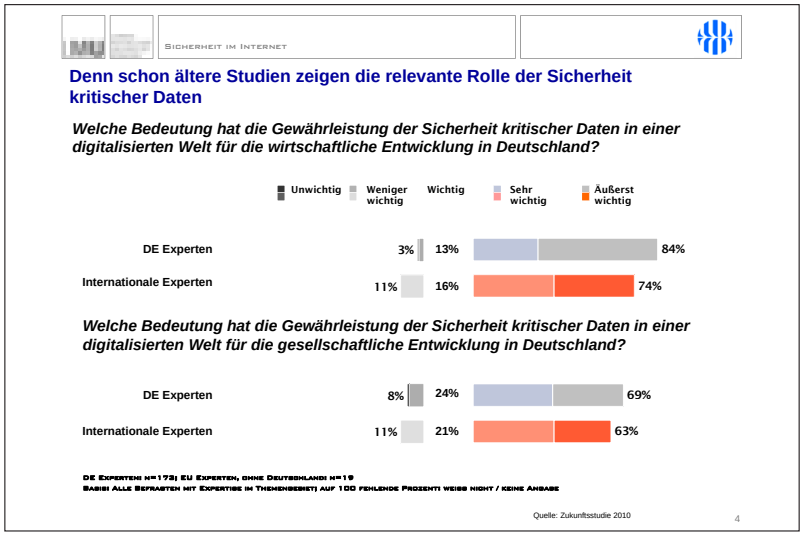


Bild 4

Bereits vor zwei Jahren wurden in der Zukunftsstudie zahlreiche Experten weltweit befragt. Dabei wurde klar, dass die Gewährleistung der Sicherheit kritischer Daten für die wirtschaftliche Entwicklung als ausgesprochen wesentlich angesehen wird. Das sagen nicht nur mehr als vier Fünftel der Experten aus Deutschland, auch die internationalen Experten, die wir hierzu zahlreich befragt haben, stufen das ganz ähnlich ein. Das gleiche gilt für die gesellschaftliche Entwicklung. Auch hier wird die Gewährleistung der Sicherheit kritischer Daten in der digitalisierten Welt als extrem wichtig eingestuft.

In einer BITKOM-Untersuchung, die kürzlich veröffentlicht wurde, zeigen sich ähnliche Tendenzen und zugleich auch gewisse Implikationen einer möglicherweise ungenügenden Sicherheit (Bild 5).

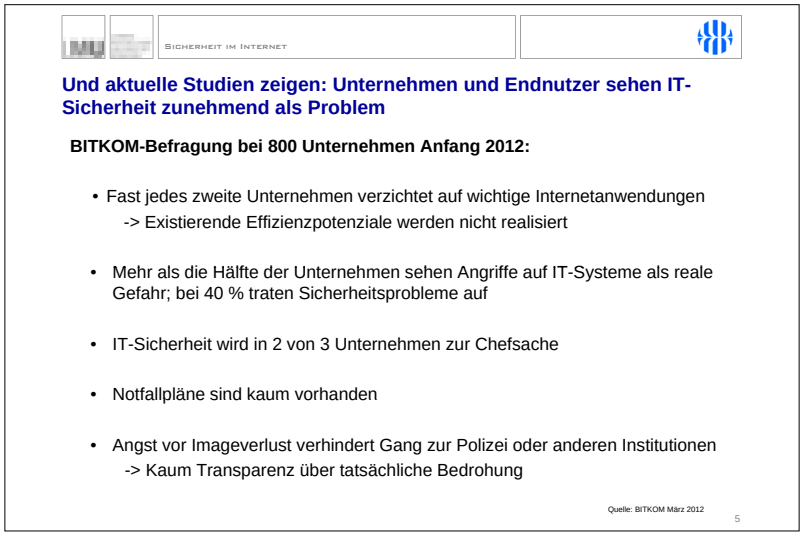


Bild 5

Zum Beispiel wird erkennbar, dass fast jedes zweite Unternehmen auf Grund von Sicherheitsbefürchtungen darauf verzichtet, wichtige Internetanwendungen durchzuführen. Ebenfalls treten bei mehr als der Hälfte der Unternehmen Angriffe auf IT-Systeme offensichtlich als reale Gefahr auf. 40% haben Sicherheitsprobleme zum Ausdruck gebracht, und in zwei von drei Unternehmen wird das sogar schon als Chefsache angesehen. Andererseits sind Notfallpläne kaum vorhanden und man meldet auch kaum die entsprechenden Vorkommnisse, weil man Angst vor Imageverlust hat. Insofern weiß man auch gar nicht ganz genau, was so alles passiert.

In der jüngsten Zukunftsstudie des letzten Jahres, die viele von Ihnen kennen, und die man wie alle früheren auch kostenlos von unserer Webpage herunterladen kann, wie es bereits rd. 150.000 Nutzer in den letzten Jahren getan haben, haben wir Anwender aus sechs Ländern befragt (Bild 6).

Bild 6

Wir haben in unseren verschiedenen Untersuchungsfoki u.a. auch Sicherheitsfragen angesprochen. Ich will Ihnen einzelne Teilergebnisse vorstellen, die zeigen, dass das kein rein deutsches Problem ist, mit dem wir uns hier beschäftigen. Manchmal wird gesagt, die Diskussion um die Internetsicherheit spiegele lediglich die übertriebene „deutsche Angst" wieder, weil die Deutschen so übersensibel seien. Woanders würde man damit viel gelassener und souveräner umgehen. Das konnten wir in unseren Untersuchungen nicht feststellen, und das will ich Ihnen kurz erläutern (Bild 7).

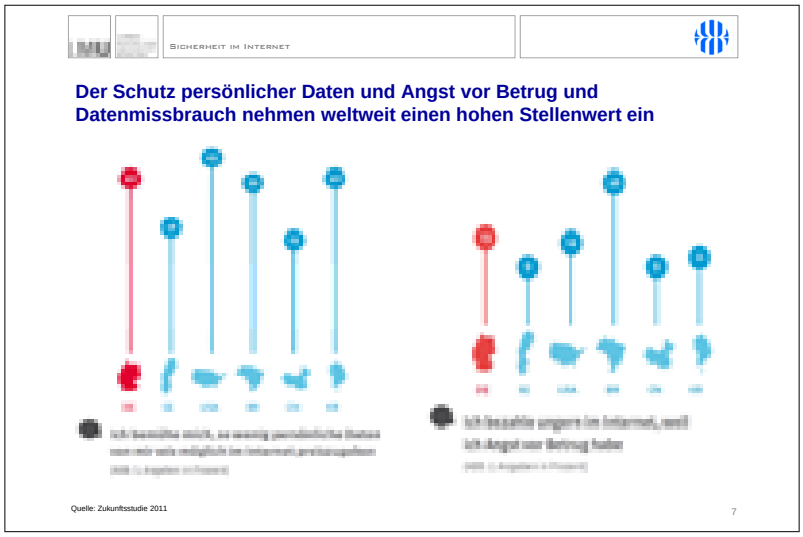


Bild 7

Zum Beispiel wurde das Statement bewertet: „Ich bemühe mich, so wenig persönliche Daten wie möglich im Internet preiszugeben". Interessanterweise ist Deutschland da nicht Weltmeister, sondern die USA und auch Korea, aber auch andere sind sehr stark ausgeprägt. Hier gibt es offensichtlich Sorgen, die nicht nur in Deutschland zuhause sind.

„Ich bezahle ungern im Internet, weil ich Angst vor Betrug habe“: Hier ist Brasilien ganz vorn, dann kommen Deutschland und USA. Es handelt sich also um ein Problem, das offensichtlich global zu sein scheint.

Wir haben dann in dieser Studie eine Reihe von sogenannten Zukunftsbildern, also zukünftig möglichen Anwendungen gezeigt, die sehr viel versprechend erscheinen, und diese in den verschiedenen Ländern bewerten lassen. Dazu gehörte z.B. das digitale Schulbuch (Bild 8).

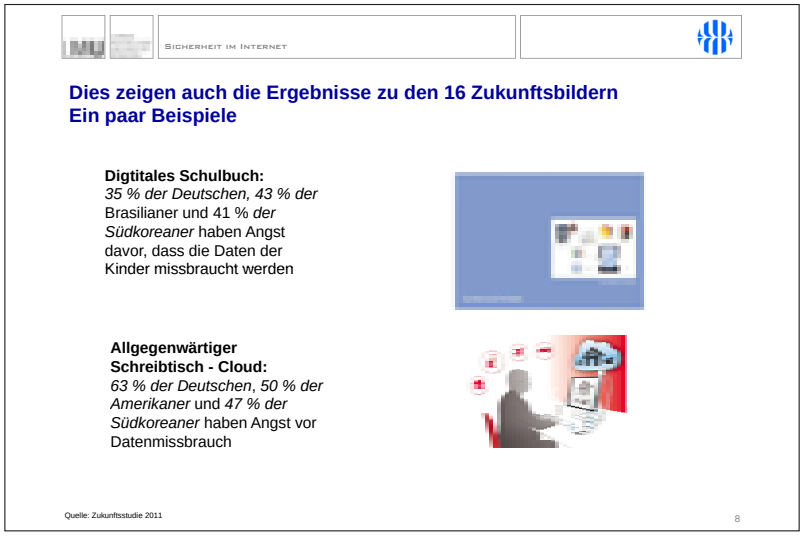


Bild 8

35% der Deutschen, 43% der Brasilianer und 41% der Südkoreaner haben geäußert, dass sie Angst davor haben, dass die Daten der Kinder von irgendwelchen Stellen missbraucht werden, wenn man ein digitales Schulbuch einführt. Ähnliches gilt für einen allgegenwärtigen Schreibtisch, der sich der Cloud sozusagen als Schreibtischinfrastruktur im Hintergrund bedient. 63% der Deutschen, 50% der Amerikaner sagen, dass sie Angst haben vor Datenmissbrauch. Auch die Südkoreaner sehen das ähnlich.

Schauen wir in eine frühere Studie, die Zukunftsstudie vom Jahre 2009. Da wurde u.a. nach den drei wichtigsten Barrieren in Bezug auf die Realisierung des Cloud Computing gefragt (Bild 9).

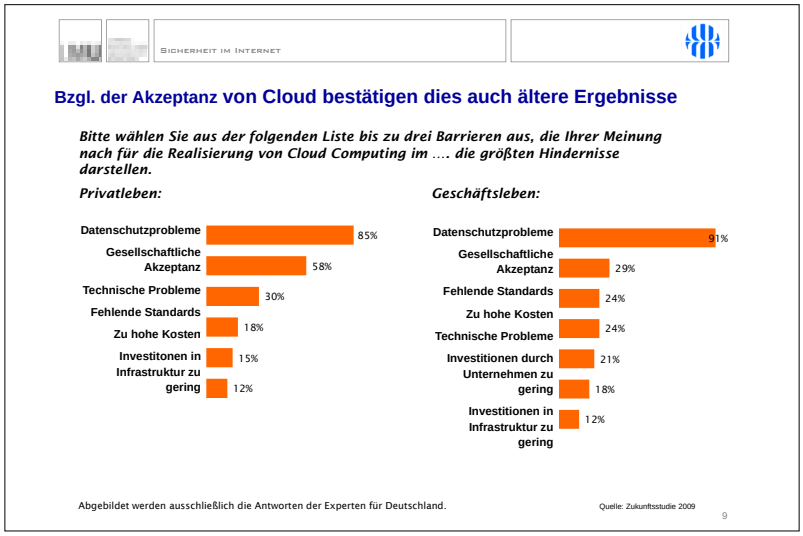


Bild 9

Absolut an erster Stelle stehen Datenschutzprobleme, sowohl im Privatleben als auch im Geschäftsleben. Danach kommen einige andere Punkte.

Die Zukunftsstudie vom letzten Jahr, die ich eben erwähnt habe, hat z.B. auch das Mobiltelefon als Zahlungsmittel bewerten lassen (Bild 10).

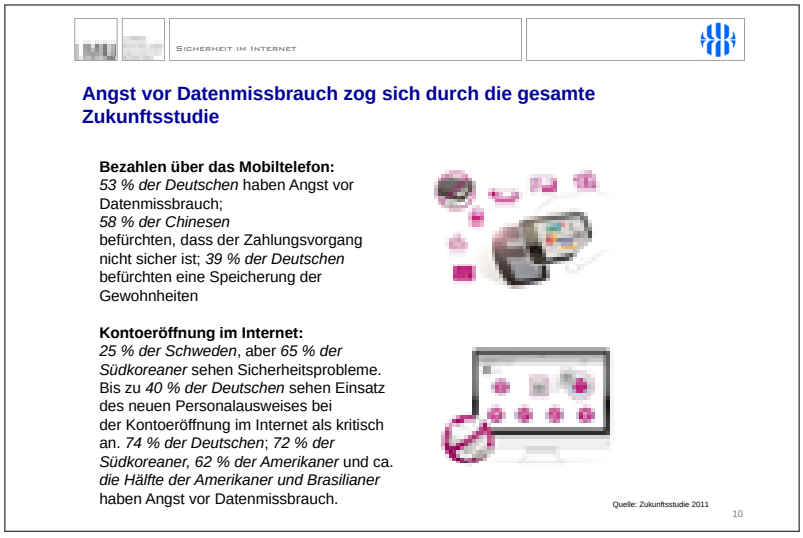


Bild 10

Erhebliche Sorgen werden in China und Deutschland auf ähnlichem Niveau geäußert, nämlich dass Missbrauch gefördert werden könne und dass man Speicherungen von Gewohnheiten befürchtet. Ähnliches gilt für Kontoeröffnung im Internet. Dabei hat man den Befragten eine flexible, bequeme und sichere Möglichkeit der online-Kontoeröffnung gezeigt. Dennoch sehen etliche Anteile der Befragten, dass hier Sicherheitsprobleme auf-

treten könnten. Interessanterweise sehen bis zu 40% der Deutschen den Einsatz des neuen Personalausweises bei der Kontoeröffnung als kritisch an. Für mich eine sehr überraschende Zahl, die man aber zur Kenntnis nehmen muss. Schließlich haben auch große Anteile der Deutschen, Südkoreaner, Amerikaner und Chinesen Angst vor Datenmissbrauch (Bilder 11, 12, 13, 14).

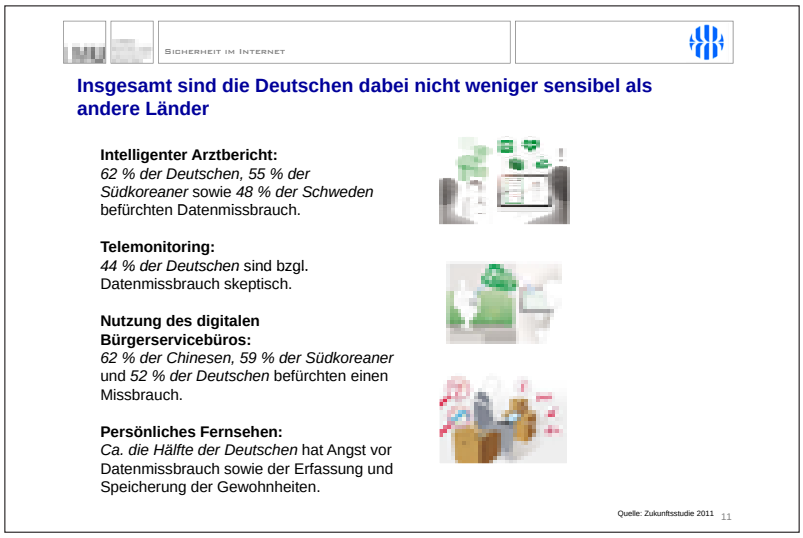


Bild 11

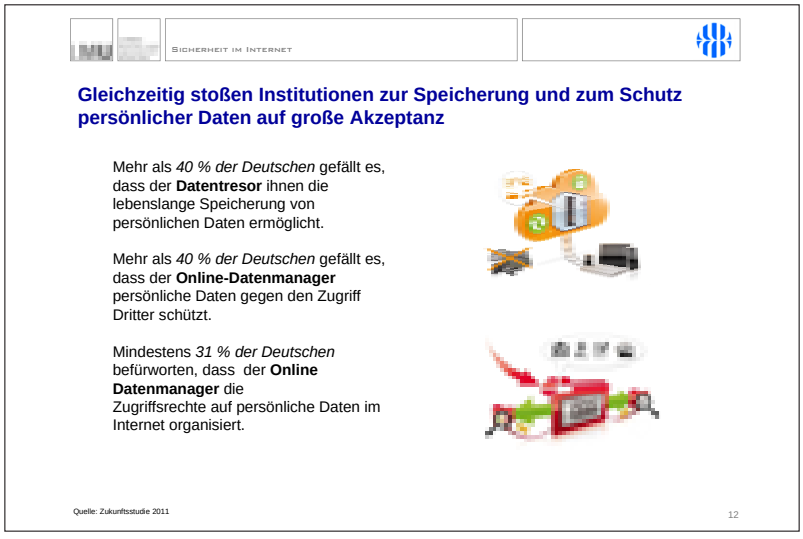


Bild 12

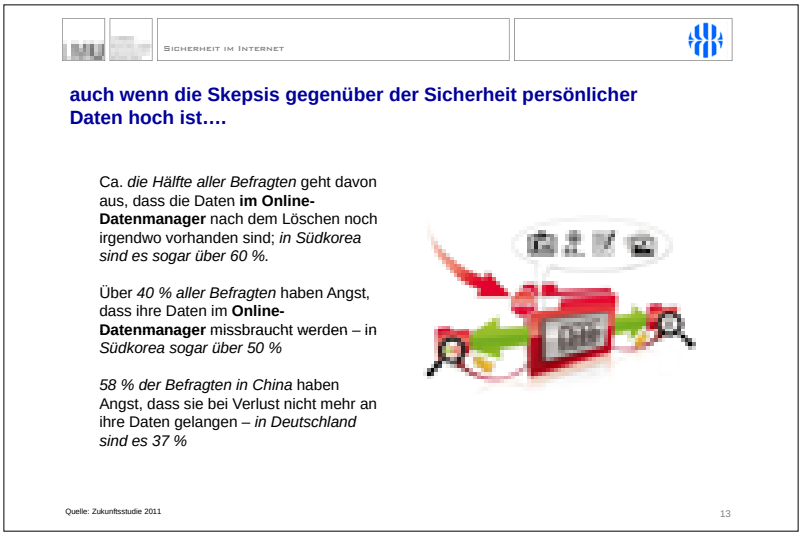


Bild 13

Bild 14

Weiter geht es hier beim intelligenten Arztbericht, beim Telemonitoring, bei der Nutzung eines Bürgerbüros und auch beim persönlichen Fernsehen. Auch hier wird überall eine Sorge von erheblichen Bevölkerungsanteilen in Bezug auf möglichen Datenmissbrauch geäußert. Das gilt auch für das Internet als einen mutmaßlich sicheren Ort für Datenspeicherung und Archivierung. Sorgen werden geäußert, dass das Löschen von Daten nicht nachhaltig stattfindet und dass die Daten irgendwie missbraucht werden könnten. Ich will die sicherheitsbezogenen Erkenntnisse zu allen Zukunftsbildern nicht im Einzelnen vortragen, sie lassen sich aus den Charts leicht erschließen. Festzustellen ist, dass es sich bei diesen Befunden um ein breit verankertes Gefühl und weit verbreitete Sorgen handelt.

Die Impressionen aus den aktuellen Studien zeigen, dass Sicherheit ein wirklich kritisches und strategisches Thema darstellt, mit welchem unsere Gesellschaft, unsere Wirtschaft so umgehen lernen muss, dass die Sicherheitsängste und die Angriffe auf die Sicherheit nicht letztlich die sozialen und wirtschaftlichen Vorteile der Internetnutzung aushebeln. Denn sonst können die Effizienz- und Innovationspotenziale des Internet und all seiner umgebenden Einrichtungen, Systeme und Institutionen in Wirtschaft, Gesellschaft und Verwaltung nicht gehoben werden. Darum geht es letztlich auch in unserer heutigen Konferenz. Es handelt sich also nicht nur um eine deutsche, sondern um eine weltweite Herausforderung. Nicht nur Unternehmer und Unternehmen, sondern auch Endnutzer und öffentliche Einrichtungen sind hier betroffen. Es geht um technische, aber auch um organisatorische und kulturelle Fragen bis hin zu Bildung und Erziehung. Sichere Prozesse sind zu organisieren, aber auch Identitäten zu sichern und Compliance mit beträchtlichen Anforderungen zu gewährleisten (Bild 15).

Bild 15

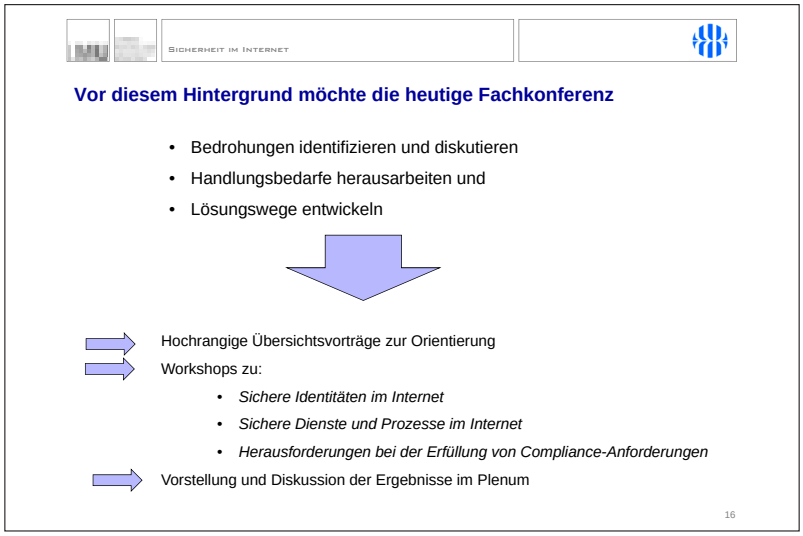


Bild 16

Somit ist dann der Rahmen für unsere heutige Veranstaltung abgesteckt (Bild 16). Wir möchten die Bedrohungen identifizieren und diskutieren, Handlungsbedarfe und Lösungswege mit Ihnen zusammen entwickeln. Dazu haben wir die Struktur gewählt, dass wir zunächst einige wichtige Übersichts- und Einführungsvorträge haben, die uns den technologischen, organisatorischen und rechtlichen Rahmen aufspannen und die sich grundsätzlich abzeichnenden Möglichkeiten skizzieren. Dann gehen wir in drei parallele Workshops, in denen wir die drei Themen Identität, Prozesse und Compliance intensiv diskutieren. Der genaue Ablauf wird nachher noch erläutert. Heute Nachmittag im Plenum führen wir die Ergebnisse zusammen und laden zur vertieften Diskussion ein.

Meine Damen und Herren, damit möchte ich überleiten zu unserer ersten Keynote und Einführungsvortrag, den dankenswerterweise Herr Marco Preuß übernommen hat. Herr Preuß ist der Head of Global Research and Analysis bei Kaspersky Deutschland. Er ist also an entscheidender Stelle in dem Ihnen allen bekannten Unternehmen Kaspersky tätig, das im Bereich der IT-Sicherheit – sowohl in der Sicherheitstechnologie als auch in der Sicherheitsberatung – eine ganz führende Rolle nicht nur in Deutschland, sondern weltweit einnimmt und daher über sehr interessante Informationen verfügt. Herr Preuß ist seit 2004 bei Kaspersky und übernahm 2010 die jetzige Position. Er hat zuvor 11 Jahre in verschiedenen IT-Unternehmen Erfahrung insbesondere im Bereich der IT-Sicherheit gesammelt. In seinem Aufgabenbereich beobachtet er die Bedrohungslandschaft in Mitteleuropa und beschäftigt sich mit Sicherheitslösungen in vielfältigen Kontexten. Herr Preuß, wir freuen uns auf Ihren Beitrag und danken Ihnen, dass Sie heute zu uns gekommen sind.

2 Bedrohung heute, Herausforderungen von Morgen

Marco Preuß, Kaspersky Labs GmbH, Ingolstadt

Mein Team und ich analysieren permanent neue Bedrohungen. Unsere Forschung dient auch dem Abschätzen neuer Gefahren und dem damit verbunden Schutz unserer Kunden. Folgend möchte ich Ihnen einen kleinen Überblick darüber geben.

Noch vor einigen Jahren, kamen die Bedrohungen hauptsächlich aus dem Amateur- und Hobbybereich (sog. Skript Kiddies), welche meist aus Jux und Tollerei oder auch aus purem Vandalismus irgendwelche Netzwerke und Systeme mit Würmern und Viren überlastet und infiziert haben.

In den letzten Jahren hat sich dies jedoch stark verändert und sich zum Bereich der Cyberkriminalität weiterentwickelt. Anhand von Statistiken kann man diesen Verlauf gut nachvollziehen. In den letzten Jahren hat sich die Reaktionszeit auf neue Bedrohungen stark verringert. Die profitgesteuerten Kriminellen – es geht im Untergrund nur um das Geld – haben hier nachgelegt und immer schneller, immer neuere Arten von Bedrohungen erstellt und in Umlauf gebracht. Man sieht, dass die Anzahl an Signaturen seit dem Jahr 2007 stark ansteigt. Derzeit haben wir über 7,5 Millionen Signaturen. Signaturen decken hierbei nicht nur einen Schädling ab, sondern meist eine Gruppe oder Familie, d.h. die tatsächliche Anzahl an Schädlingen ist weitaus höher.

Aber nicht nur Windows-PC-Systeme sind heutzutage Ziel von Angriffen. Auch alternative Plattformen, wie z.B. Mac-Systeme werden seit längerer Zeit angegriffen. Nahezu tagtäglich kommen neue Schädlinge heraus. Dies begann im Jahr 2006 als Apple auf die Intel-Plattform umgestiegen ist. Die Nutzeranzahlen von Mac-Systemen sind extrem gestiegen, wodurch die Kriminellen hier einen neuen profitablen Markt für sich entdeckt haben. Ebenso sind auch mobile Geräte bedroht. Android belegt im Bereich von mobilen Schädlingen über 85%.

Neben den Cyberkriminellen an sich, die nur profitorientiert agieren, sind neue Bedrohungen hinzugekommen, also neue Täter. Das ist einerseits Spionage, teilweise auch vermischt mit Sabotageakten und natürlich der sogenannte Hacktivismus, d.h. Gruppen, die aus politischen Motiven oder persönlichen Einstellungen heraus agieren, und Schaden anrichten.

Folgend ein paar Beispiele aus dem Untergrund. Eines der wichtigsten Tools sind natürlich Botnetze. Botnetze, ein Zusammenschluss von Rechnern, gibt es in unterschiedlichen Größen von einigen Hundert Rechnern bis mehreren Tausend. Erst gestern haben wir über das zweite HLUX-Botnet Sinkholing gesprochen, mit über 110.000 infizierten Clients, eingesetzt für Spamattacken und um private Daten und Adressen zu sammeln. Aktuelle Preise im Untergrund in sog. Discountershops, 1.000 Clients für 30 $.

Zum Aufbau solcher Botnetze werden meist professionelle Tools benutzt, sog. Exploit Kits, um Drive-by-Attacken durchzuführen. Hier ein Beispiel von Crime Pack. Es gibt eine ganze Fülle von Exploit Kits, die sich auf die unterschiedliche Bereiche spezialisiert haben. Sehr weit verbreitet ist zum Beispiel das Blackhole Exploit Kit, welches nicht gekauft wird, sondern nur als Service zur Verfügung gestellt wird, d.h. die Kriminellen nutzen Dienstleistungen im Untergrund welche wöchentlich oder monatlich gemietet werden.
Um gesammelte Daten zu verkaufen gibt eine Reihe an Untergrundforen um bspw. Accounts zu verkaufen.

In den letzten Jahren kamen zunehmend sog. Targeted Attacks, also die gezielten Attacken, hinzu. Ein Beispiel ist HBGary von denen über 50.000 teilweise höchst vertrauliche Emails geleakt wurden. Der Reputationsschaden der Firma führte zum Rücktritt des CEO. Ein weiteres Beispiel ist der RSA-Hack. Es gibt eine ganze Reihe ähnlicher Vorfälle, wo in Netzwerke eingedrungen und vertrauliche, sensible Daten gestohlen wurden. Diese Angriffe sind nicht auf Windows PCs beschränkt. Wenn die Kriminellen oder entsprechende Gruppen Interesse haben, in ein bestimmtes Netzwerk reinzukommen, spielen die Plattformen keine Rolle.

Ein ganz neues Thema ist natürlich auch der Cyberwar. Interessant ist hierbei, wenn ein Angriff nicht mehr nur virtuell im Umfeld des Internet stattfindet, sondern wenn diese Angriffe auch wieder auf die Realität zurückgeführt werden. Duqu und Stuxnet sind ebenfalls Beispiele hierfür, wobei Spionage bzw. Sabotage durchgeführt wurde (Bild 1).
Was erwartet uns in Zukunft? Was kommt noch so auf uns zu?

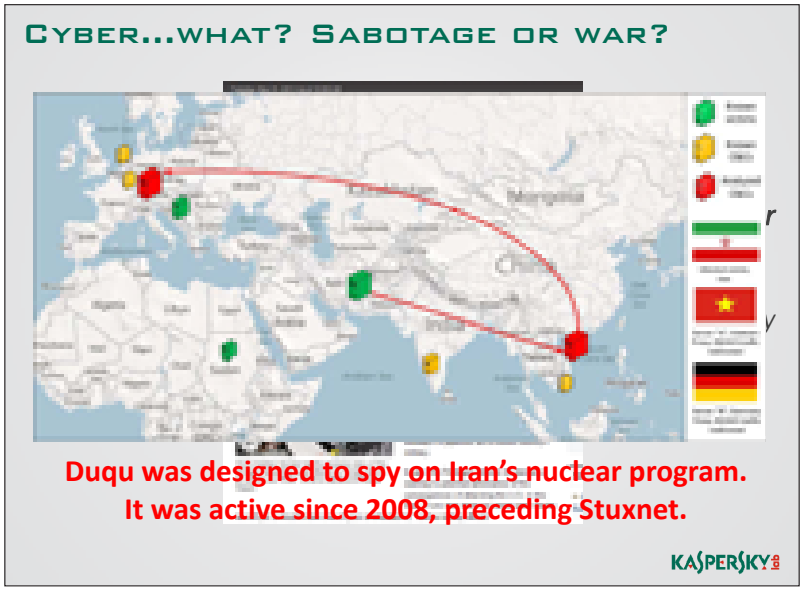


Bild 1

Neue Systeme, die mehr und mehr „smart“ werden. Beispielsweise im Medizinbereich, wenn Insulinpumpen oder auch Herzschrittmacher smarter werden, um remote kontrolliert zu werden. Hier zwei Beispiele mit existierenden Hacks (Bild 2). Welche neuen medizinischen Gerätschaften werden noch erfunden und sind angreifbar? Wie werden Kriminelle dies ausnutzen?

Bild 2

Ein weiteres Beispiel sind Drohnen (Bild 3). Diese Version wird seit 2001 eingesetzt. Bereits 2009 ist der erste Hack gelungen, wobei Aufnahmen der Kamera abgefangen werden konnten und direkt Einsätze live überwacht werden konnten. Zwei Jahre später wurde das komplette Kontrollzentrum einer solchen Drohnenarmee infiziert und die Aktionen mitgeloggt und ausgespäht.

Bild 3

Aber auch direkt in Hardware implementierte Backdoors sind neue Angriffsmethoden.
Ein Beispiel eines Cryptochip, mit implementierter Backdoor. Der Chip gibt den Verschlüsselungskey heraus und die vermeintlich sicheren Daten können gelesen werden.
Eine Bedrohung sind fest installierte Backdoors, bspw. nicht änderbare system-accounts wie bei diesen Storage-Systemen. Ein weiteres Beispiel an Kryptospeichern, mit eingebauter Backdoor.

Auch professionelle Einrichtungen sind nicht davor gefeit. Hier ein Chip mit eingebauter Backdoor, welches vom US Militär für den Einsatz in Raketen, Drohnen, Flugzeugen u. ä. bestellt wurde. Es wurden 59.000 solcher Chips gekauft (Bild 4).

Bild 4

Die Zukunft birgt noch eine ganze Reihe neuer Herausforderungen für uns - weit weg von klassischen PC Systemen. Die Entwicklung geht rasend schnell voran – wie man an der Entwicklung mobiler Geräte sieht.

3 Cybersicherheitsstrategie – Stand und nächste Schritte

Martin Schallbruch, Bundesministerium des Innern, Berlin

Meine sehr geehrten Damen und Herren, bedroht fühlen Sie sich jetzt offenbar alle schon, wie ich gelernt habe. Trotzdem kann man als Vertreter eines Innenministeriums nicht ganz darauf verzichten, ein paar Worte zur Bedrohung zu sagen, bevor ich dann zur Strategie der Cybersicherheit der Bundesregierung kommen werde.

Bild 1

Wir haben eben von Herrn Preuß schon viel gehört, wie sich Bedrohungslagen verändern. Ich will nur noch einmal kurz den Blick auf die Ursache der Cyberbedrohung richten, die wir im Augenblick erleben (Bild 1). Die Ursache liegt in technischen Schwachstellen der IT-Systeme, täglich neuen Schwachstellen in IT-Produkten, täglich neuen Schadprogrammen, die darauf aufgesetzt sind, daneben manipulierte Websites, die über Schwachstellen manipuliert werden können, weiterhin ein Schwarzmarkt, in dem Schwachstellen und Exploits gehandelt werden und letztlich eine steigende Komplexität der IT-Systeme, die die Verwundbarkeit weiter erhöht. Wenn Sie sich die IT-Vorfälle ansehen, die wir beispielsweise in den letzten Jahren im Regierungsumfeld und den Unternehmen hatten, stellt man fest, dass der häufigste Fall das Ausnutzen von Schwachstellen war, für die Patches schon vorhanden und entsprechende Updates nicht eingespielt worden sind. Kurzum: schlecht administrierte, schlecht betriebene IT-Systeme sind die größte Verwundbarkeit.

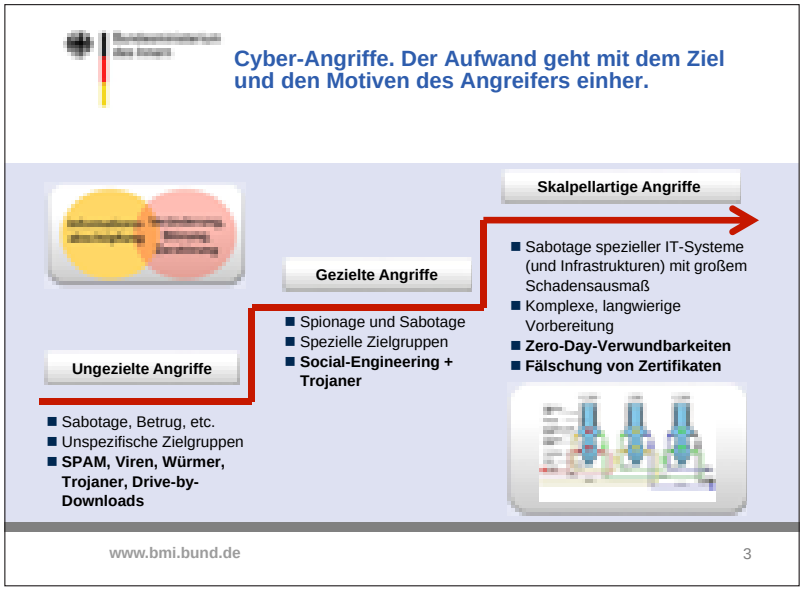


Bild 2

Wenn man sich die Art der Cyberangriffe anschaut, gewissermaßen eine technische Analyse, stellen wir hier eine Steigerung von Komplexität und auch Zielgerichtetheit der Angriffe fest (Bild 2). Die ersten sogenannten Cyberangriffe waren recht ungesteuert. Ob das Denial of Service Attacks gegen Online-Casinos waren, ob das Phishing, Pharming oder ähnliche Attacken waren: die Angriffe waren nicht sehr zielgerichtet. Das waren erste Schritte. Technologien, SPAM, Würmer, Viren, Trojaner usw.

Die nächst komplexere Stufe, die die vorige nicht abgelöst sondern ergänzt hat, sind gezielte Angriffe aus Motiven der Spionage oder Sabotage. Wir erleben im Augenblick im Schnitt fünf gezielte Spionageangriffe pro Tag auf die Regierungsnetze der Bundesregierung, die wir durch die an den Grenzen der Netze vom BSI errichteten Schadprogramm-Erkennungs- und -Analysesysteme entdecken. Das sind gezielte Angriffe. Das sind keine irgendwie flächendeckenden Massenangriffe nach dem Motto: es könnte vielleicht eine Information aus der Bundesregierung ins Netz gehen, sondern das sind auf spezifische Adressaten, Ministerien, Behörden gerichtete Angriffe: Häufig haben solche Angriffe auch mit Social Engineering zu tun: Dass man an der Stelle eine Beziehung zu einem Adressaten herstellt und versucht, sie auszunutzen, um einen Trojaner zu platzieren.

Eine neue Qualität, die 2010/11 dazugekommen ist, sind sogenannte skalpellartige Angriffe – Herr Preuß hatte dazu bereits Beispiele gebracht -, die sich sehr gezielt gegen spezifische IT-Systeme mit Steuerungsverantwortung richten. Das prominenteste Beispiel ist natürlich Stuxnet. Solche skalpellartigen Angriffe, die bestimmte Systeme beeinträchtigen wollen, nutzen typischerweise Zero-Day-Exploits aus und sind häufig auch mit sehr ausgefeilten Überwindungen von Sicherheitstechnologien verbunden. Was wir in den letzten Jahren auch erlebt haben, sind Angriffe gegen Sicherheitsinfrastrukturen des Internets. Stichwort: DigiNotar; sie dienen zur Vorbereitung solcher skalpellartiger Angriffe, z.B. gegen Prozessteuerungsanlagen.

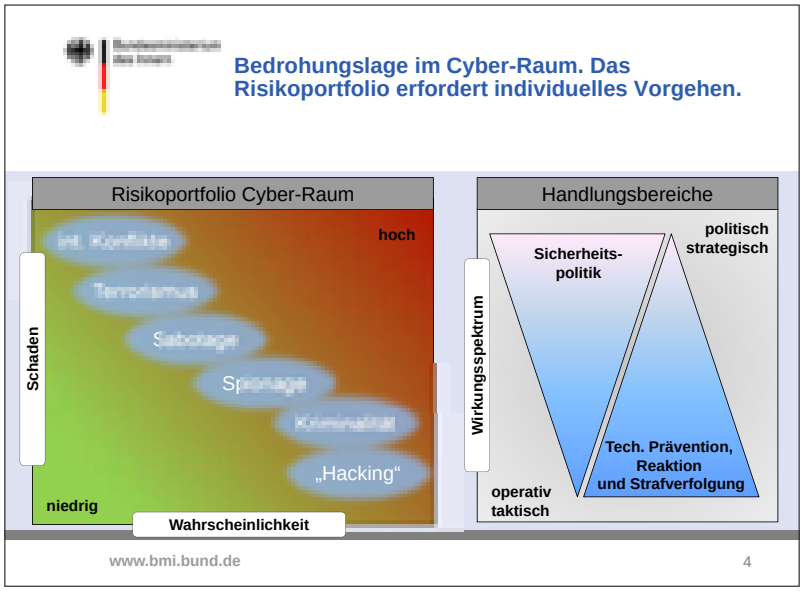


Bild 3

Wenn man sich die Motivlagen für Cyberangriffe anschaut, finden wir ein ganzes Bündel (Bild 3). Praktisch jede Form von Kriminalität finden wir auch im Cyberspace, sei es Spionage, Sabotage, organisierte Kriminaltität, die Organisation terroristischer Gruppierungen usw. Betrug ist natürlich das größte Massenphänomen, was wir im Bereich der Cyberkriminalität haben. Das bildet sich allerdings nicht in den polizeilichen Kriminalstatistiken ab. Die Zahlen dort sind noch verhältnismäßig gering. Wenn Sie sich aber Infas-Bürgerumfragen „Waren Sie schon einmal von Betrug im Internet betroffen?“ vom vergangenen Sommer anschauen, haben 8,4 Millionen Menschen in Deutschland das bejaht. Die Betroffenheit reichte von Abo-Fallen über Phishing bis zu Waren- und Terminbetrug. An der Diskrepanz zwischen der polizeilichen Kriminalstatistik und dieser Umfrage sieht man, dass eine große Dunkelziffer besteht und dass wir hier im Hellbereich nur einen kleinen Teil sehen, weil in der Regel die Diensteanbieter den Betroffenen die Schäden abnehmen und deshalb keine Anzeigemotivation da ist.

Diesem sehr komplexen Risiko auf der technischer Ebene und auch auf Ebene der Kriminalitätsphänomene zu begegnen, erfordert ein Handeln sowohl auf einer politisch-strategischen als auch auf einer operativ-taktischen Ebene.

Um die Cybersicherheit zu verbessern, müssen wir unsere IT-Systeme sicherer machen. Das ist etwas, was die IT-Administratoren, die verantwortlichen Produkthersteller, die Dienstebetreiber betrifft. Das betrifft aber auch die Managementebenen, die Vorstände und Geschäftsführer von Unternehmen, die Behördenleiter usw., die sich klar machen müssen, wie abhängig sie von welchen IT-Systemen sind und sie ihre Kerngeschäftsprozesse schützen können. Es ist sozusagen eine ‚Bottom-up‘ und eine ‚Top-down‘ Aktivität, die hier parallel erfolgen muss.

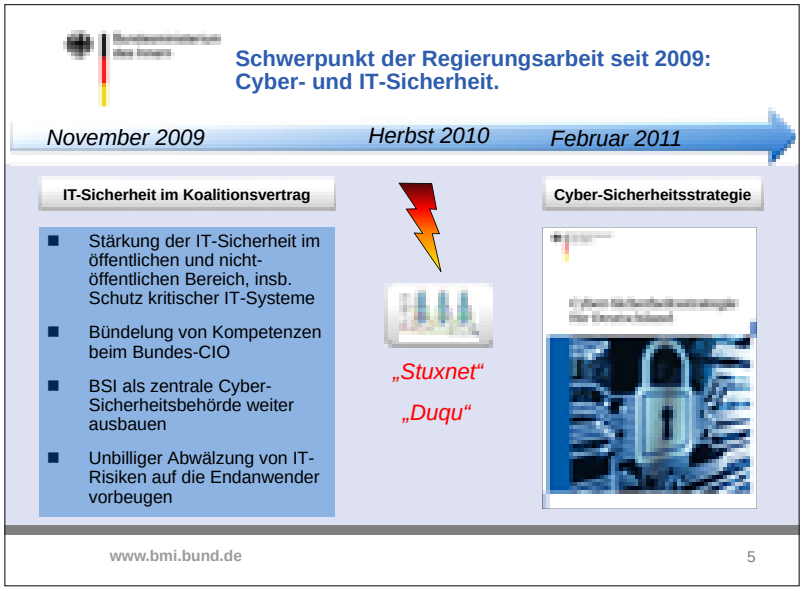


Bild 4

Für die Bundesregierung ist das Thema Cybersicherheit seit den Koalitionsvereinbarungen von CDU/CSU und FDP im Herbst 2009 ein besonders wichtiges Thema geworden (Bild 4). Wir haben sehr deutliche Verabredungen zwischen den die Bundesregierung tragenden Parteien, was den Ausbau der Cybersicherheit angeht. Das BSI ist beispielsweise die einzige Bundesbehörde, die aufgrund des Koalitionsvertrags überhaupt ausgebaut wird. In allen anderen Bereichen wird eingespart.

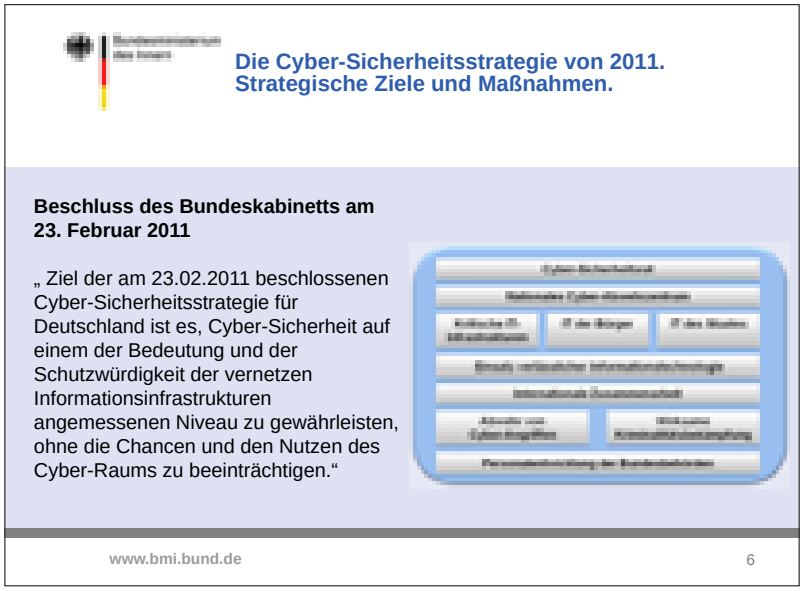


Bild 5

Wir haben als Ausformung dieses Auftrags der Koalition in der Bundesregierung im Februar 2011 eine Cybersicherheitsstrategie beschlossen, die das Thema insgesamt adressiert (Bild 5). Sie hat das Ziel, den Cyberraum sicher zu machen und gleichzeitig die Chancen, den Nutzen, die Möglichkeiten und auch die wirtschaftliche und gesellschaftliche Innovation, die im Internet, im Cyberspace liegt, zu erhalten und weiter auszubauen.

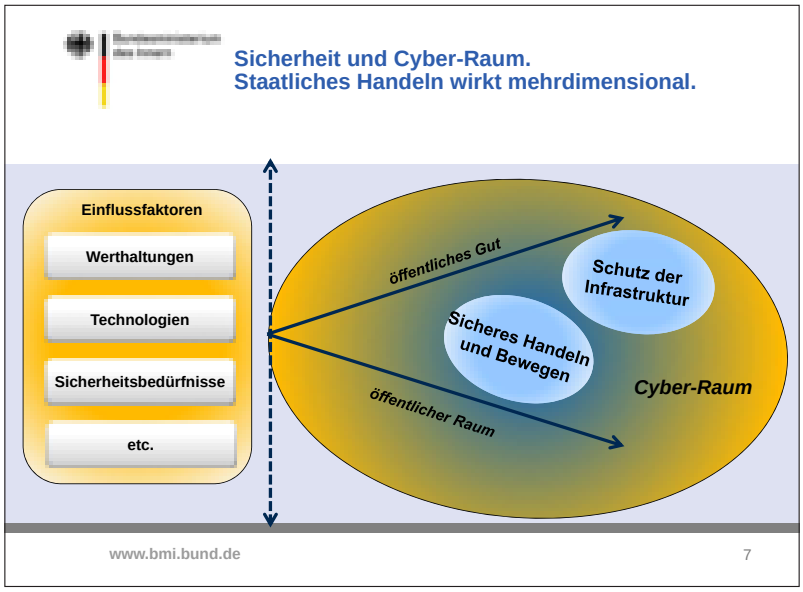


Bild 6

Ich werde einige der in der Cybersicherheitsstrategie definierten Maßnahmenbereiche vorstellen können (Bild 6). Einige, auf die ich nicht eingehen kann, sind natürlich auch der Ausbau der polizeilichen Kriminalitätsbekämpfungsmöglichkeiten, auch durch Weiterqualifizierung des Personals, die Investition in die Forschung und Entwicklung von Sicherheitstechnologien. Auf andere Bereiche werde ich näher eingehen.

Der Grundgedanke unserer Cybersicherheitsstrategie ist eine präventive Sicherheitspolitik, die den Cyberspace einerseits als eine Infrastruktur sieht, die erforderlich für unser Leben, Wirtschaften, Arbeiten, Handeln ist; sozusagen: der Cyberspace als öffentliches Gut. Ohne Cyberspace können wir das Leben, was wir führen, so nicht mehr führen. Wir können die Innovationen, die die Unternehmen haben wollen, nicht realisieren. Zum anderen müssen wir den Cyberspace aber auch als öffentlichen Raum begreifen, in dem wir leben. Wir haben im Jahr 2010 sehr intensive Diskussionen zur Netzpolitik durchgeführt, einen langen Dialog mit verschiedensten Beteiligten damals noch unter der Leitung von Minister de Maizière, und haben netzpolitische Grundsätze des Bundesinnenministeriums formuliert. Ein ganz wichtiger Punkt hierbei ist: der Cyberspace ist für uns ein öffentlicher Raum, in dem wir leben, arbeiten, handeln und entsprechend den Grundsätzen unserer Innenpolitik gilt auch hier: die Menschen sollen auch im Cyberspace frei und sicher leben. Das sind zwei unterschiedliche Ziele, der infrastrukturelle Aspekt, aber auch der Aspekt, dass wir uns im Cyberspace aufhalten und unser Leben ein Stück weit dort verbringen.

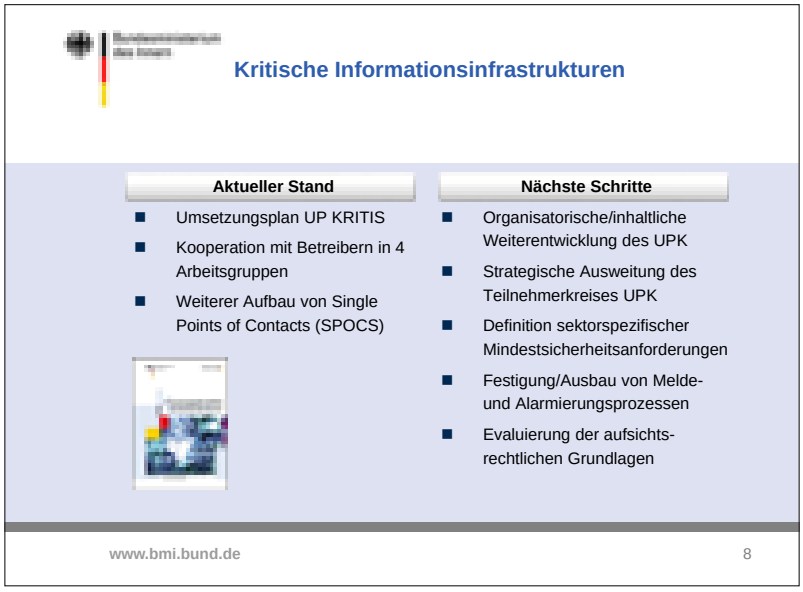


Bild 7

Höchste Priorität in unserer Cybersicherheitsstrategie hat der Schutz der kritischen Informationsinfrastrukturen (Bild 7). Das ist eigentlich weltweit in allen relevanten Bereichen so. Wir haben an dieser Stelle auch schon viel früher angefangen als in anderen Bereichen der Cybersicherheit. In Deutschland hat die Zusammenarbeit mit den kritischen Infrastrukturen in Bezug auf die IT, die Informationssicherheit, 2007 begonnen. Wir haben damals mit dem Umsetzungsplan KRITIS eine Zusammenarbeit zwischen Staat und Wirtschaft etabliert, dieser Zusammenarbeit einen Rahmen gegeben, in dem wir gemeinsam agieren. Der Umset-

zungsstand ist inzwischen so fortgeschritten, dass wir hinsichtlich mancher Branchen sagen würden, dass kaum Wünsche offen bleiben. Die Zusammenarbeit zwischen Staat und Wirtschaft ist gut. Die Branche ist gut aufgestellt. Es gibt Lagezentren, Single Points of Contact, die mit staatlichen Behörden zusammenarbeiten usw. Aber das ist nicht in allen Branchen so. Gute Beispiele sind Versicherungswirtschaft und Banken. Es gibt andere Bereiche, die viel komplizierter strukturiert sind. Wenn Sie allein an die Wasserversorgung o. ä. denken, wo viele kommunale Betriebe Verantwortung tragen: dort ist es sehr viel schwieriger, einen Rahmen für die Zusammenarbeit zwischen kritischer Infrastruktur und Staat zu organisieren.

Im nächsten Schritt werden wir allerdings zu einem gleichmäßigeren Schutz aller KRITIS-Branchen kommen müssen. Das diskutieren wir gerade im UP KRITIS, und wir diskutieren es auch innerhalb der Bundesregierung im Hinblick auf notwendige gesetzgeberische Maßnahmen. Wir haben einen Auftrag aus der Cybersicherheitsstrategie, die rechtlichen Instrumente zu prüfen. Wichtige Punkte sind hier natürlich Melde- und Alarmierungsprozesse, sektorspezifische Mindestsicherheitsanforderungen, aber auch die aufsichtsrechtlichen Grundlagen, weil kritische Infrastrukturen in Deutschland typischerweise schon reguliert sind durch Eisenbahngesetz, Telekommunikationsgesetz, Kreditwesengesetz usw. Das heißt, wir haben sektorspezifische Regulierung, und Cybersicherheit muss auch dort einfließen, so wie auch die Aufsichtsbehörden in dem jeweiligen Bereich sich zunehmend auch mit Fragen der Cybersicherheit beschäftigen müssen.

Regulierung und freiwillige Zusammenarbeit müssen sich hier in einem guten Verhältnis finden. Wir sind mit unserem Partner in dem UP KRITIS einig, dass wir den Unternehmen und auch den Branchen das Wie der Umsetzung von Sicherheitsanforderungen weitgehend überlassen wollen, weil Branchen dafür zu unterschiedlich strukturiert sind. Da wir als Staat allerdings die Verantwortung für das Funktionieren des Landes insgesamt haben, müssen wir übergreifende Anforderungen definieren, die nötig sind, damit kritische Infrastrukturen auch unter dem verschärften Cybersicherheitsbedingungen dauerhaft funktionieren. Sie sind dann branchenspezifisch herunterzubrechen.

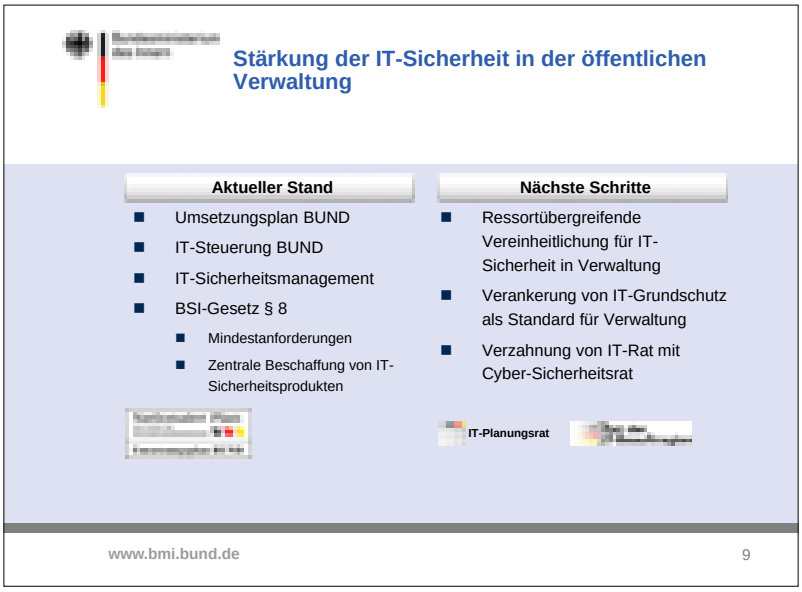


Bild 8

Kritische Infrastruktur ist natürlich auch die IT des Staates (Bild 8). Insofern ist auch das einer der wichtigen Punkte in der Umsetzung der Cybersicherheitsstrategie. Für die Bundesverwaltung haben wir durch entsprechende Regeln, Umsetzungsplan Bund u. ä., sowie durch eine Änderung des BSI-Gesetzes 2009 schon wesentliche Grundlagen geschaffen.

Eine sehr große Bedeutung in der praktischen Arbeit hat das Thema im IT-Planungsrat. Die deutsche Verwaltung ist ja föderal organisiert und wir haben eine kommunale Selbstverwaltung. In den Ländern und Kommunen haben wir uns im IT-Planungsrat darauf verständigt, dass wir eine IT-Sicherheitsleitlinie erarbeiten wollen, die Sicherheitsmanagement für alle deutschen Behörden vorgibt. Durch die Möglichkeiten des IT-Planungsrates, der aufgrund einer Grundgesetzänderung geschaffen wurde, haben wir nunmehr die Chance, verbindliche IT-Sicherheitsvorgaben für alle deutschen Behörden von der kommunalen Ebene bis zur Bundesebene zu machen. Daran wird gearbeitet und ich hoffe, dass wir im Herbst eine solche Sicherheitsleitlinie haben werden.

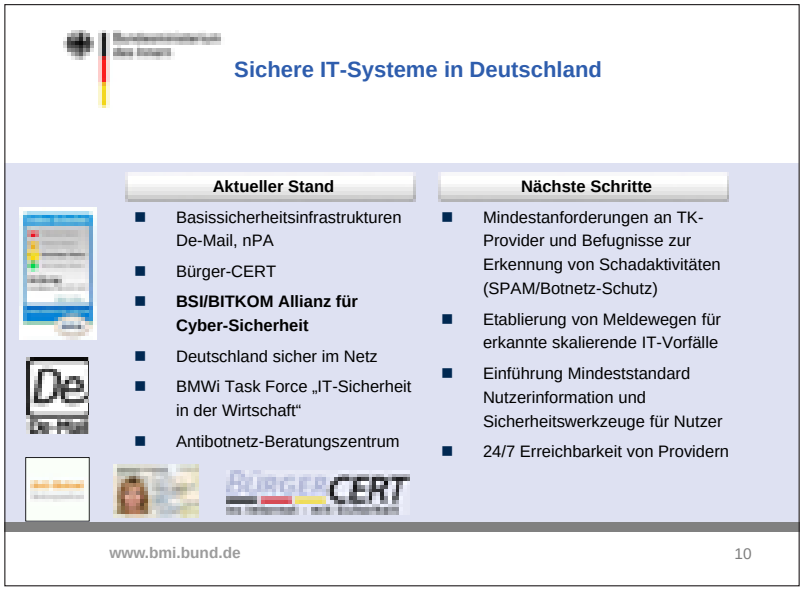


Bild 9

Den dritten Bereich der Strategie haben wir „sichere IT-Systeme in Deutschland“ genannt (Bild 9). Damit meinen wir die IT-Systeme, die bei den Bürgerinnen und Bürgern, bei den Unternehmen im Einsatz sind. Auch hier müssen wir das Sicherheitsniveau erhöhen. Wenn Sie sich Denial of Service Attacks oder Ähnliches ansehen, dann ist es nicht so, dass diese von Botnetzen ausgeführt werden, deren Bots überwiegend in Uruguay oder Kasachstan stehen und von dort beispielsweise Server der Bundesregierung oder eines Konzerns angreifen. Vielmehr sind die Bots typischerweise Systeme, die hier im Land oder den europäischen Nachbarländern im Einsatz sind, die von Bürgerinnen und Bürgern betrieben werden, die keine Ahnung haben, dass ihr System einen Trojaner hat und Teil eines Botnetzes ist. Die Angriffe werden über unsere Netze hier im Land auf unsere Einrichtungen gefahren.

Das werden wir nur verändern können, wenn wir das Cybersicherheitsniveau in Deutschland insgesamt erhöhen. Wir haben da in den letzten Jahren eine ganze Menge getan. Einige Beispiele seien hier erwähnt. Das Anti-Botnetz Beratungszentrum ist eine gemeinsame Initiative des BSI und der deutschen Internetprovider, die die Aktivität von Botnetzen in Deutschland schon spürbar hat senken können. Da bekommen die Betroffenen von ihrem Provider mitgeteilt, dass sie möglicherweise Teil eines Botnetzes sind und Möglichkeiten gezeigt, wie sie herauskommen können, von technischen Tools bis hin zur telefonischen Hotline. Das hat als Projekt begonnen und wir würden es gern verstetigen und zu einer Dauereinrichtung machen.

Wir sehen die Provider in einer Schlüsselrolle. Sie sind diejenigen, die die Menschen mit dem Internet verbinden. Hier sehen wir die Notwendigkeit, die Verantwortung wahrzunehmen, die Nutzerinnen und Nutzer möglichst sicher ans Internet zu lassen, Hilfestellungen zu geben, Tools zur Verfügung zu stellen, mit den Behörden zusammenzuarbeiten, Informationen über die statistischen Vorfälle zu liefern, die man hat usw. Da sehen wir den Provider in der Pflicht, seine Kunden zu schützen und damit die Gesamtsicherheit in Deutschland zu erhöhen. In dieses Handlungsfeld fällt auch die Förderung von Sicherheitstechnologien, die das Handeln, Leben, Arbeiten im Cyberspace sicherer machen. Beispiele sind der neue Personal-

ausweis, der am 1.11.2010 als eine solche Sicherheitstechnologie eingeführt worden ist, mit der wir technologisch aber auch im Hinblick auf Datenschutz und Datensicherheit Vorreiter sind. Ein anderes Beispiel: De-Mail als sichere Kommunikationsmöglichkeit. Wir haben seit der CeBIT die ersten De-Mail Provider, die akkreditiert sind und ihre Dienste anbieten. Damit steht eine Technologie zur Verfügung, die sichere Kommunikation in Deutschland flächendeckend auch für die Bürgerinnen und Bürger erlaubt. Wir bereiten gerade das eGovernment-Gesetz vor, das die Nutzung von De-Mail und neuem Personalausweis gerade in Verwaltungsangelegenheiten sehr stark vereinfacht, so dass wir hier auch zu einer weiteren Förderung der Nutzung kommen werden.

Bild 10

Als wir die Cybersicherheitsstrategie entwickelt haben, haben wir auch darüber diskutiert, wie wir unsere Behördenlandschaft anpassen, um den Cyberbedrohungen besser Herr zu werden. Es wird immer diskutiert, bei welcher Behörde man die Aufgabe der Cybersicherheit ansiedelt. Nach einer sehr gründlichen Analyse und Diskussion sind wir zu dem Ergebnis gekommen, dass wir eine Struktur brauchen, die die verschiedenen Behörden bei dieser Aufgabe dauerhaft miteinander verklammert. Natürlich soll das Eisenbahnbundesamt weiterhin zuständig sein dafür, dass Eisenbahnen sicher sind und nicht zusammenstoßen, aber auch nicht aus dem Cyberspace angegriffen werden mit dem Ziel der Beeinflussung von Steuerungssystemen. Natürlich soll die Atomaufsicht für Atomkraftwerke zuständig sein. Natürlich haben wir eine BaFIN, die Bankenaufsicht macht und das Risikomanagement der Banken auch im Hinblick auf IT-Sicherheit prüfen sollte. Natürlich haben wir Strafverfolgungsbehörden und Nachrichtendienste, die Strafverfolgung im Cyberspace intensiver betreiben müssen als in der Vergangenheit und nachrichtendienstlich ihre Grundlagen ausbauen müssen. Wir haben daneben eine für Cybersicherheitsfragen zuständige Spezialbehörde: das BSI.

Weil wir diese Notwendigkeit der Vernetzung gesehen haben, wollten wir keine neue Behörde schaffen oder alles bei einer Behörde konzentrieren, sondern nach dem Vorbild des gemeinsamen Terrorabwehrzentrums ein Cyberabwehrzentrum schaffen, das die verantwort-

lichen Behörden zusammenbringt und das eine ganzheitliche Lagebeurteilung und eine abgestimmte Festigung von Maßnahmen ermöglicht (Bild 10). Dieses Cyberabwehrzentrum unter Federführung des BSI hat am 1.4.2011 seinen Betrieb aufgenommen. Wir haben es seitdem in mehreren Schalen erweitert. Es gab drei Behörden, die begonnen haben. Sieben weitere Behörden kamen im Juni 2011 dazu. Heute sind neben BSI, Verfassungsschutz und Katastrophenschutzbehörde das Bundeskriminalamt, das Zollkriminalamt, die Bundespolizei, die Bundeswehr, der militärische Abschirmdienst und der BND dabei. Wir sind gerade dabei, die dritte Schale zu bauen, nämlich die Aufsichtsbehörden für die kritischen Infrastrukturen an dieses Cyberabwehrzentrun anzubinden. Das sind solche Ämter, wie ich sie schon genannt habe; Luftfahrtbundesamt, Eisenbahnbundesamt, BaFIN usw., also Behörden, die über bestimmte Sektoren der kritischen Infrastrukturen eine spezielle Aufsicht haben und dabei Cybersicherheitsaspekte berücksichtigen müssen.

Wir haben gute Erfahrungen gemacht mit dem Cyberabwehrzentrum, wenn es darum geht, komplexe schwierige Großlagen mit Auswirkungen in verschiedene Bereiche zu koordinieren, den Informationsaustausch zu organisieren. Wir haben im November/Dezember 2011 über zwei Tage auch eine entsprechende Übung namens Lükex durchgeführt, in der wir eine Cyberattacke auf Deutschland gemeinsam mit fünf Ländern und 30 Unternehmen geübt haben.

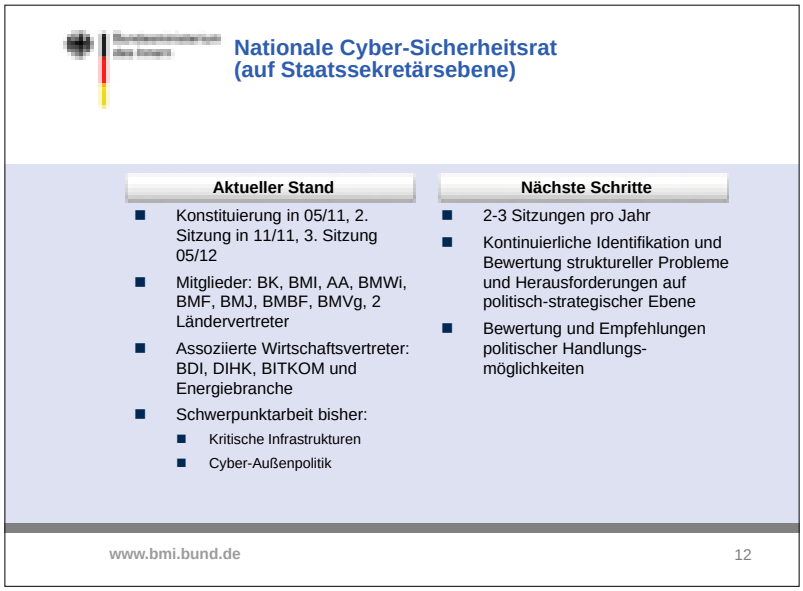


Bild 11

Natürlich muss auch eine politische Koordinierung erfolgen (Bild 11). Hierfür haben wir einen Cybersicherheitsrat auf Staatssekretärsebene unter Vorsitz der Beauftragten der Bundesregierung für Informationstechnik, Frau Rogall-Grothe, gegründet, der die strategische Steuerung der Cybersicherheitsstrategie übernimmt. Es sind die relevanten Ressorts, zwei Vertreter der Länder, die die Innenministerkonferenz geschickt hat, und auch die Wirtschaftsverbände vertreten. Da sprechen wir über kritische Infrastrukturen, über Cyberaußenpolitik, über Ausrichtung der Cybersicherheits-Forschungsförderung u. ä.

Bild 12

Über die nationale Arbeit hinaus ist Cybersicherheit eines der Themen, bei dem wir eine ganz intensive internationale Zusammenarbeit brauchen (Bild 12). Das ist eine allgemeine Erkenntnis, die uns im Augenblick etwas zu schaffen macht, weil sie dazu führt, dass praktisch in jeder bilateralen, multilateralen, internationalen Zusammenarbeit und in jeder internationalen Organisation Cybersicherheitsaspekte diskutiert werden. Wir haben schon in der NATO intensive Diskussionen geführt über die NATO-Strategie. Wir haben jetzt eine ganz intensive Diskussion im Bereich der Vereinten Nationen begonnen, an der wir uns sehr beteiligen. Es ist unser politisches Anliegen, auf internationaler Ebene so etwas wie „Norms of State Behavior“ zu definieren als Softlaw Regeln, wie sich Staaten im Cyberspace verhalten, wie sie zusammenarbeiten, wie sie bei grenzüberschreitenden Angriffen miteinander kooperieren, wer wen unterrichtet usw.. Das sind schwierige Themen, weil es da einer Weiterentwicklung des Völkerrechts bedarf. Aber der Weg, der jetzt begangen wird, ist vernünftig: über Softlaw zu einer Vereinheitlichung von Regeln und zu einer Vereinbarung zu kommen, die dann in einigen Jahren zu einer Weiterentwicklung des Völkerrechtes auch im klassischen formellen Sinne führen kann. In dieser UN-Expertengruppe arbeiten wir mit und bringen unsere Ideen ein, nachdem wir es schon sehr intensiv im G8-Bereich und vor allem gemeinsam mit Frankreich, USA und UK vorgedacht haben und mit diesen drei Staaten auch gemeinsam entsprechende Papiere entworfen haben, welche Inhalte solche Norms of State Behavior haben sollten.

Ein wichtiger Punkt bei der internationalen Arbeit ist für uns naturgemäß der Schutz kritischer Infrastrukturen. Da wird Deutschland Gastgeber für die Meridian-Konferenz im November 2012 sein. Das ist eine globale Konferenz zum Schutz kritischer Informationsinfrastrukturen, eine Regierungskonferenz, wo wir dieses Thema voranbringen werden.

Ganz entscheidend für uns ist die Zusammenarbeit in der Europäischen Union. Das ist sozusagen der internationale Kreis, mit dem wir am engsten verknüpft sind. Wir haben in der EU schon seit etlichen Jahren eine Zusammenarbeit in Fragen der Informationssicherheit und Netzwerksicherheit. Wir haben die europäische Agentur für Netzwerk- und Informations-

sicherheit (ENISA) und setzen uns dafür ein, dass das Mandat der ENISA erweitert und verlängert wird und dass die Informationssicherheit in der Europäischen Union einen noch festeren Platz bekommt, auch was die IT-Sicherheit der Europäischen Einrichtungen selbst angeht. Da sehen wir als Bundesregierung durchaus noch deutlichen Nachholbedarf und würden uns wünschen, wenn Kommission, Rat und Parlament mit Unterstützung der ENISA mehr tun würden.

Wir begrüßen es, dass die zuständige EU Kommissarin Frau Kroes angekündigt hat, bis zum Ende diesen Jahres eine Cybersicherheitsstrategie für die Europäische Union vorzulegen und haben hier bereits Input gegeben.

Meine Damen und Herren, das war der Überblick über die Cybersicherheitsstrategie der Bundesregierung und den Stand der Umsetzung. Das sind sehr viele verschiedene Handlungsstränge und Handlungsfelder und ich freue mich, dass der Münchner Kreis mit der heutigen Konferenz gleich mehrere dieser Handlungsstränge und Handlungsfelder aufgegriffen hat und vorantreibt.

4 Sicherheit in Telekommunikationsnetzen – neueste Entwicklungen

Thorsten Schneider, Nokia Siemens Networks GmbH, München

Ich werde über das Thema Sicherheit in den Telekommunikationsnetzen sprechen und mich vor allem auf die neuesten Entwicklungen in dem Bereich fokussieren.

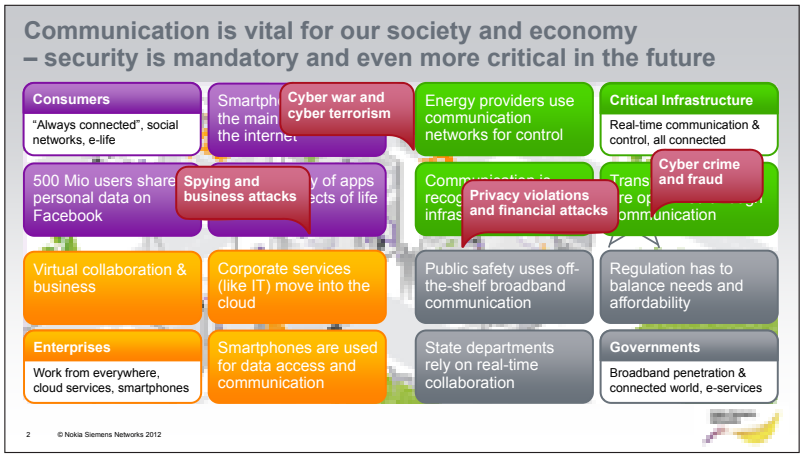


Bild 1

Heute werden die Telekommunikationsnetze von einer ganzen Reihe von verschiedenen Nutzern verwendet, um Informationen auszutauschen, um zu kommunizieren, aber auch um ihre Prozesse darüber abzuwickeln (Bild 1). Wir haben auf der einen Seite die privaten Nutzer, die den Mobilfunk aber auch das Festnetz dafür verwenden um sich in Sozialen Netzwerken zusammenzuschließen, um Bankgeschäfte abzuwickeln oder auch um in Online Shops einzukaufen. Auf der anderen Seite haben wir die Unternehmen, die heute ihren Mitarbeitern mobile Endgeräte zur Verfügung stellen oder die auch ihren Mitarbeitern immer häufiger erlauben, ihre eigenen mobilen Geräte, sei es das Smartphone, sei es Tablets mitzubringen. Über diese Geräte wird natürlich auf die Firmendaten zugegriffen. Auf der anderen Seite werden die Firmendaten, aber auch private Daten auf diesen Geräten gespeichert. Der Zugriff auf die Daten erfolgt nicht nur im Bereich der Unternehmen sondern wo immer der entsprechende Mitarbeiter dann ist, entweder in Deutschland oder aber auch im Ausland, und mit den entsprechenden Herausforderungen der Verbindung, aber auch der Sicherheit.

Verschiedene Industrien nutzen heute schon sehr stark Telekommunikationsnetze für ihre Prozesse. Es ist auch in den beiden Vorträgen vor mir angeklungen, dass dies für die Energienetze, Stichwort Smart Grid, aber auch für Produktionsunternehmen, z.B. Nutzung von Machine-to-Machine Kommunikation oder für Versorgungsnetze im allgemeinen zutrifft. Auch in Transport oder Logistik wird heute sehr viel abgewickelt über Online oder Real Time Communication und Probleme bei der Kommunikation haben direkten Einfluss, wenn an der Stelle etwas nicht funktioniert oder wenn entsprechend etwas verändert und dann fehlgeleitet wird.

Herr Schallbruch hat darüber gesprochen, dass auch staatliche Behörden die öffentlichen Telekommunikationsnetze nutzen, z.B. Polizei und Feuerwehr. Wenn wir gerade auch über die neueren Technologien nachdenken, z.B. über das 4G, dann wird in Deutschland heute, nicht aber in anderen Ländern, die LTE-Technologie genutzt, um Polizeiinformationen,

sogenanntes Public Safety LTE über diese Netze zu transportieren. Damit erreicht man höchstmögliche Datenbreite um Informationen möglichst schnell inklusive von Bildern und Detailinformationen übermitteln zu können.

Durch diese Nutzung und auch durch die Daten, die hier transportiert werden, entsteht natürlich ein wirtschaftliches und auch politisches Interesse, diese Infrastrukturen anzugreifen, um sie entweder zu beschädigen, teilweise lahmzulegen oder aber auch, um Informationen daraus zu stehlen.

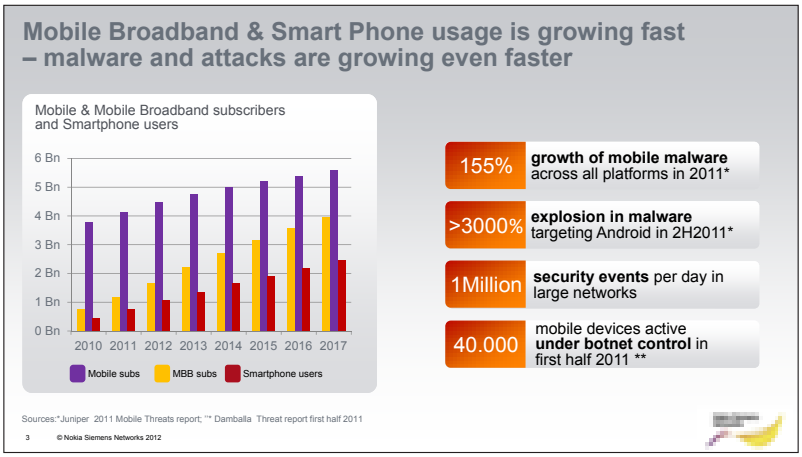


Bild 2

Wenn wir ein bisschen näher auf die Mobilfunknetze im Spezifischen eingehen, wenn wir sehen, wie die Nutzung dieser Netze wächst, haben wir heute schon weltweit über vier Milliarden Nutzer in Mobilfunknetzen (Bild 2). Wir werden dieses Jahr über eine Milliarde Nutzer von Smartphones haben. Allein letztes Jahr sind um die 500 Millionen Smartphone Nutzer dazu gekommen, also Smartphone und Tablet Nutzer an der Stelle, um Ihnen ein bisschen ein Gefühl zu geben, wie schnell sich dieses Thema entwickelt und wie viel das an Anforderungen an die Telekommunikationsnetze stellt. Wir gehen davon aus, dass im Jahr 2020, was noch ein paar Jahre in der Zukunft liegt, aber nicht mehr so sehr weit weg ist, pro Nutzer pro Tag ungefähr ein Gigabit über diese Netze transportiert wird. Natürlich werden einzelne Nutzer entsprechend mehr und andere etwas weniger Daten transferieren, aber es ist schon ein sehr hoher Datenaustausch und Verkehr, der hier stattfindet.

Auf der anderen Seite sehen wir, getrieben durch diese Entwicklung und auch in den letzten zwölf Monaten getrieben durch die Explosion der Nutzung von Smartphones, die auch noch weiter geht, ein sehr starkes Wachstum bei den Schadprogrammen, die auf diese Infrastrukturen und diese Endgeräte abzielen. Über die gesamten IOS, über die gesamten Plattformen hinweg, haben wir mehr als 150% Wachstum der Schadprogramme gesehen. Wenn man allein das Android Thema nimmt, sind es über 3000 % Wachstum, also ein exponentieller Anstieg. Ich denke, dass wir auch in den nächsten Monaten und Jahren einen weiteren kontinuierlichen Anstieg sehen werden. Aber auch Beispiele, wo wirklich täglich in großen Netzen eine extrem große Anzahl von Angriffen stattfinden.

Viele dieser Angriffe kommen nicht in die Presse und sind deswegen nicht sichtbar. Über einige, die wirklich in die Presse kommen, haben Sie vorher Beispiele gesehen. Die meisten dieser Themen betreffen allerdings den Bereich der IT und auch das Festnetz. Aus dem Bereich des Mobilfunks sieht man heute relativ wenig, wobei natürlich gerade durch das

Thema Android usw. schon viel mehr Themen in die Presse gekommen sind.
Die Probleme werden erwähnt, aber die konkreten Informationen sind oft in der Presse noch nicht so detailliert wie insgesamt in dem Security Thema.

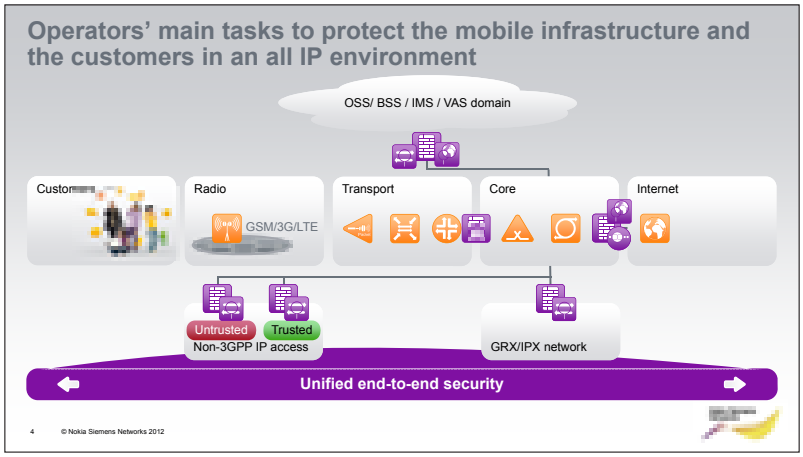


Bild 3

Wenn wir ein bisschen näher auf die Mobilfunknetze eingehen, sehen diese Netze heute so aus: Man hat ein Kernnetz, ein Transportnetz und ein Zugangsnetz, das Radionetz. Die Mobilfunkunternehmen müssen sich mit anderen Mobilfunkunternehmen im Land, aber auch international verbinden, d.h. sie haben auch eine Verbindung mit ihren Roaming Partnern (Bild 3). Durch die ganzen Bereiche entwickelt sich immer mehr die Verwendung von IP, von IP-basierten Protokollen und IP-basierten Systemen. Einmal getrieben aus Kostenaspekten aber auch durch die neuen Möglichkeiten, die die IP-Technologie bietet, um sich entsprechend weiterzuentwickeln und neue Dienste anbieten zu können.

In der Vergangenheit hat sich das Thema IP sehr stark in dem Kernnetz und in dem Transportnetzbereich ausgebreitet und auch in den Zusatzdiensten, die angeboten werden. Mit der Einführung von LTE oder 4G und dem Rollout dieser Technologien hält das Thema IP auch Einzug in die Radioschnittstelle, also in den Zugangsbereich der Netze. Smartphones und Tablets, die das mobile Broadband nutzen, werden dadurch schneller und leistungsfähiger.

Mit der Einführung der offenen Kommunikation über IP muss der Mobilfunkanbieter seine Netze schützen und muss sicherstellen, dass die Infrastruktur von Ende bis Ende entsprechend abgesichert wird, so dass er in der Lage ist, seinen Kunden einen entsprechend sicheren aber auch verfügbaren Service zu bieten. Er muss sich auf der einen Seite schützen gegen seine Roaming Partner, und verhindern dass deren ankommende Daten keinen Schaden in seinem Netz anrichten. Es gibt durchaus einige Länder, die extrem starken Verkehr auf die Netze schieben und die auch oft Ursprung von Attacken sind.

Auf der anderen Seite muss der Mobilfunkanbieter natürlich auch sicherstellen, dass er in der Kommunikation mit anderen Ländern, aber auch mit anderen Mobilfunkunternehmen und Festnetzunternehmen in Deutschland, nicht blockiert wird, weil sich die anderen Marktteilnehmer entsprechend schützen. Deswegen muss er sicherstellen, dass er nicht geblacklisted wird und sich darum kümmern, dass möglichst wenig Spam von seinem Netz in andere Netze fließt und dort die Netze schädigt oder belastet.

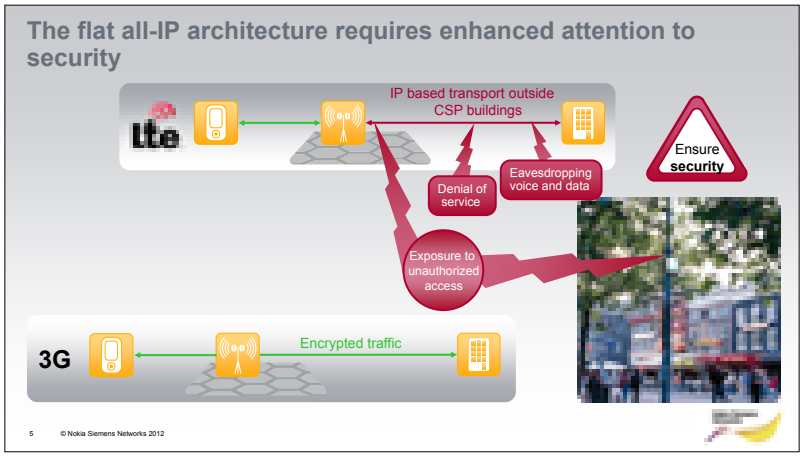


Bild 4

Im Weiteren werde ich vor allem ein bisschen mehr auf die neuen Entwicklungen im Radiobereich und im Smartphone Bereich eingehen, weil dort die stärksten Entwicklungen stattfinden, während der Core Bereich sich bereits über die letzten Jahre entwickelt hat. Wenn man auf den Radiobereich, also den Zugangsbereich schaut, d.h. wenn Sie Ihr Handy nehmen und dieses Handy verbindet sich mit einer Basisstation, dann muss die Basisstation die Kommunikation mit dem Kernnetz herstellen.

In der Vergangenheit, in der 2G und 3G Welt, wurde das typischerweise über proprietäre Verbindungen gemacht. Die Basisstationen haben sich normalerweise in physikalisch geschützten Bereichen befunden, entweder in geschütztem Gelände oder auf einem Antennenmast oder Dach, in der Regel schwer zugänglich.

Wenn wir jetzt über die neuen Technologien nachdenken, über 4G LTE, Long Term Evolution, dann befinden sich diese Basisstationen nicht immer – wie Sie hier auf Bild 4 sehen - an physikalisch wirklich geschützten Stellen. Das ist die eine Thematik. Die andere Thematik ist, dass diese Basisstationen heute auch über IP angebunden werden und dass damit die typischen Gefahren, die wir aus der IT oder IP Welt kennen, jetzt auch auf diesen Verbindungen Anwendung finden. Ich habe Ihnen vorhin ein bisschen das Wachstum des Mobilfunks oder des mobilen Broadbands und damit des Smartphones gezeigt und dass damit auch ein wirtschaftlich deutlich erhöhtes Interesse besteht, diese Verbindungen anzugreifen. Deswegen müssen sich die Mobilfunkunternehmen entsprechend schützen, was sie auch machen. Auf der einen Seite müssen sie den Verkehr, den Datenaustausch zwischen den Basisstationen und ihren Kernnetzen entsprechend schützen und verschlüsseln. Auf der anderen Seite müssen sie auch sicherstellen, dass diese neueren Basisstationen, die, wie gesagt, leichter zugänglich sind, ganz klar identifiziert werden können und auch sichergestellt werden kann, dass nicht jemand diese Basisstationen verändert oder austauscht und damit Zugriff auf die Daten bekommt, die darüber kommuniziert werden oder auch entsprechende Schadprogramme hier in die Netze einspeisen kann.

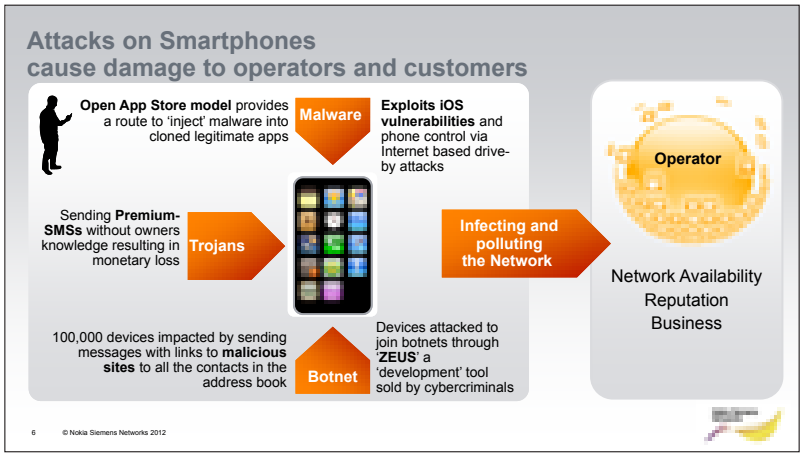


Bild 5

Die zweite Entwicklung, auf die ich eingehen möchte, ist das Thema Smartphone (Bild 5). Es steht an der Stelle synonym für smarte Endgeräte wie z.B. Tablets. Diese Geräte verbinden sich sehr oft über die Mobilfunknetze. Wir sehen, wie gesagt, eine Steigerung der Schadprogramme, die auf diese Geräte abzielen. Wenn Sie heute überlegen, dass 84 % der Nutzer dieser Geräte entweder private oder berufliche vertrauliche Daten auf den Geräten haben, dann ist es von extremem Interesse, an diese Daten heranzukommen. In Frankreich beispielsweise gehen täglich 500 dieser Geräte verloren oder werden gestohlen, in England sind es 1000 pro Tag. Sind diese Daten ungeschützt, dann sind sie für den Dieb oder Finder verfügbar und können missbraucht werden. Eine andere Gefahr geht davon aus, dass sehr viele Nutzer einfach Daten oder Programme aus dem Internet herunterladen, diese auf ihren Geräten installieren und nicht immer ist sichergestellt, dass diese Applikationen entsprechend sicher sind oder aber Viren, Trojaner oder andere Programme beinhalten, die dann in der Konsequenz z.B. Premium SMS verschicken, was ihre Mobilfunkrechnung entsprechend in die Höhe treibt.

Schadprogramme können auch dazu benutzt werden Botnet Angriffe zu initiieren. Letztes Jahr wurden 40.000 Smartphones für eine Botnet Attacke in Mobilfunknetzen zusammengeschaltet. Das ist durchaus ein steigender Trend. Das Ergebnis ist sowohl ein wirtschaftlicher Schaden als auch ein negativer Einfluss auf die Infrastruktur und die Verfügbarkeit der Netze. Der von Botnet Attacken generierte Verkehr kann zu Netzausfällen führen.

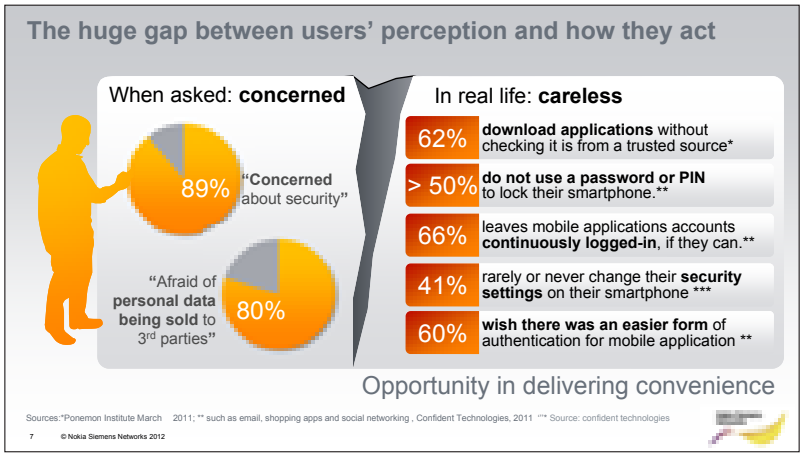


Bild 6

Interessant ist auch, dass es eine sehr starke Differenz gibt zwischen dem, was die Nutzer wollen und wie sie auf der anderen Seite agieren (Bild 6). Wir kennen heute aus der PC- oder IT Welt, das sich typischerweise neun von zehn Nutzern schützen. In der Mobilwelt ist das deutlich niedriger. Dort sind es heute nur ca. 23 %, die sich schützen. Andererseits wollen 89 % sichere Dienste haben. Den Menschen ist es irgendwo bewusst, dass sie Sicherheit wollen, aber sie agieren nicht immer entsprechend.

Dazu möchte ich Ihnen noch einige interessante Daten zeigen. Über 60% laden Applikationen und Software aus ungeschützten oder nicht unbedingt vertrauenswürdigen Quellen herunter, weil die Programme natürlich interessant sind und sie gern damit spielen oder irgendetwas machen möchten. Mehr als 50% schützen heute ihre Daten auf den mobilen Endgeräten nicht über Passwörter oder Pins und die Daten sind im Falle von Diebstahl oder Verlust frei zugänglich. Fast 60% oder zwei Drittel nutzen heute Funktionen, um immer mit den Applikationen verbunden zu bleiben, sprich: um ihre User Login und Passwort auf dem mobilen Endgerät zu speichern, so dass der Zugang zu den Applikationen möglichst einfach ist. Wie Sie sich vorstellen können, sind damit auch die entsprechenden Risiken verbunden. Gerade wegen dieser Differenz zwischen Sicherheitsbedürfnis auf der einen Seite und Nicht-Agieren der Nutzer auf der anderen Seite, ist es aus Unternehmenssicht extrem wichtig, sich um das Thema Sicherheit zu kümmern. Sicherheit ist ein gesamtgesellschaftliches Thema, was Industrie, Staat und Betreiber zusammen vorantreiben müssen, um den entsprechenden Sicherheitslevel zu erreichen, den wir für die einzelnen Unternehmen, aber auch für den Staat benötigen.

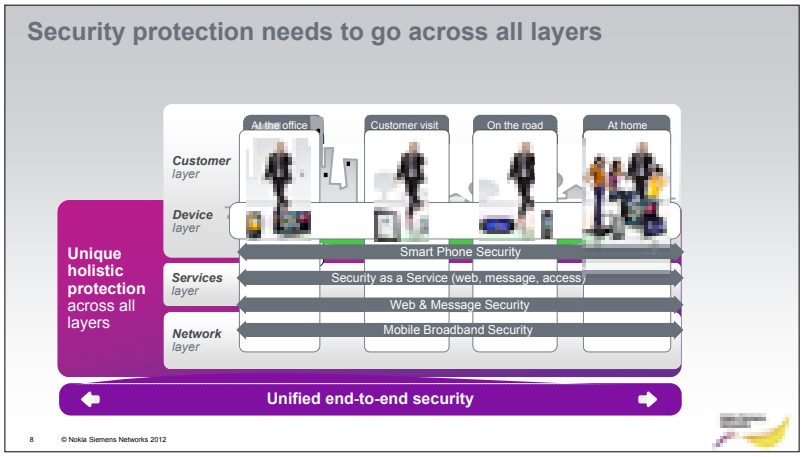


Bild 7

Das bedeutet für die Telekommunikationsnetze heute, dass die Infrastruktur sowohl auf der Netzebene gesichert werden muss gegen Denial of Service und Botnet Angriffe, dass aber auch die entsprechenden Services hier gesichert werden müssen (Bild 7). Z.B. müssen SMS Spam, Email Spam, MMS Spam entsprechend reduziert werden. Es muss auch verhindert werden, dass z.B. illegaler Content durch die Netze fließt und verteilt wird bis hin zu den Smartphones und Tablets.

In dem Zusammenhang denken wir und sehen auch, dass gerade die Telekommunikationsbetreiber eine erhöhte Verantwortung, aber auch Chance haben, Sicherheit wirklich zusammen mit ihren Kunden zu realisieren, weil sich viele dieser Endgeräte mit den Mobilfunknetzen verbinden und entsprechend über diese gesteuert werden.

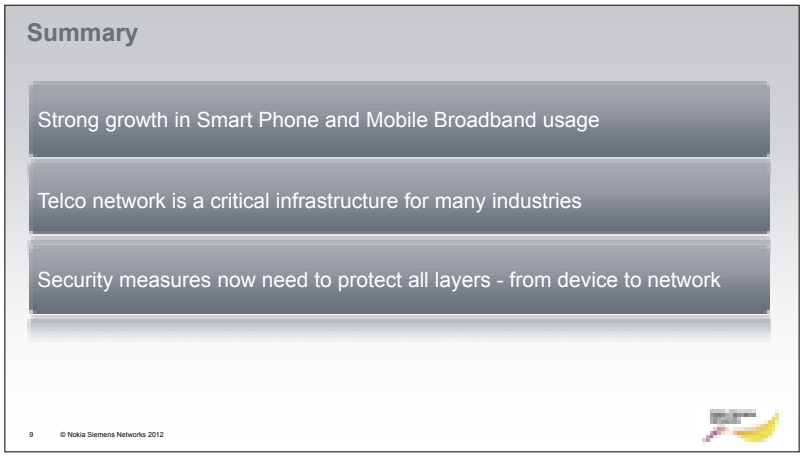


Bild 8

Zusammenfassend zu dem Thema Sicherheit in Telekommunikationsnetzen (Bild 8):
Wir haben ein sehr starkes Wachstum von dem mobilen Breitband und den Smartphones.

Die Telekommunikationsnetze sind definitiv eine kritische Infrastruktur, weil auch viele andere kritische Infrastrukturen sie nutzen, um ihre Prozesse zu steuern, um zu kommunizieren, um ihre Wirtschaftsleistung am Ende zu erbringen. Viele sind heute davon abhängig, und die Anforderungen an die Sicherheit an der Stelle wird immer breiter, weil immer mehr IP Technologie sich durch die ganzen Netze verteilt und diese wirklich End-to-End geschützt werden müssen.

5 Sicherheit im Internet: Sichere Identität, sichere Dienste und Compliance

Claudia Eckert, TU München, Fraunhofer AISEC München

1. Einführung

Informations- und Kommunikationstechnologie (IKT) ist heute in vielen Bereichen des wirtschaftlichen und gesellschaftlichen Lebens von zentraler Bedeutung. Sowohl im beruflichen als auch im privaten Alltag sind wir umgeben von IT-Systemen, die uns mit Informationen versorgen, uns bei Entscheidungen unterstützen, Geschäftsprozesse beschleunigen oder aber auch einfach unseren Komfort fördern (Bild 1).

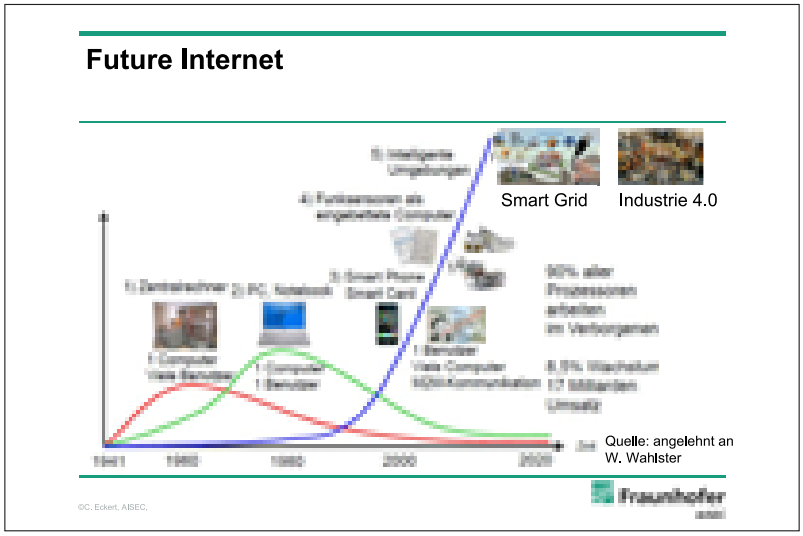


Bild 1: Allgegenwärtige IKT

Ohne intelligente, IKT-gestützte medizinische Geräte, ohne die IKT-unterstützte Fern-Diagnose- und Fern-Therapiemöglichkeiten wäre der heutige hohe Standard in der Gesundheitsversorgung nicht möglich. Unsere hoch-technologisierten Produktions- und Fertigungsanlagen, die Spitzenprodukte z.B. für die Automobilindustrie und den Maschinenbau fertigen, sind ebenfalls ohne komplexe Roboter und IKT-gesteuerte Produktionsanlagen nicht denkbar. Ähnliches gilt für moderne Logistikprozesse, die für eine ressourcenschonende, kosteneffiziente, just-in-time-Produktion unerlässlich sind. Auch im Privatleben nutzen wir zunehmend Informations- und Kommunikationstechnologien, um beispielsweise über das Internet Einkäufe oder Bankgeschäfte elektronisch abzuwickeln, oder um soziale Kontakte über soziale Netzwerke zu pflegen. Durch mobile Endgeräte hat sich der Anteil der Internet-Nutzer in den letzten Jahren gewaltig erhöht. Medien wie Youtube, oder soziale Netze wie Facebook verändern das Kommunikations- und Interaktionsverhalten und den Umgang mit persönlichen Daten. Gleichzeitig findet eine Veränderung in den Unternehmensabläufen statt. Mit dem Stichwort „Bring your own Device“ wird ein Trend bezeichnet, der den Wunsch vieler Mitarbeiter beschreibt, ihre privaten Geräte auch für Unternehmensprozesse zu verwenden.

Die Verschmelzung der physikalischen Welt mit der IT-gestützten, virtuellen wird sich in der Zukunft noch weiter beschleunigen. Das Internet der Dinge (Things) wächst mit dem Internet der Dienste (Services, Cloud Computing) zusammen und wird zum mobilen Internet der nächsten Generation (Bild 2). Es entsteht das Future Internet mit einer Vielzahl von neuen Möglichkeiten, um zentrale gesellschaftliche Herausforderungen, wie die alternde Gesellschaft, die drohende Ressourcenknappheit oder auch die Unterstützung selbstbestimmter Mobilität zu meistern. Insbesondere für eine hoch-technologisierte Wirtschaftsnation wie Deutschland ist IKT eine Schlüsseltechnologie für Innovationen und zur Festigung des Wirtschaftsstandorts.

Große Datenmengen (big data) werden täglich erhoben, analysiert, verarbeitet, gespeichert und ausgetauscht. Durch die systematische Verknüpfung von Daten durch Verfahren der Business Intelligence und Data Analytics-Ansätze entstehen personalisierte Mehrwertdienstleistungen, die eine Vielzahl neuer, interessanter Geschäftsmodelle ermöglichen. Daten und Informationen sind Werte (assets), die es zu schützen gilt.

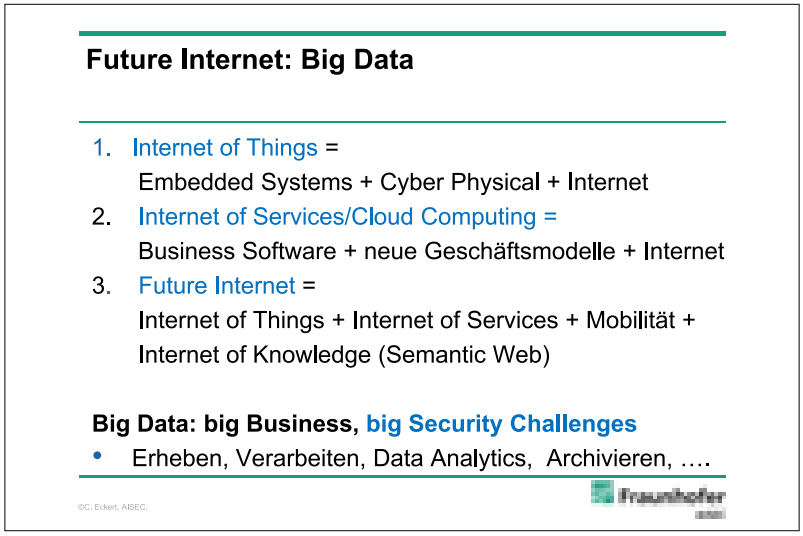


Bild 2: Future Internet: Big Data und big Business

2. IKT benötigt Sicherheit und Vertrauen

Die immense Menge an Daten und Informationen, die täglich erfasst, auf unterschiedlichsten Wegen, insbesondere über das Internet, übertragen und auf diversen Geräten verarbeitet und gespeichert werden, sind die zentralen Einheiten, um die für Unternehmen und die Gesellschaft kritischen Infrastrukturen zu steuern und zu überwachen. Sie steuern das Verhalten von Fahrzeugen ebenso wie auch sicherheitskritische Anlagen, wie Chemieanlagen. Eine gezielte Manipulation dieser Daten könnte verheerende Konsequenzen haben. Daten und Informationen sind ein wertvolles Wirtschaftsgut, wenn es beispielsweise um Finanzdaten, oder Kundendaten geht. Diese sind vor unberechtigten Zugriffen und Manipulationen unbedingt zu schützen. Täglich hinterlassen wir eine Vielzahl von Datenspuren, sei es mehr oder weniger bewusst, durch die Nutzung des mobilen Internets oder eher unbewusst, wie beispielsweise über Aufnahmen durch Videoanlagen, die aus Gründen der öffentlichen

Sicherheit in Geschäften, öffentlichen Anlagen oder Plätzen installiert sind. Aufenthaltsdaten, Bewegungsprofile, Nutzungsprofile oder auch Gewohnheiten werden auf diese Weise erfasst und stellen eine erhebliche Bedrohung für unsere Privatsphäre dar. Die Gewährleistung einer datenschutzbewahrenden Verarbeitung von Daten ist demnach eine zentrale Aufgabe. Dies allein reicht jedoch nicht aus, um die Sicherheitsbedürfnisse im Future Internet, dem Cyber Space, zu befriedigen. Vielmehr werden sehr viel umfassendere Maßnahmen erforderlich sein, um die Korrektheit, Vollständigkeit und rechtzeitige Verfügbarkeit der Daten, sowie die sichere Kommunikation und die Vertrauenswürdigkeit der eingesetzten IT-Komponenten zu gewährleisten. Dies stellt deshalb eine Herausforderung sowohl für die Wissenschaft als auch für die Wirtschaft und unsere gesamte Gesellschaft dar.

3. Herausforderungen

Die überwiegende Zahl der Nutzer bewegt sich heute in der offenen Infrastruktur des Internets so, als gäbe es keine Gefahren und Bedrohungen für schützenswerte Daten und Identitäten. Gleichzeitig nimmt jedoch die kriminelle Energie und die organisierte Cyber-Kriminalität rasant zu. In der Geschäftswelt haben große Unternehmen ihr Bewusstsein für Sicherheit und Datenschutz weitgehend geschärft und begonnen, entsprechende Regeln (Policies, Governance und Compliance-Maßnahmen) zu entwickeln, die regelmäßig auditiert und angepasst werden. Kleine Unternehmen (Mittelstand), Freiberufler und Privatpersonen sind dagegen in der Regel viel unbekümmerter, solange sie nicht direkt merkbar geschädigt werden.

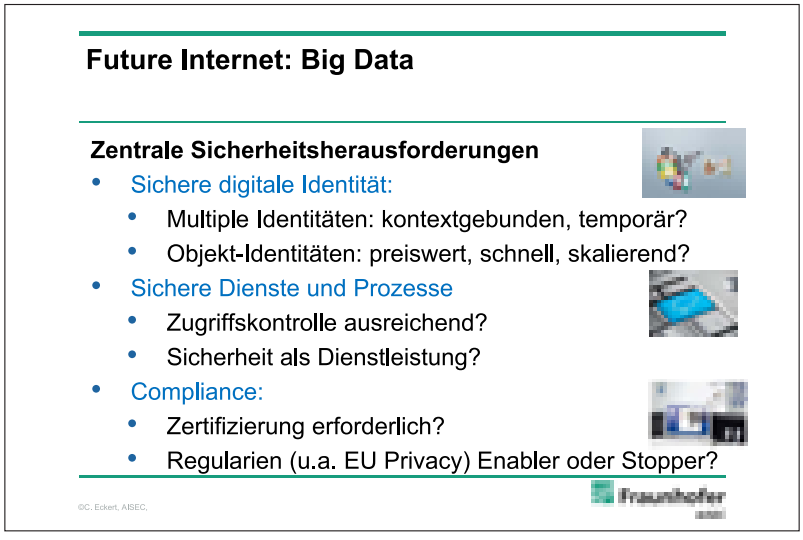


Bild 3: Zentrale Sicherheitsherausforderungen

Zu den zentrale Herausforderungen für die Erhöhung der Sicherheit im Internet zählen deshalb folgende drei Bereiche, denen sich die Münchner Kreis Konferenz hauptsächlich gewidmet hat: (1) die Bereitstellung sicherer Identitäten, (2) die Bereitstellung sicherer Dienste und Internet-basierter Prozesse sowie (3) die Erfüllung von Compliance-Anforderungen (Bild 3). Die drei skizzierten Themenstränge wurden in der Münchner-Kreis Konfe-

renz in Arbeitsgruppen diskutiert mit dem Ziel, Bedrohungen, Lösungsansätze und Handlungsempfehlungen für die Politik, Wirtschaft und auch die Wissenschaft zu identifizieren.

3.1. Sichere Identität

Alle Prozesse, Transaktionen, Zugänge, Rollen und Berechtigungen im Internet erfordern digitale Identitäten (eID). Das Management elektronischer Identitäten gewinnt zunehmend an Bedeutung. Die zunehmende IKT Durchdringung führt zudem zu einem sehr starken Anstieg der Kommunikation zwischen IKT-basierten Komponenten. Automatisierte Updates von Sensoren, beispielsweise in Fahrzeugen, im Zuge von Wartungsarbeiten sind hierfür bekannte Beispiele. Für die direkte Kommunikation zwischen Sensoren und anderen Komponenten, die so genannte Machine-to-Machine (M2M) Kommunikation, werden ebenfalls eindeutige Objektidentitäten benötigt, die einfach zu erzeugen, einfach zu überprüfen und nicht fälschbar sind. Dies ist gerade für die Vielzahl der Objekte im Future Internet eine sehr große Herausforderung.

Meine Eingangsthese für den Workshop 1 ist, dass man multiple Identitäten (Bild 4) benötigt, die kontextgebunden ggf. auch nur mit temporärer Gültigkeit (Wegwerf-Identitäten) so erzeugt werden können, dass sie genügend Vertrauenswürdigkeit für geschäftliche und soziale Transaktionen im Internet bieten.

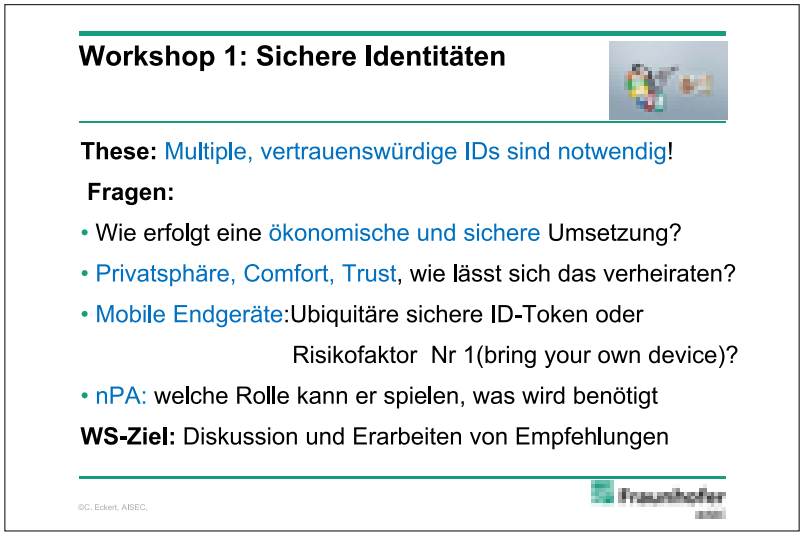


Bild 4: Herausforderung: Sichere Identität

Multiple Identitäten ermöglichen die Verwaltung unterschiedlicher Profile, so dass damit auch unterschiedliche Berechtigungen und auch Pflichten festgelegt werden können. Die Herausforderung und Fragestellung ist demnach, wie man multiple, digitale Identitäten ökonomisch und vertrauenswürdig umsetzen kann, so dass sowohl Privacy-Anforderungen umgesetzt, als auch eine einfache Nutzung (Comfort-Funktion) ermöglicht werden. Mit

mobilen Endgeräten, die bereits heute flächendeckend im Einsatz sind, könnte eine Technologie zur Verfügung stehen, um mobile, ubiquitär nutzbare, persönliche Identitäten zu erzeugen und zu verwalten. Dem stehen jedoch die noch nicht zufriedenstellenden Sicherheitskonzepte heutiger mobiler Endgeräte gegenüber, die den Einsatz dieser Geräte heute eher zu einem Sicherheitsrisiko werden lassen. Die sichere Einbindung mobiler Endgeräte in Unternehmensprozesse (Bring Your own Device) und deren Nutzung als identitäts-Token mit unterschiedlichen Identitäten stellt damit eine große Herausforderung, aber auch ein großes Potential dar. Der Impulsvortrag von Dr. Grassie von Giesecke & Devrient geht auf diese Thematik ein und stellt einen möglichen Lösungsansatz vor.

Mit dem neuen Personalausweis, dem nPA, der bereits seit 2010 flächendeckend in Deutschland ausgerollt wird, steht eine vertrauenswürdige ID-Infrastruktur zur Verfügung, so dass zu untersuchen und zu diskutieren ist, welche Rolle der nPA in erweiterten Nutzungsszenarien spielen kann und welche Rahmenbedingungen hierfür zu schaffen sind. In seinem Impulsvortrag verdeutlicht Herr Reisen vom BMI dazu noch einmal den erreichten Stand bei der Einführung des nPA und die weitere Roadmap zu dessen Nutzung.

3.2 Sichere Dienste und Prozesse im Internet

IKT-basierte Dienste bilden die technologische Basis für die nächste Generation an Dienstleistungsangeboten von und für Unternehmen, die unter dem Stichwort Industrie 4.0 derzeit diskutiert werden. Sichere und vertrauenswürdige Cloud-Infrastrukturen bilden die Grundlage für neue Dienstleistungen (Cloud-Services) und für Geschäftsmodelle im Internet-basierten Dienstleistungssektor. Viele Unternehmen zögern derzeit jedoch, die Vorteile des Cloud Computing zu nutzen. Sicherheitsprobleme im Cloud Computing bestehen vor allem im Kontrollverlust für den Nutzer, im mangelhaften Monitoring – also wo liegen welche Daten, welche Sicherheitsvorkehrungen sind getroffen, wie wirksam sind diese etc. – und in den Eingriffsmöglichkeiten und Datenschutzverletzungen durch ungenügende Isolierungskonzepte. Auch der mobile Zugriff über Smartphones auf die Cloud führt zu Problemen, wenn über ungesicherte mobile Endgeräte Schadfunktionen oder manipulierte Daten in die Cloud eingespeist werden können. Die Frage, wie der Kontrollverlust durch die Weitergabe von sicherheitskritischen Daten in die Cloud durch vertrauensbildende Kontrollmaßnahmen aufgefangen werden kann, oder aber die Frage nach der vertrauenswürdigen Verwaltung digitaler Identitäten und des vertrauenswürdigen Zugriffs auf Daten in offenen Cloud-Umgebungen, die Frage nach dem Schutz der Privatsphäre sind noch weitestgehend ungelöst. Meine Eingangsthese für den Workshop Sichere Dienste und Prozesse lautet deshalb (Bild 5), dass die Gewährleistung von Informationssicherheit im Internet der Dienste und im Cloud-Computing eine Abkehr von der klassischen Zugriffskontrolle hin zu einer Nutzungskontrolle erfordert. Das bedeutet, dass Konzepte und Kontrollmechanismen benötigt werden, so dass Datennutzungen durchgehend überwacht werden, so dass beispielsweise eine Daten-Weitergabe an Dritte unterbunden werden kann, z.B. in sozialen Netzen, wenn entsprechende Regeln, die mit den Daten verknüpft sind, dies verbieten und Kontrollkomponenten dafür sorgen, dass diese Regeln eingehalten werden. Damit dies auch für die Nutzer nachvollziehbar und prüfbar ist, werden technologische Lösungen notwendig, damit Unternehmen die Prozesse auch in der Cloud überwachen und kontrollieren können. Um der fehlenden Transparenz Abhilfe zu schaffen, muss die Sicherheit von Clouds messbar sein. Auch stellt sich die Frage, ob Haftungsregeln, wie sie in anderen Umgebungen bereits seit langem üblich sind, zu fordern sind, um die Sicherheit der Systeme zu erhöhen.

Eine wesentliche Herausforderung besteht darin, Migrationspfade von bestehenden zu neuen Schutzkonzepten zu etablieren, so dass ein solcher dringend erforderlicher Paradigmenwechsel mit ökonomisch vertretbarem Aufwand erfolgen kann. Im Internet der Dienste stellt sich zunehmend die Frage nach vertrauenswürdigen Sicherheits-Diensten, die im Sinne von ‚Security as a Service' als Dienstleistung angeboten werden. Identitäts-Services, oder TrustCenter-Dienstleistungen sind bekannte Beispiele für Sicherheitsdienste. Jedoch könnte man sich auch Dienstleistungen vorstellen, die im Sinne eines Sicherheitschecks, wie ihn der AppStore durchführt, Apps oder Dienste, die über eine Plattform zur Verfügung gestellt werden sollen, auf mögliche Schwachstellen und Verwundbarkeiten überprüfen. Aber auch spezielle, auf Cloud- und SOA-Architekturen zugeschnittene Monitoringdienste sind hier denkbar, die vergleichbar mit den bekannten Intrusion-Detection Systemen eine Cloud-Plattform laufend im operativen Betrieb auf die Einhaltung von Vorgaben überwachen.
Auf die Frage nach einem notwendigen Paradigmenwechsel in der IT-Sicherheit in Unternehmen geht auch der erste Impulsvortrag von Frau Dr. Georg, Detecon Schweiz, ein, während Herr Prof. Schwenk von der Ruhr-Universität Bochum sich in seinem Impulsvortrag auf die Schwachstellen heutiger Browser konzentriert, die als Schnittstelle zur Nutzung von Cloud-Diensten häufig vernachlässigt werden. Einmal mehr ergibt sich die Forderung nach einer ganzheitlichen Sicherheitsbetrachtung, die alle Komponenten eines Eco-Systems umfasst, wie die Web-Schnittstelle oder aber auch mobile Endgeräte.

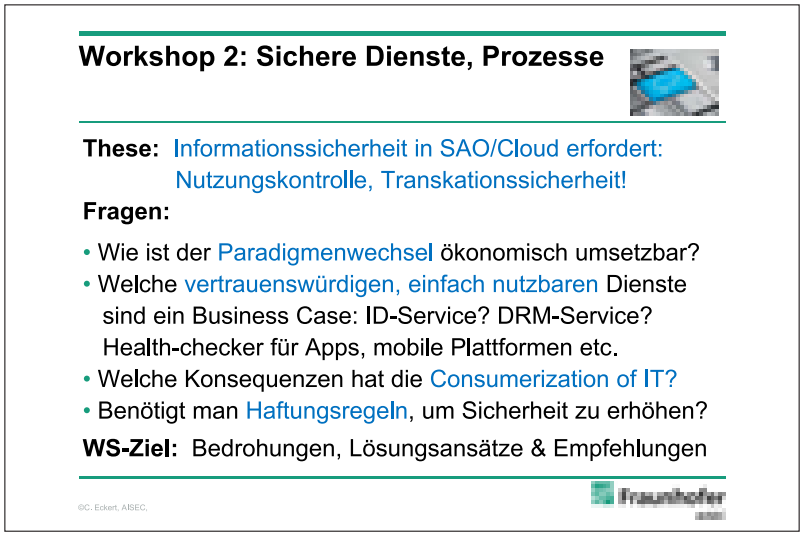


Bild 5: Paradigmenwechsel von Zugriffs- zu Nutzungskontrolle

3.3 Herausforderungen bei der Erfüllung von Compliance-Anforderungen

Die im Zusammenhang mit Datenschutz und IT-Sicherheit bestehenden Compliance-Anforderungen sind vielfältig. Betrachtet man beispielsweise die Kundendaten eines Unternehmens, so stellt sich die Frage nach der zulässigen Erhebung, Verarbeitung und Nutzung. Wie lange darf ein Unternehmen zudem bei ihm gespeicherte Daten vorhalten? Welche Art von Monitoring und Protokollierung, gerade beim Online-Zugriff, ist erlaubt? Hinzu treten

die Themen Outsourcing, Funktionsübertragung und Auftragsdatenverarbeitung. Eine zusätzliche Problematik ergibt sich, wenn Daten über Ländergrenzen hinweg übermittelt und dort gehostet oder verarbeitet werden sollen. Hieran sind je nach Zielland unterschiedliche rechtliche Anforderungen zu stellen. Compliance-Verstöße in diesem Zusammenhang können auf jeder Unternehmensebene empfindliche Folgen nach sich ziehen. Diese reichen von Reputationsrisiken über Schadensersatzforderungen und Bußgelder, bis hin zu Geld- und sogar Freiheitsstrafen.

Kleine Unternehmen sind häufig überfordert, wenn sie selber die erforderlichen technischen und organisatorischen Maßnahmen etablieren müssen, um die Compliance-Vorgaben nachweislich zu erfüllen. Hinzu kommen neue gesetzliche Regelungen, die derzeit u.a. im EU Kontext mit der Privacy Regulierung vorbereitet werden, die eine Meldepflicht beim Auftreten von Sicherheitsvorfällen fordern. Dies setzt voraus, dass man derartige Störfälle überhaupt erkannt hat, was in heutigen IKT-Systemen keinesfalls selbstverständlich ist. Damit bin ich bei der Eingangsthese des dritten Workshops (Bild 6), dass Cloud-Computing sogar eine Security Enhancing-Technologie sein könnte, wenn man den Unternehmen gesicherte und nachweislich regelkonforme Dienste anbieten kann und sie davon entlastet, eine gesicherte und vertrauenswürdige IT-Infrastruktur selber zu betreiben.

Bild 6: Sicheres Cloud-Computing als Security& Compliance Enhancing Technology

Dies erfordert jedoch die Bereitstellung entsprechender technischer Infrastrukturmaßnahmen zur Kontrolle und kontinuierlichen Überwachung der Abläufe. Es stellt sich die Frage, wie solche Maßnahmen aussehen können und ob zertifizierte Komponenten erforderlich sind, um die erforderliche Vertrauenswürdigkeit der IKT-Komponenten zu prüfen und nachzuweisen.

In seinem Impulsvortrag greift Herr Lotz von SAP diese Frage nach technischen Maßnahmen zur Prüfung der Compliance im Business Web auf und stellt mögliche Ansätze vor. Herr Köhler vom EMC/RSA geht in seinem Impulsvortrag umfassend auf Compliance und Risk-Management Fragen ein.

Wir möchten Sie nun alle einladen, die drei Workshops als interaktive Foren zu nutzen, um Ihre Sichten und Handlungsempfehlungen aktiv in die Diskussion einzubringen (Bild 7).

Bild 7

6 Selbstbestimmtes Handeln im Netz - Infrastrukturleistungen des Staates

Andreas Reisen, Bundesministerium des Innern, Berlin

Das Internet und die zunehmende Vernetzung bieten heute ganz neue Möglichkeiten der Kommunikation, der Teilhabe, aber auch innovativer Geschäftsideen. Das ist positiv und chancenreich, hat aber auch seine Schattenseiten. Zum einen sind unsere Identitäten in der Online-Welt zunehmend stärker bedroht und zum anderen wird die Kontrolle der persönlichen Daten gleichzeitig uneinsichtiger und schwieriger. Die objektive Wahrnehmung der gestiegenen Internetkriminalität und die subjektiv empfundene Gefahr durch die Berichterstattung über Trojaner, Phishing, Identitätsdiebstahl etc. hat die Erwartungen von Bürgerinnen und Bürgern an die Organisation von Netz-Sicherheit geprägt. Viele Nutzerinnen und Nutzer haben das Gefühl, zu wenig über die Funktionsweise des Netzes, die bestehenden Bedrohungen, die eigene Gefährdung und die Schutzmöglichkeiten zu wissen.

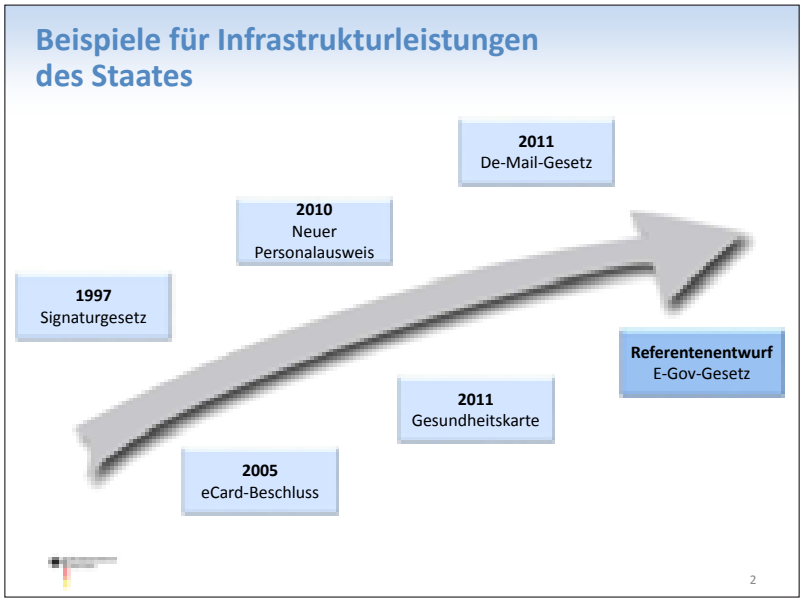


Bild 1

Das Gefühl der abhanden kommenden Selbstbestimmtheit im Netz wird weiter zunehmen, wenn den Bürgerinnen und Bürgern nicht ein vollständiges sowie leicht zugängliches und zu erlernendes „Koordinatensystem“ von Sicherheitsinfrastrukturen zur Verfügung gestellt wird.

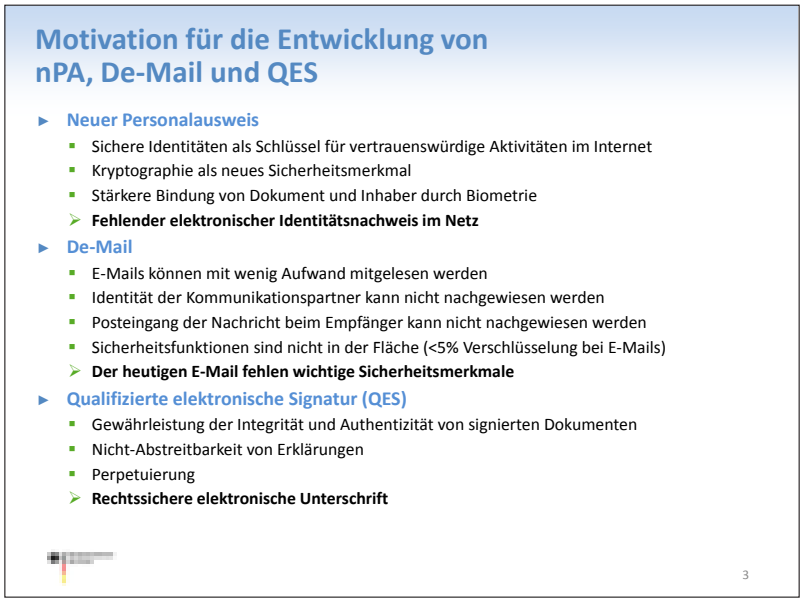


Bild 2

Einige Infrastrukturelemente für ein solches Koordinatensystem bestehen bereits (Bild 1, Bild 2). Beispiele für Infrastrukturleistungen des Staates sind das Signaturgesetz (1997), der eCard-Beschluss (2005), die Einführung des neuen Personalausweises (2010) und die Gesundheitskarte (2011), die Schaffung der rechtlichen Rahmenbedingungen für die sichere und vertrauliche elektronische Kommunikation durch das De-Mail-Gesetz (2011) sowie der Referentenentwurf für ein E-Government-Gesetz zur weiteren Förderung des breiten Einsatzes von sicheren elektronischen Identitäten.

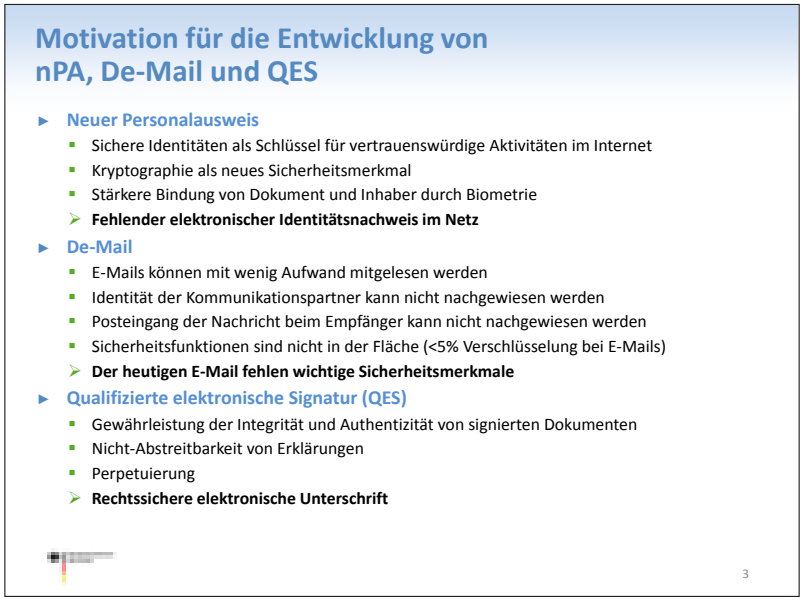


Bild 3

Ein zentraler und wichtiger Baustein auf dem Weg zum selbstbestimmten Handeln im Netz ist der neue Personalausweis (Bild 3). Bislang wurden rund 11,5 Millionen neue Ausweise ausgegeben. Die Einführung wurde fristgerecht erreicht – kein leichtes Unterfangen angesichts von rund 5.400 Behörden und vielen weiteren Akteuren. Die Anfangsschwierigkeiten wurden schnell behoben. Derzeit liegt die Bearbeitungszeit bei ca. sechs Tagen. Gleichzeitig steigt die Zahl innovativer und attraktiver Online-Anwendungen für die Online-Ausweisfunktion. So gibt es bereits 43 Diensteanbieter mit Live-Anwendungen wie z.B. die Eröffnung eines Bankkontos, der Abschluss einer Kfz-Versicherung oder die Beantragung einer Meldebescheinigung. Weitere Anwendungen werden folgen. Die Vergabestelle für Berechtigungszertifikate des Bundesverwaltungsamts hat bislang 116 Berechtigungen für neue Dienste erteilt.

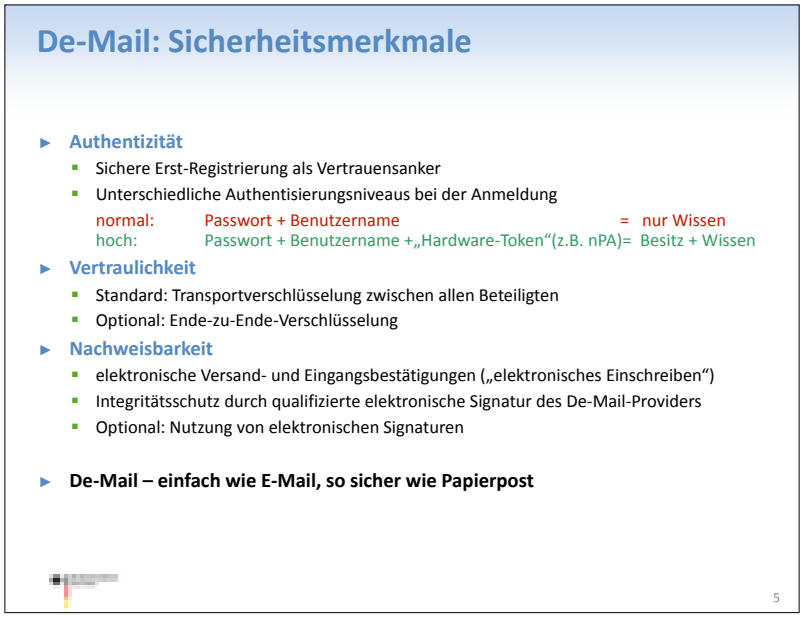


Bild 4

Ein weiterer, wichtiger Baustein für mehr Sicherheit im Netz ist De-Mail (Bild 4). Am 3. Mai 2011 ist das De-Mail-Gesetz in Kraft getreten. Interessierte Anbieter können seitdem beim Bundesamt für Sicherheit in der Informationstechnik die Akkreditierung als De-Mail-Anbieter beantragen. Im Rahmen der Akkreditierung müssen De-Mail-Anbieter nachweisen, dass sie die hohen gesetzlichen Anforderungen an die organisatorische und technische Sicherheit erfüllen. Bis jetzt haben sich die Deutsche Telekom, T-Systems und Mentana Claimsoft als Anbieter akkreditieren lassen. United Internet (1&1, WEB.DE, GMX) hat die Akkreditierung für den Sommer 2012 angekündigt.

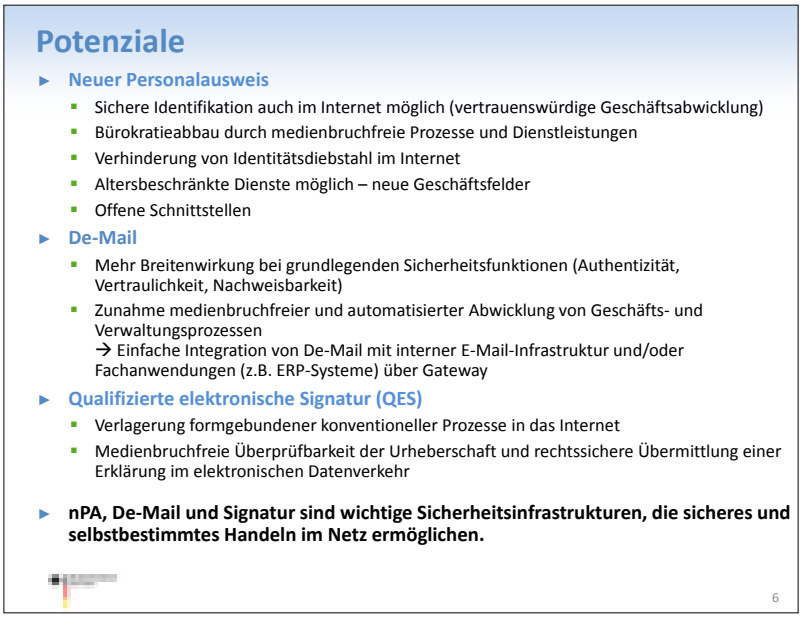


Bild 5

Beide Technologien entwickeln sich weiter, zugleich nimmt ihre Verbreitung deutlich zu. Der Bund unterstützt und fördert diese positiven Entwicklungen. Im Zusammenhang mit dem neuen Personalausweis werden verschiedene Kommunikationsmaßnahmen den Bürgerinnen und Bürgern helfen, die Vorteile des neuen Personalausweises noch besser zu verstehen, und folglich die Steigerung der eID-Einschaltquote bewirken. Bislang haben sich bereits rund vier Millionen Bürgerinnen und Bürger für die Online-Ausweisfunktion entschieden und können somit ihre Daten im Internet sicher und verschlüsselt an die berechtigten Diensteanbieter übermitteln. Gleichzeitig setzt der Bund durch die E-Government-Initiative sowie die Mittelstandsoffensive weitere wichtige Impulse und gibt Hilfestellungen zur Entwicklung neuer Anwendungen im E-Government und im E-Business. Schließlich soll den Bürgerinnen und Bürgern auch der Zugang zu Infrastrukturkomponenten wie den Kartenlesegeräten und der Standardsoftware (z.B. die AusweisApp) durch niedrigere Anschaffungskosten und eine verbesserte Nutzbarkeit erleichtert werden.

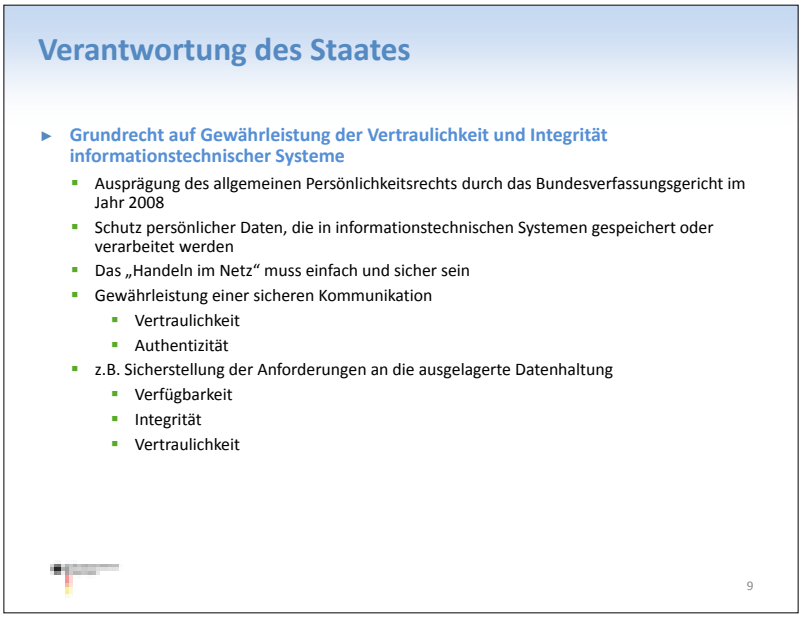


Bild 6

Es gibt einen gesellschaftlichen Konsens darüber, dass alle (Staat, Unternehmen, Bürgerinnen und Bürger) bei der Verbesserung der Sicherheit im Internet zusammenwirken müssen (Bild 6). Der Staat kommt mit den angestoßenen Infrastrukturprojekten seiner Verantwortung nach, den Schutz persönlicher Identitäten zu gewährleisten.

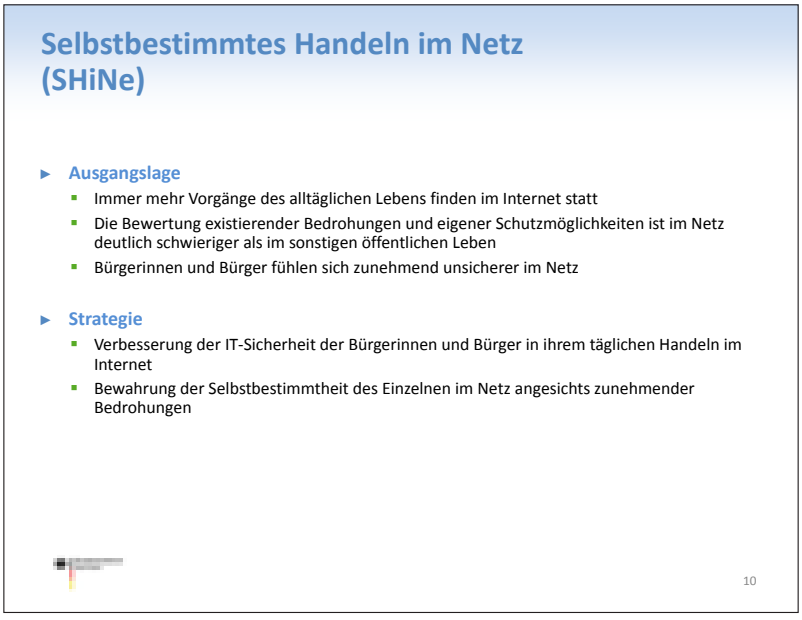


Bild 7

Auch der Anspruch auf den Schutz der Vertraulichkeit und der Integrität persönlicher Daten ist seit dem Urteilspruch des Bundesverfassungsgerichts im Jahr 2009 rechtlich fest verankert und zieht eine Bereitstellung entsprechend geschützter informationstechnischer Systeme bei den Diensteanbietern nach sich. Dieser grundrechtlichen Verankerung liegt auch die staatliche Verantwortung zugrunde, das „Selbstbestimmte Handeln im Netz“ einfacher und durch die Gewährleistung einer vertraulichen und authentischen Kommunikation sicherer zu machen (Bild 7). Es muss langfristig gewährleistet werden, dass Bürgerinnen und Bürger sicher und selbstbestimmt im Internet handeln können.

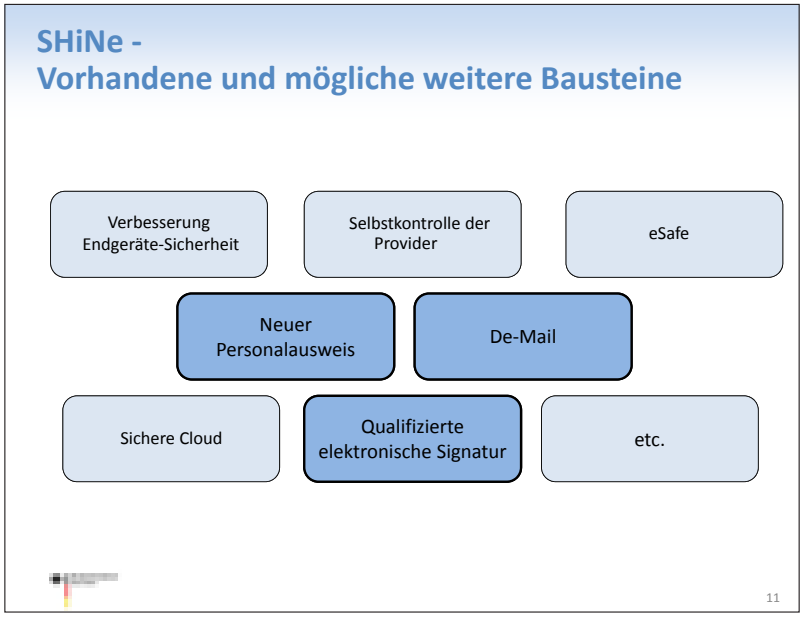


Bild 8

Um das zu erreichen, müssen Technologien in der Fläche – das heißt für jedermann –zur Verfügung stehen, die den Nutzerinnen und Nutzern erlauben, sich sicher, souverän und selbstbestimmt im Netz bewegen zu können (Bild 8). Die hierfür erforderlichen Bausteine müssen vereinheitlicht und verständlich kommuniziert werden. Der Staat muss, wo erforderlich, hierfür den Rechtsrahmen schaffen und weitere Hürden abbauen, damit die erforderlichen Infrastrukturen entstehen und genutzt werden können. Dieses weiter zu entwickelnde Portfolio von Sicherheitstechnologien – oder wie oben genannte „Koordinatensystem“ – soll dazu führen, dass Bürgerinnen und Bürger existierende Bedrohungen im Netz und eigene Schutzmöglichkeiten genauso gut einschätzen können, wie im sonstigen Leben. Das Bundesministerium des Innern erarbeitet hierzu eine Strategie „Selbstbestimmtes Handeln im Netz“, durch die bestehende und noch zu erarbeitende Bausteine zusammengefügt werden sollen. Mögliche weitere Handlungsfelder zur Umsetzung der Strategie sind die Aufklärungsarbeit im Allgemeinen (Gefahren & Schutzmöglichkeiten), der leichtere Zugang und die Verbreitung bestehender Infrastrukturen (neuer Personalausweis, De-Mail, Verschlüsselung, Signatur) sowie die Entwicklung und Optimierung von Technologien (Endgerätesicherheit, Verfügbarkeit & Speicherung in der Cloud).

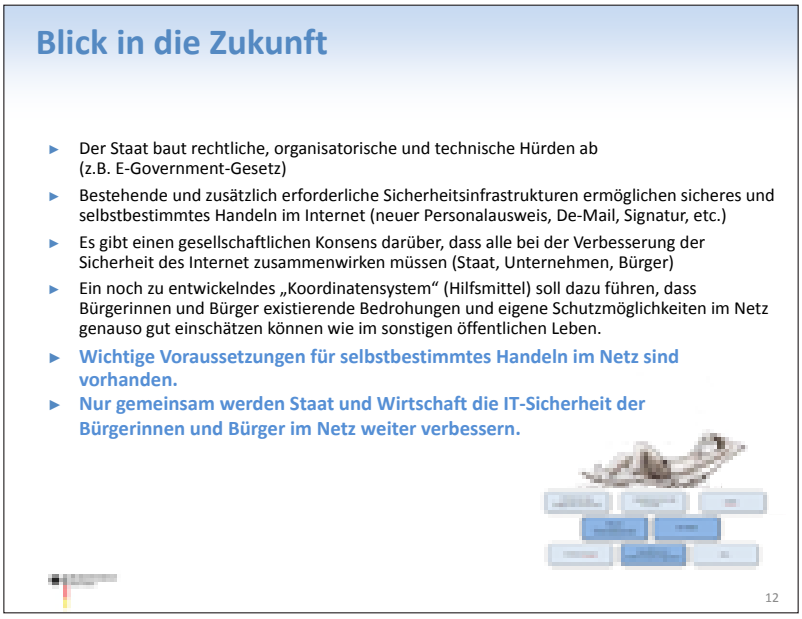


Bild 9

Wichtige Voraussetzungen für mehr Sicherheit und mehr Selbstbestimmung im Netz sind bereits geschaffen worden. In weiteren Kooperationen können nun Staat und Wirtschaft die Sicherheit der Bürgerinnen und Bürger im Netz weiter verbessern (Bild 9). Aber auch die Bürgerinnen und Bürger tragen als Nutzer der neuen Technologien persönliche Verantwortung für mehr Sicherheit und Selbstbestimmtheit. Letztlich muss klar sein: Resultate werden hier vor allem dann zufriedenstellend ausfallen, wenn die Verantwortungsgemeinschaft aus Staat, Anbietern und Nutzern gemeinsam an einem Strang zieht.

7 Globale Herausforderungen an IT-Sicherheit – eine europäische Perspektive

Prof. Dr. Udo Helmbrecht, ENISA, Heraklion

Ich bedanke mich für die Einladung zur heutigen Tagung. Mein Ziel ist es, Ihnen die globalen Herausforderungen der IT-Sicherheit aus europäischer Perspektive darzustellen (Bild 1).

Bild 1

Dabei werde ich Ihnen auch einige der aktuellen ENISA Projekte vorstellen. Lassen Sie mich aber zunächst etwas zu ENISA sagen:

Bild 2 „ENISA“

ENISA ist eine europäische Agentur (Behörde) mit Sitz in Heraklion auf Kreta in Griechenland. ENISA wurde 2004 gegründet (Bild 2). Unsere Hauptaufgaben sind:

- Bewertung von IT-Sicherheitsfragen. Im Sinne eines Think Tanks bearbeiten wir gemeinsam mit Vertretern der Industrie und der Regierungen/Behörden aktuelle IT-Sicherheitsthemen und veröffentlichen diese auf unserer ENISA Web-Seite (www.enisa.europa.eu)

- Unterstützung der Europäischen Kommission und der Mitgliedsstaaten.

- Förderung von Mitgliedsstaats-übergreifenden IT-Sicherheitsthemen/-projekten

- Unterstützung der Mitgliedsstaaten bei der Umsetzung von Europäischen Recht in nationales Recht

Bild 3 „500 million people“

Europa: das sind heute etwa 500 Millionen Einwohnen in 27 Mitgliedsstaaten mit 23 unterschiedlichen Sprachen (Bild 3).

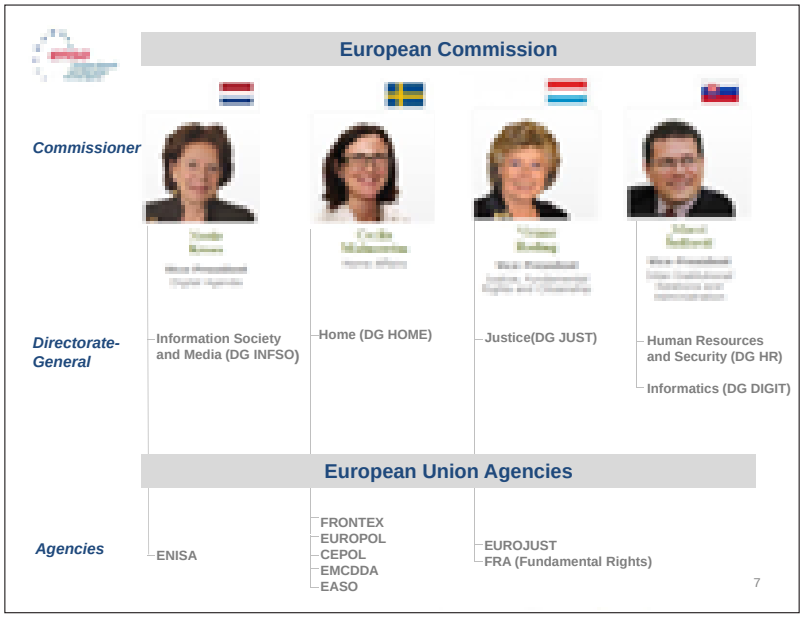


Bild 4 „European Commission“

Präsident der Europäischen Kommission ist José Manuel Barroso. In Fragen der IT und IT-Sicherheit sind 4 Kommissare involviert (Bild 5). Kommissarin und Vizepräsidentin Neelie Kroes verantwortet das Portfolio „Digitale Agenda“. Kommissarin und Vizepräsidentin Viviane Reding ist zuständig für Justiz, Grundrechte und Bürgerschaft, sie hat vor kurzem eine Novellierung der Europäischen Datenschutzrichtlinie vorgeschlagen. Es sei hier auch Kommissar und Vizepräsident Maroš Šefčovič, „Interinstitutionelle Beziehungen und Verwaltung“, erwähnt, weil wir im Gegensatz zu den deutschen Ministerien eine Besonderheit haben: einen Kommissar, der für die horizontalen Dienste, wie Personalwesen, IT, etc. zuständig ist. Kommissarin Cecilia Malmstöm ist für „Inneres“, und damit für die innere Sicherheit Europas verantwortlich. Die Agenturen sind einzelnen Kommissaren zugeordnet. Wir haben hier die ENISA als IT-Sicherheits Agentur im Portfolio von Kommissarin Kroes. FRONTEX (Schutz europäischer Grenzen) und EUROPOL sind bei Kommissarin Malmström angesiedelt. EUROJUST und FRA (Fundamental Rights) bei Kommissarin Reding. Die Kommissare nutzen diese Agenturen auch, um sich politisch beraten zu lassen.

Ich habe im Folgenden Bilder, die ich benutzte, als ich beim Europäischen Parlament, bzw. Rat eingeladen war, um IT und IT-Sicherheit zu erklären. Im Kreis der hier anwesenden Fachleute möchte ich mich auf ein paar Botschaften beschränken.

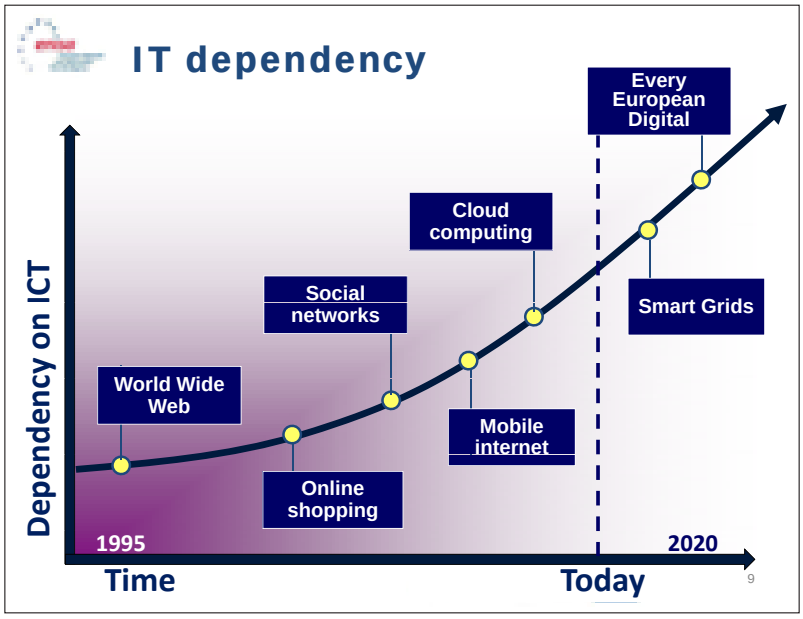


Bild 5 „IT dependency“

Mit dem Internet beschäftigen wir uns ja erst seit 15 Jahren (Bild 5), was kein großer Zeitraum ist, aber trotzdem mit einer dynamische Entwicklung: Social Networks, Cloud Computing über Smart Grids hin zu „Every European Digital“. Letzteres entstammt der Strategie der Europäischen Kommission, die als Ziel hat, bis 2020 überall Breitband und IT-Dienstleistung bis zu jedem Bürger Europas zu bringen. Das ist eine große Herausforderung. Es ist die politische Ambition, die wir haben.

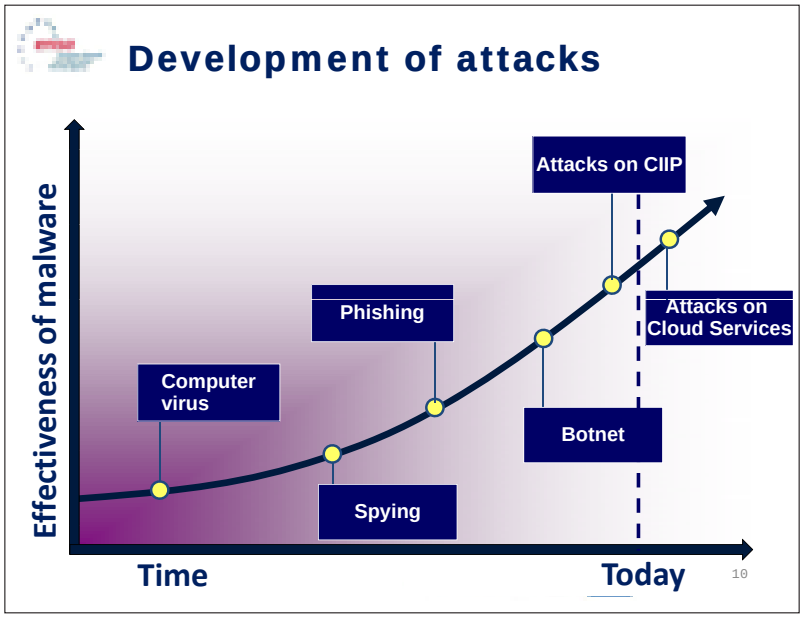


Bild 6 „Development of attacks“

Bild 6 möchte ich nicht missverstanden wissen im Sinne von „Oh Gott, was kommt da auf uns zu“, sondern im Gegenteil: es ist mein Ziel aufzuzeigen, wie wir uns präventiv darauf vorbereiten können und müssen. Das ist auch die Botschaft von ENISA: wir sind eine präventive Behörde. Ein paar Anmerkungen dazu. Hier finden Sie Phishing und Botnetze. Attacken auf kritische Infrastrukturen haben wir mit Stuxnet gesehen. Die Frage ist daher, wie wir uns auf Angriffe auf kritische Infrastrukturen wie intelligente elektrische Netze, sogenannte Smart Grids, vorbereiten. Wenn wir uns Cloud Computing anschauen, ist das auch eine kritische Infrastruktur. Die Frage ist, was tun wir, damit diese auch geschützt sind? Wenn Sie diese beiden Slides näher betrachten, steckt noch mehr dahinter. Unsere Branche ist technologiegeben oder ökonomisch getrieben. Warum investieren wir in bestimmte Technologien? Weil es für das Unternehmen wirtschaftlicher ist oder weil eine Technologie in den Markt getrieben wird? Wenn wir uns mit dem Thema IT-Sicherheit beschäftigen, dann sind das normalerweise Techniker oder technische Behörden. Wir antworten mit technischen Lösungen. Aber manchmal vergessen wir das Menschliche. Beispielsweise ist Phishing heute nichts anderes als früher der Banküberfall.

Heute Morgen bei den Vorträgen ist mir aufgefallen, dass wir präventiv bei vielen Dingen ganz gut aufgestellt sind, weil wir die Risiken erkannt haben, weil wir Maßnahmen ergriffen haben, wenn Firmen Lösungen anbieten, wenn wir an anderer Stelle, wie Herr Schallbruch dargestellt hat, politisch aktiv sind, dann verbessern und mindern wir die Risiken und stellen unsere Unternehmen und Behörden gegen Bedrohungen gut auf. Die große Frage, die für mich dahinter steht, ist, was passiert gesellschaftlich, und ändert sich nicht doch mehr durch die Nutzung der Technik, Stichwort Soziale Netzwerke, in unserem unternehmerischen oder privaten Umfeld, als etwa früher in der Einführung neuer Technologien in der analogen Welt? Wenn Sie ein paar Beispiele nehmen, so haben wir uns früher immer mit Risiken beschäftigt; Autos: Sicherheitsgurte; Flugzeuge: Fluggastkontrollen. Wir haben klassische Viren im biologischen Bereich. Wir bereiten uns darauf präventiv mit Impfungen vor. Aber wir haben einen wesentlichen neuen Punkt, wenn wir uns mit IT beschäftigen: Sobald eine neue

Anwendung auf den Markt kommt, wird diese sofort kriminell missbraucht. Wenn wir technologisch ein neues Auto haben, wissen wir, dass einmal technisch etwas nicht funktionieren kann. Wir habe bei Flugzeugen - zum Glück - heute sehr viel weniger Unfälle. Aber wenn wir uns mit IT beschäftigen, dann war das beim Auto nicht so, dass wenn ein neues Automodell auf den Markt kam, gleich jemand versuchte, kriminell damit Geld zu erwirtschaften, außer wenn er es gestohlen hat. Aber sobald ich eine neue Anwendung habe, ein neues Wirtschaftsmodell, Cloud Computing oder Smart Grids einführe, wissen wir heute, dass sobald dieses Smart Grid da ist, versucht wird, es zu missbrauchen, um es lahmzulegen, jemanden zu erpressen oder sonst etwas. Die Frage ist, was da eigentlich zukünftig mit unserer Infrastruktur passiert, weil wir davon abhängig sind. Ich will Ihnen später noch ein anderes Beispiel geben.

Bild 7 „New virtual world“

Zu Bild 7 will ich kurz erwähnen, dass wir Dienstag in Berlin eine Veranstaltung von BITKOM hatten, auf der ähnliche Themen angesprochen wurden. Wir haben keine nationalen Grenzen, das weiß jeder. Wenn Sie an IT denken, dann ist IT europäisch leider noch keine kritische Infrastruktur. Fragt man sich warum, kann man darauf leider nur antworten: Das ist unsere heutige politische Landschaft. Wir gehen europäisch die „Kritische Infrastrukturen Richtlinie“ wieder an und ich gehe davon aus, dass IT-Infrastrukturen dann enthalten ist. Ich erwähnte schon, dass auch die Datenschutz-Richtlinie überarbeitet wird. Ziel ist, eine einheitliche Umsetzung in allen Mitgliedstaaten zu erreichen.

Wenn Sie diese beiden Punkte nehmen, ist es eine positive Botschaft: Die Themen sind politisch erkannt und es wird etwas getan. Wenn Sie Deutschland anschauen, Herr Schallbruch hat das sehr schön dargestellt, so sind wir der Zeit voraus. Wir haben viel getan in Deutschland: Umsetzungsplan KRITIS. Das BSI ist gefördert worden. Wir haben ein Cyber-Abwehrzentrum. Es gibt Public Private Partnerships. Das heißt, die Politik nimmt das Thema ernst. Und Deutschland ist damit sehr gut aufgestellt.

Europäisch gibt es in den Mitgliedsstaaten ein Nord-Süd-Gefälle. In den mediterranen Ländern unterstützt ENISA noch viel. Aber es ist auf europäischer Ebene politisch erkannt, d.h. wir haben eine Kommissarin, die das Thema aufnimmt. Wir haben Kommissarin Kroes, die bis zum Jahresende eine Internet-Sicherheitsstrategie vorstellen will. Kommissarin Kroes arbeitet dabei eng mit Kommissarin Malström zusammen. Kommissarin Malström hat vor ein paar Tagen veröffentlich, dass ein Cyber Crime Centre bei EUROPOL aufgebaut wird. Und ENISA soll mehr Aufgaben bekommen. Im Entwurf des neuen ENISA-Gesetzes steht, dass ENISA mit EUROPOL zusammenarbeiten soll. Das sind Themen, die man in dem Bereich Strafverfolgung und Prävention andenkt, wie es BSI und BKA seit Jahren kennen. Die Botschaft ist, dass sich politisch viel tut und wir uns damit auch besser aufstellen.

Den dritten Punkt dieser Folie möchte ich wie folgt beschreiben. Wir reden viel über Privatsphäre, soziale Netze. Wir reden viel über personenbezogene Daten oder persönliche Daten. Und dann beklagen wir, wie damit im Internet umgegangen wird. Wir müssen aber registrieren, dass alle neuen Geschäftsmodelle, mit denen wir heute wirklich Gewinn erwirtschaften, auf Profilbildung bestehen, auf dem Zusammenführen von personenbezogenen Lokationsdaten, Kontendaten und anderen personenbezogenen Daten. Ob es zukünftig ein Google, ein Facebook oder ein Amazon ist, ob es Apple- oder Android- Stores sind, es geht darum, wie ich mit dedizierter Werbung mehr Gewinn erwirtschaften kann, was beispielsweise Google ganz offen sagt. Und dedizierte Werbung funktioniert auf mich als Anwender nur, wenn alle wissen, wo ich wann bin und was ich mache, welche Vorlieben ich habe.
Die Frage ist, wie wir diesen Spagat zwischen neuen Geschäftsmodellen auf der einen und berechtigten Interessen unserer Persönlichkeitssphäre auf der anderen Seite zusammen bringen.

Ein Beispiel. Unsere Generation erzählt in Podiumsdiskussionen unseren Kindern, wie sie sich in sozialen Netzen verhalten sollen. Dann komme ich nach Hause und mein Sohn erzählt mir, wie ich mich im Netz verhalten soll. Die Frage ist, was sich da verändert. Wer von Ihnen kennt die App, die WhatsApp heißt? Mein Sohn sagte zu mir, dass ich die haben muss, weil er sie auch hat und wir dann kostenlos SMS austauschen können.

Punkt 1: Das Geschäftsmodell der Telekommunikationsanbieter von SMS wird damit zerstört, so ähnlich wie Skype das Telefongeschäftsmodell zerstört.
Punkt 2: Wenn Sie es installieren, wird Ihr komplettes Adressbuch irgendwohin geladen, und Sie erfahren ganz plötzlich wer noch WhatsApp hat.

Kritisch ist für mich bei solchen Anwendungen, dass wir als Nutzer gar nicht mehr gefragt werden, was mit unseren Daten geschieht. Wenn hier z.B. irgendwelche Fotos gemacht werden, habe ich auch nicht eingewilligt, dass Sie die irgendwo posten. Wenn wir das nicht in den Griff kriegen, müssen wir uns ernsthaft Gedanken machen, wie wir mit Privatsphäre zukünftig umgehen. Ich frage mich mittlerweile, ob unsere Kinder nicht vielleicht doch Recht mit diesem offenen Umgang personenbezogener Daten haben.

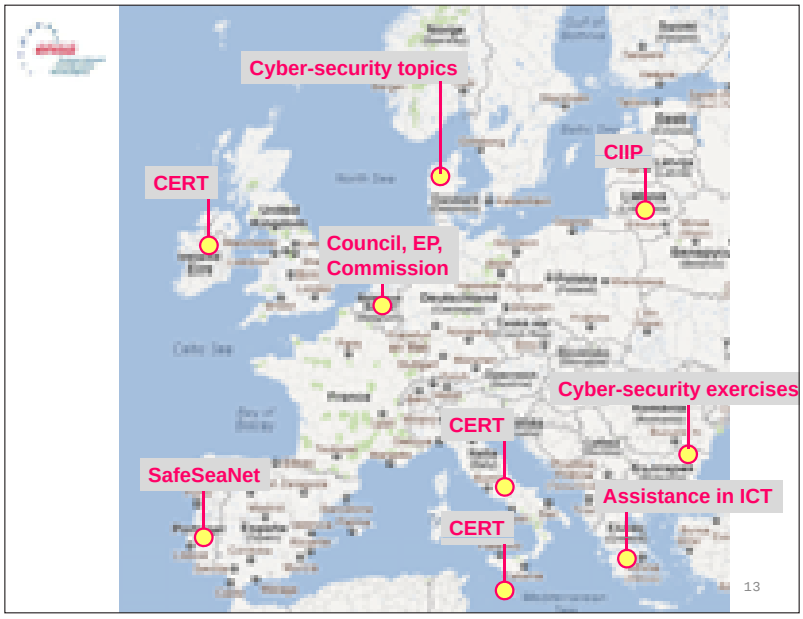


Bild 8: EU-Karte

Was tun wir als ENISA nun für die Mitgliedsstaaten? Grundsätzlich erstellen wir ein jährliches Arbeitsprogramm, das von unserem Verwaltungsrat verabschiedet und dann veröffentlicht wird. Darüber hinaus haben wir in unserem ENISA Gesetz stehen, dass uns Mitgliedstaaten um Hilfe bitten können. Typische Fälle sind, dass Mitgliedsstaaten um Hilfe beim Aufbau eines nationalen CERTs bei eGovernment-Projekten oder auch Unterstützung bei der Formulierung von Gesetzesvorhaben bitten.

Bild 8 zeigt einige Anfragen aus dem letzten halbe Jahr. Hier sind beispielsweise CERT Unterstützungen in Irland, Rumänien, Malta, Italien, d.h. es gehen Mitarbeiter von uns in die Mitgliedstaaten und helfen im Tagesgeschäft oder halten Schulungen ab. Was Sie allerdings politisch als Nord-Süd-Gefälle sehen, wenn Sie in die Tagespresse schauen, erleben wir im Detail bei unserer europäischen Behörde. Das heißt, wir bekommen keine Unterstützungsanfragen aus Frankreich oder Deutschland. Dort gibt es die ANSSI oder das BSI. Auch Schweden oder Finnland sind sehr gut aufgestellt. Wenn Sie aber die neuen Mitgliedsstaaten betrachten, dann versuchen wir diese auf das gleiche Niveau zu bringen. Dort liegt das Risiko, die Schwachstelle Europas. Das heißt, wenn ich Europa angreifen will, dann suche ich Schwachstellen. Unsere Herausforderung ist, wie ich mit diesen Schwachstellen umgehen kann.

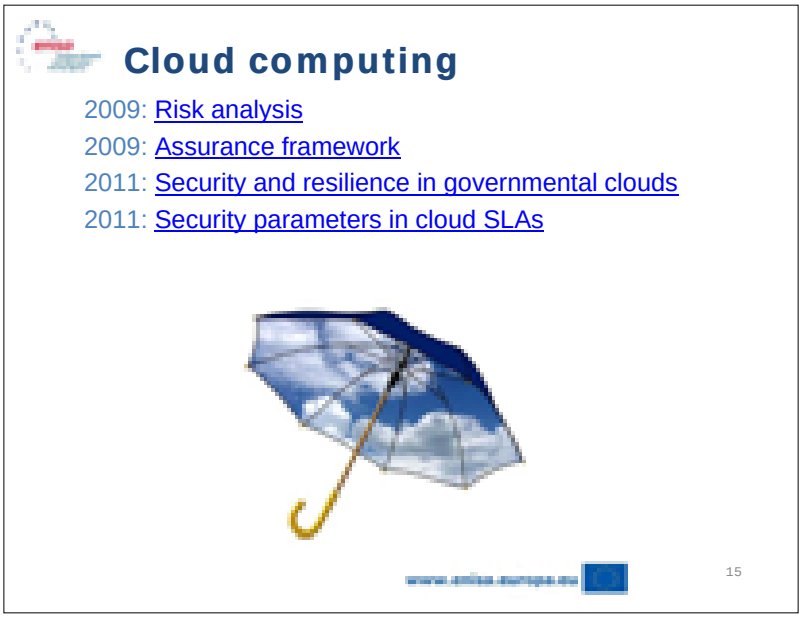


Bild 9: „Cloud Computing“

Ein paar Stichworte für die Diskussion hinterher. Wir haben uns mit Cloud Computing beschäftigt (Bild 9). Wir sind stolz darauf, dass wir das beim Beginn des Hypes erkannt haben. Uns kommt es darauf an, darzustellen, was Vor- und Nachteile sind. Wobei es uns als ENISA wie eingangs geschildert als europäische Binnenmarktagentur darum geht, wo die Chancen sind. Wie kann ich die Chancen sicher machen?

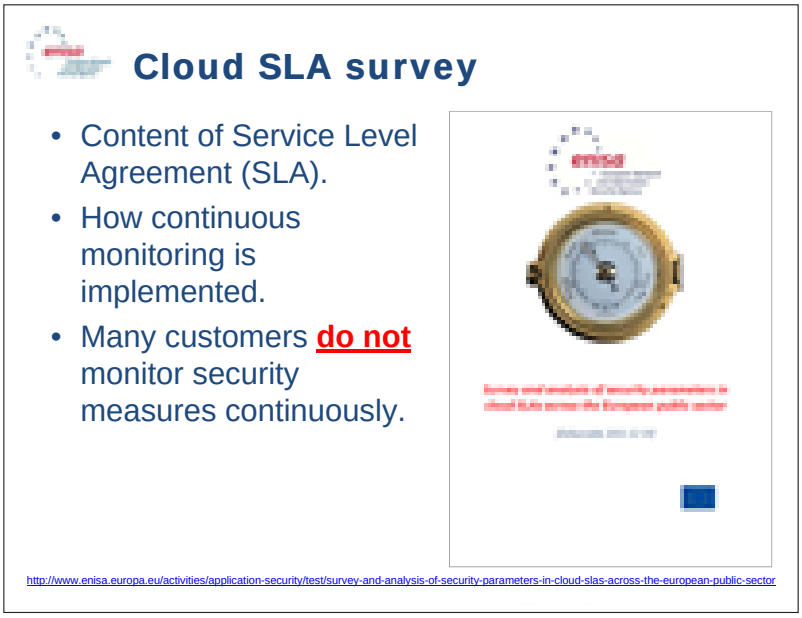


Bild 10: „Cloud SLA survey“

Deswegen auch unser Ansatz über SLAs (Bild 10). Wir haben Empfehlungen veröffentlicht, die auch in der Cloud Assurance Alliance diskutiert werden. Wie gehe ich mit den SLAs um? Woran muss ich denken, wenn ich in die Public oder Private Cloud gehe oder worauf Regierungen achten sollten?

Bild 11: „Findings“

Es gibt viele SLAs, wo Sie z.B. Pönalen für Verfügbarkeit haben (Bild 11). Es gibt aber heute nur ganz wenige SLAs, die Sicherheitsaspekte mit einbeziehen und unser Versuch ist es, das zu verbessern.

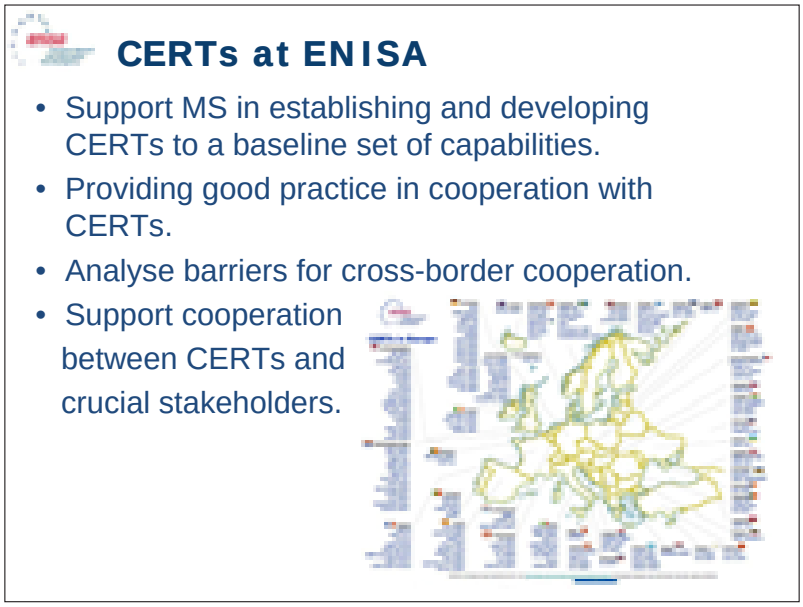


Bild 12: „CERTs at ENISA“

2009 hat die Kommission eine Communication veröffentlicht mit dem Ziel bis 2012 dafür zu sorgen, dass jedes Mitgliedsland ein nationales CERT hat, ein Regierungs-CERT. Wir werden dieses Jahr fertig – Rumänien haben wir letztes Jahr unterstützt, Malta werden wir dieses Jahr schaffen, d.h. dass dann jedes europäische Land ein Regierungs-CERT hat. Die Folie zeigt den Stand Ende 2011. Wir haben ungefähr 150 CERTs, die in einem Verband wie FIRST engagiert sind; neben Regierungs-CERTs hier auch z.B. Bayern-CERT, Telekom-CERT und andere.

Bild 13 „CERT for EU institutions“

Wenn jedes Mitgliedsland ein CERT hat, was ist mit den europäischen Institutionen Kommission, Parlament, Rat, Foreign Action Service, EZB, die Agenturen? Deshalb hat man vor einem Jahr ein CERT für die europäischen Institutionen eingerichtet, das gerade evaluiert wird. Die größte Diskussion in dem Umfeld ist keine technische sondern eine politische. Mitgliedsstaaten haben Angst, dass ein CERT, das in Brüssel gerade seine Arbeit aufgenommen hat, auf einmal ein Super-Europa-CERT wird. Wir versuchen bei allen Gelegenheiten, diese Angst auszuräumen.

Ich möchte Ihnen in dem Zusammenhang folgendes erläutern: Der Lissabon-Vertrag hat unsere europäische Welt verändert. Mit dem Lissabon-Vertrag hat die Kommission ein Initiativrecht. Sie muss nicht mehr in allen Angelegenheiten die Mitgliedsstaaten fragen. Wenn sich heute Präsident Barroso mit Präsident Obama trifft, treffen sich zwei Präsidenten und vereinbaren Themen der Zusammenarbeit. Große und einflussreiche Mitgliedsstaaten wollen aber direkt mit den USA reden, haben ihre bilateralen Beziehungen. Die USA wollen aber nicht über alle Themen mit allen 27 Mitgliedsstaaten reden sondern wollen einen Ansprechpartner. Das beginnt die Kommission zu bieten. Schwierig wird es nun, wenn jemand nach dem Ansprechpartner für das Thema IT-Sicherheit fragt. Da würde ich sagen, natürlich ENISA. Aber das wollen nicht alle Mitgliedsstaaten. Sie sehen, dass Europa ein Prozess ist: wir müssen Prozesse finden, wie wir uns aufstellen und wie wir miteinander arbeiten. Positiv ist, dass das auf der Arbeitsebene sehr gut funktioniert.

Die Botschaft ist: Techniker verstehen sich im Allgemeinen sehr gut. Irgendwann hoffen wir, dass die Politiker das auch untereinander tun.

Bild 14: „Article 13a“

Artikel 13 a ist interessant, weil er zwei Aspekte beinhaltet (Bild 14). Es geht um die Telekommunikationsnovellierung, die 2009/2010 stattgefunden hat. Im Artikel 13a geht es um die Meldung von Sicherheitsvorfällen, Data Breach Notification. Hier war europäisches Recht in nationales Gesetz umzuwandeln. Der eine Aspekt ist, dass ENISA im Telekommunikationsgesetz explizit erwähnt wurde. ENISA wurde eine bestimmte Rolle im Gesetz zugewiesen. Der zweite Aspekt ist, dass wir zusammen mit den Regulierungsbehörden und den Ministerien der Mitgliedsstaaten zusammensaßen und berieten, wie man das europäische in nationales Recht umsetzen kann. Natürlich gab es divergierende Interessen verschiedener Mitgliedsstaaten. Es hat aber letztlich gezeigt, dass man mit den Fachbehörden und Fachministerien zu Lösungen kommen kann.

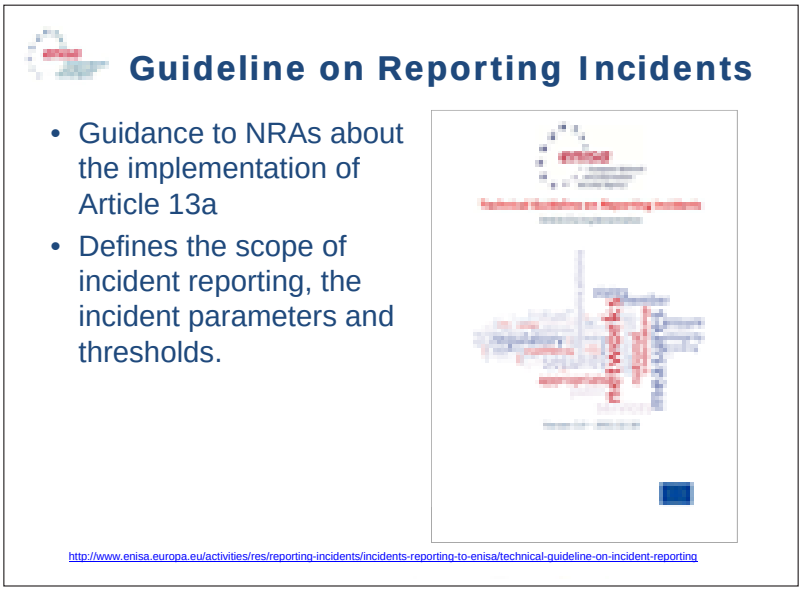


Bild 15: „Guideline on Reporting Incidents“

Heute haben wir sehr gute Vorschläge, wie das umgesetzt funktionieren soll, und wie ein Sicherheitsvorfall vom nationalen Provider über den nationalen Regulierer zu ENISA geht (Bild 15). Aus diesem Projekt sind Empfehlungen mit vielen Standards entstanden und

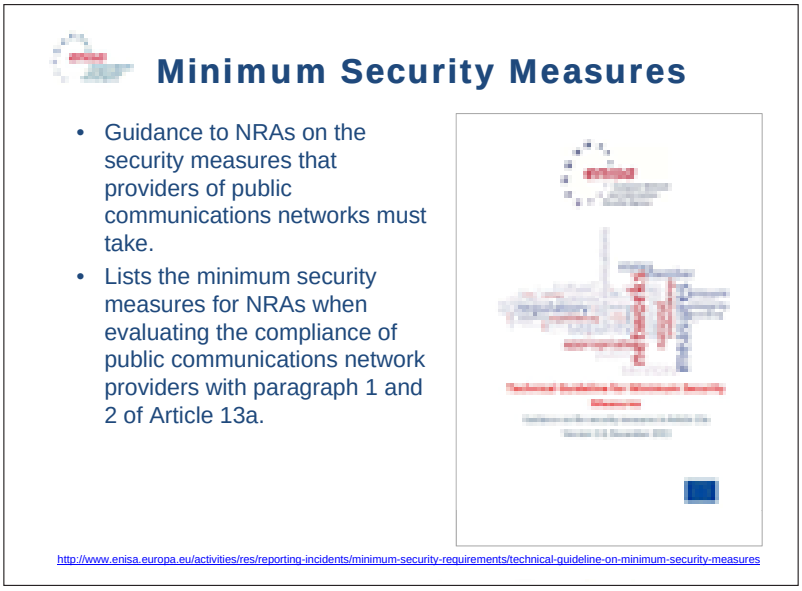


Bild 16: „Minimum Security Measures“

Empfehlungen, wie nationale Regulierer arbeiten sollen, damit es europäisch harmonisiert ist. Als Ergebnis ist die ENSIA Dokumentation über „Minimale Sicherheits Maßnahmen“ entstanden (Bild 16).

Die Botschaft ist, dass Europa an dieser Stelle zusammenarbeitet. Wir stellen uns immer besser auf.

Als Anregung für die folgenden Podiumsdiskussion möchte ich Ihnen mitgeben, dass wir neben allen technischen Lösungen und Geschäftsmodellen, die wir diskutieren, und den Anstrengungen, um das Hase und Igel Spiel zu gewinnen, wir auch den gesellschaftspolitischen Aspekt diskutieren müssen: Was wird sich durch die Piratenpartei politisch ändern? Wie wird die Diskussion um Netzneutralität ausgehen? Wie gehe ich mit geistigem Eigentum, Intellectual Property, um? An welchen Stellen verändert sich die Gesellschaft? Was bedeutet das für uns? Insofern sollten wir diesen gesellschaftspolitischen Aspekt nicht vergessen, wenn wir über neue Technologien und IT-Sicherheit reden.

8 PRÄSENTATION der WORKSHOP-ERGEBNISSE

Moderation: Prof. Dr. Claudia Eckert, TU München, Fraunhofer AISEC
Prof. Dr. Jörg Eberspächer, Technische Universität München

Teilnehmer: Referenten des Tages

Prof. Eberspächer:
Jetzt folgt zuerst die Berichterstattung über die drei parallelen Workshops. Anschließend werden wir ausführlich sowohl über die Ergebnisse der Workshops diskutieren als auch allgemein über die Themen der Konferenz.

Prof. Eckert:
Dann übernehme ich das Kommando sozusagen über die Herren hier. Wir möchten einen kurzen knackigen Report von unseren Rapporteuren aus den Workshops haben. Ich würde gern Workshop 1, 2, 3 aufrufen und Herrn Fromm um eine kurze Zusammenfassung bitten, was die wesentlichen Themen und Erkenntnisse gewesen sind. Was können Sie dem Auditorium mitgeben? Was wurde an offenen Punkten herauskristallisiert, auch an Fragestellungen an die Politik und die Unternehmen?

Bericht zum Workshop „Sichere Identitäten im Internet“

Herr Fromm:
Ich habe die Freude oder vielleicht auch das Problem, dass ich jetzt fast zwei Stunden Diskussion in fünf bis zehn Minuten kurz darstellen darf. Angefangen hat es bei uns im Workshop mit einem interessanten Vortrag von, wie kann es anders sein, Herrn Reisen zum Thema „Infrastrukturleistungen des Staates“, gefolgt von Herrn Dr. Grassie von G&D zu dem Thema „Mobil sicher – sicher mobil“, wo es sehr stark auch um Secure Elements und Trusted Security Modules und Management ging. Also, darum der Versuch einer kurzen und knappen Strukturierung der Diskussion. Es wurde sehr kontrovers über Infrastrukturleistungen des Staates diskutiert, d.h. was muss oder was kann der Staat bereitstellen an Lösungen. Wo kann und sollte der Staat beteiligt sein? Was muss der Staat vielleicht auch für Entwicklungen vorantreiben? Und der Staat steht sicherlich auch in Konkurrenz am Markt, d.h. er muss auch mit Marktlösungen konkurrieren können.

Er sehr wichtiges Thema ist auch das Thema Usability versus Sicherheit. Wir haben auch gerade beim Personalausweis festgestellt, dass es vielleicht nicht nur um Sicherheit gehen kann, sondern auch gerade darum, wie man eigentlich sichere Lösungen nutzt. Das führt, wenn zu viel Komplexität im Produkt steckt, auch teilweise nur zu Nischenprodukten.
Plug and Play wurde hier sicher diskutiert oder auch das Thema Early versus Late Adopters, d.h. wer nutzt schlussendlich Technologien?

Divergent diskutiert wurde auch Technologievielfalt versus Standards, d.h. wie geht man mit neuen Technologien um? Wie bringt man die in die Verbreitung? Oder auch: wie schafft man ein Anwendungsangebot? Wie geht man mit Kosten für Sicherheit um? Wie erklärt man den Bürgerinnen und Bürgern oder den Ämtern, wenn dann auch entsprechende Kosten für Sicherheit entstehen?

Das Thema Datenschutz und Datensicherheit in Bezug auf Identitäten wurde diskutiert, Anonymität, Pseudonymität. Wie stellt man Identität dar? Und auch immer wieder das Thema Vergesslichkeit im Netz. Wie gehen wir mit einmal vorhandenen Daten im Netz um? Hier ein Stichwort: the cloud trust as a service oder auch smart elements und der Standardspruch ‚die Kette ist nur so stark wie das schwächste Glied in der Kette'. Immer wieder darauf hingewiesen worden ist auch, dass Medienkompetenz und Öffentlichkeitsarbeit wichtig sind. Hier sollte man Gefahren dosiert kommunizieren, aber auch gerade die Potentiale, die bestimmte Lösungen bieten können, jetzt sehr stark in Bezug auf den neuen Personalausweis. Aber hier muss man natürlich auch immer sehen, wie man mit den Kosten solcher Kampagnen umgeht.

Darauf hingewiesen wurde auch, dass man natürlich das auch europäisch und international betrachten muss, d.h. wir können nicht nur in Deutschland aktiv sein. Darum möchte ich ganz kurz zu vier Handlungsempfehlungen kommen, die so explizit nicht erarbeitet wurden. Aber ich habe versucht, die aus den Kommentaren der Beteiligten im Workshop zu extrahieren, d.h. es geht um eine Interoperabilität auf allen Ebenen, technisch, semantisch, organisatorisch, politisch. Es geht um einen Dialog zwischen Industrie, Verwaltung und Wissenschaft, vielleicht auch um dokumentierte Schnittstellen, um genau diese Themen voranzubringen. Ziel ist ein selbstbestimmtes Handeln im Netz, dass der Nutzer eine Wahlmöglichkeit hat zwischen anonymem Surfen, aber auch einem identifizierten Surfen. Dass er Themen wie Datenschutz annehmen kann, sich sicher bewegt, aber das trotzdem irgendwo noch nutzbar ist. Dass er aufgeklärt wird in Marketing- und Öffentlichkeitsarbeitskampagnen. Dass man früh mit Medienkompetenzaufbau anfängt und dass eine Aufklärung zu bestimmten Sachthemen vorangetrieben wird. Wichtig ist sicher auch, und das sage ich ganz bescheiden als Fraunhofer, natürlich die Forschung. Hier sind Themen in der Zukunft interessant, wie der digitale Radiergummi. Wie ermöglicht man eigentlich hier die Vergesslichkeit im Netz bestimmter Daten? Themen, wie sichere Clouds etc. Das ist sicher auch eine Bilanz, dass wir uns nicht auf bestimmten Entwicklungen ausruhen können, sondern eigentlich in die Zukunft schauen müssen.

Prof. Eckert:
Herr Fromm, herzlichen Dank. Ich denke, da sind doch sehr viele Aspekte noch einmal zusammengetragen worden. Vielen Dank auch noch mal für die Strukturierung. Ich war selber im Workshop dabei, und es ging durchaus etwas hin und her. Herr Fromm, Sie hatten eine schwierige Aufgabe, diese Diskussion knapp zusammenzufassen, deshalb noch einmal herzlichen Dank für die sehr gute Zusammenstellung und auch herzlichen Dank dem Protokollanten. Sie haben hier die Handlungsempfehlungen mitgegeben, auf die wir sicher später in der Diskussion zurückkommen werden, was wir daraus dann wirklich machen. Ich möchte jetzt Herrn Rannenberg bitten, als Rapporteur von Workshop 2 zu berichten, was hier die wesentlichen Diskussionspunkte waren. Was sind die Handlungsempfehlungen rund um sichere Dienste, sichere Prozesse?

Bericht zum Workshop „Sichere Dienste und Prozesse im Internet"

Prof. Rannenberg:
Wir, das heißt Lutz Neugebauer und ich, hatten „Sichere Dienste und Prozesse im Internet" als Thema in Workshop 2. Dabei hatten wir schon erwartet, dass es eine Vielfalt von Beiträgen geben würde und haben darum von vornherein versucht, das Thema ein bisschen vorzustrukturieren − mit vier Leitfragen, auch in Zusammenarbeit mit unseren Impulsrefe-

renten Dr. Georg und Prof. Schwenk. Die Themen der beiden, nämlich „Sicherheit 3.0: Der Weg von Perimetersicherheit zur Informationssicherheit“ und „Cloud Computing, Webservices und HTML5: Was ist noch sicher?“ sehen Sie auch in den Unterlagen. Wir haben uns gefragt:

1) Welche Richtung nimmt die Informationssicherheit in Unternehmen allgemein?
2) Welche Handlungsbedarfe ergeben sich daraus für Unternehmen?
3) Wie steht es mit der Haftung in den Unternehmen? Hilft dieses Konzept, die Sicherheit besser zu verankern (analog zur Financial Services Industry)?
4) Vor dem Hintergrund der Herausforderungen einer Cybersecurity-Strategie: Welches sind die „Lessons Learned“ aus dem Workshop und welchen Beitrag können die im Workshop genannten Aspekte hierzu leisten?

Wir hatten die Fragen am Anfang noch etwas komplizierter und detaillierter gestellt. Wegen der Zeitknappheit habe ich sie hier verkürzt. Aber trotzdem sollte man erwähnen, dass wir nicht imstande gewesen wären, diese Folien überhaupt hinzubekommen, wenn Volker Reible als Dokumentar nicht einen so herausragenden Job geleistet hätte.

Was sind also die Trends, die Sie vielleicht auch schon einmal gesehen haben und die wir hier herausgefiltert haben aus dem, was als Trendmeldungen von den Workshop Teilnehmern kam? Wir haben diese „national-international“-Debatte, die eben auch gerade angesprochen wurde, ebenso ganz erheblich erlebt, und das Problem tut mehr und mehr weh, erst recht, wenn man Regelungen durchsetzen und ihre Einhaltung managen und anderen als Garantie versprechen will. Auch beim Thema „Awareness“ merkt man das.

Perimeterschutz, wie es ihn klassisch gegeben hat, reicht nicht mehr aus. Der Kampf zwischen Firewallbauern und Firewallverfeinerern einerseits und denen, die sich Anwendungen ausdenken, die durch Firewalls wieder hindurch kommen, haben wir schon immer gesehen. Jörg Schwenk hat ihn an einigen neuartigen und interessanten Beispielen noch einmal vorgeführt. Insofern muss in diesem Bereich irgendwas passieren. Wir kommen gleich noch darauf zurück.

Substitution von Passwörtern – alle Leute sagen, dass man etwas anderes und mehr haben muss. Aber die Frage bzw. Anforderung ist nicht konsequent umgesetzt. Darüber, ob wir das überhaupt noch konsequent umgesetzt haben wollen, gab es auch ein bisschen Debatte. Dann ändern sich Business und private Kommunikation: Die Frage war, wie bedeutend Email als Kommunikationsmedium überhaupt noch ist? Macht es Sinn, über Email-Sicherheit so viel nachzudenken? Muss man sich nicht vielmehr um Dinge kümmern wie Messenger-Dienste oder Social Media, weil da eigentlich das wesentliche Business stattfindet und die wesentlichen Risiken lauern? Man hat gesehen, wie das generationsunterschiedlich eingeschätzt wurde: Einige haben gesagt, dass Email sowieso überholt ist. Dass man sie nicht mehr sichern muss, weil sie absolut unwichtig geworden ist.

Demzufolge hat sich herausgestellt, dass Google und Facebook ganz wesentliche Schwachstellen sind. Single-Sign-on kennen wir eigentlich als Sicherheitsmechanismus. Dass man aber, wenn man sich bei Google mit einem Account eines Social Network (etwa Google-Plis) einloggt, auch bei den anderen Google-Anwendungen gleich mit drin ist, kann durchaus ein ganz erhebliches Problem sein, weil die Grenzen, die man vorher hatte, verschwimmen und damit auch die Daten beliebig hin- und herfliegen, z.B. aus dem Unternehmen heraus. Always online zu sein, ist an der Stelle auch ein ganz erhebliches Risiko, und bei eingebetteten Systemen, etwa Autosteuerungen mittels des CAN-Bus ist diese Entgrenzung auch ein Problem.

So ergibt sich einiges an Handlungsbedarf: Ganz oben steht Awareness. Das erste dabei ist, dass das Top-Management deutlich nicht nur mitbekommen muss, dass Sicherheit eine Herausforderung ist, sondern dass es als Top-Management selber vorbildlich sein muss. Wir hatten da einige „nette“ Geschichten: Die ersten, die Sicherheitsrichtlinien überschreiten, sind die Top-Manager. Die wollen unbedingt mit dem iPhone Email lesen oder in jede Social Network Anwendung rein. Sie wollen alles als allererste haben und treiben die Information Security Officer so an den Rand des Wahnsinns. Gleichzeitig muss man bei Top-Managern möglicherweise am meisten darauf achten, was eigentlich vermarktbar ist und was für sie der Nutzen ist. Es gilt für sie und für ihre Kunden.

Ein Punkt war: Social Media kann sehr wohl Enabler sein für Akzeptanz. Einerseits weil die Leute sich via Social Media austauschen, auch wenn das natürlich ein Risiko sein kann, andererseits auch, weil die Leute in Social Media Fehler machen können und Fehler hoffentlich in irgendwelchen Bereichen machen, wo es noch nicht gleich ganz so weh tut, man daraus aber dann auch irgendetwas lernen und ein bisschen besser machen kann.
Noch etwas zum Thema Email für die Fraktion, die sagt, dass das noch wichtig ist. Der Punkt dazu war, dass das, was es für Email an Sicherheitslösungen gibt, vereinheitlicht werden muss, weil die Leute sonst in der Komplexität ersticken.

Daten – wir werden sie haben – werden sich durch die Perimeter nicht mehr schützen lassen. Also, müssen wir sie irgendwie so mit Sicherheit ausstatten, dass sie sich selber schützen. Ob das Sticky Policies sind oder Rights Management Anwendungen oder was auch immer. Da muss etwas passieren!

Schwachstellen bei Webanwendungen sind die, die am meisten wehtun. Wir brauchen im Prinzip bessere Webprotokolle, die auch standardisiert werden müssen. Es ist relativ klar, dass man eine Cloud an sich – das war die Frage am Morgen, „Cloud als Security Enabler“ -, dass man einen Cloud Server relativ sicher betreiben kann, aber die Schnittstelle zum Cloud Server ist das Riesenproblem. Jörg Schwenk hat es eindrücklich vorgeführt, und auch in der Diskussion kam immer wieder vor, ob man deswegen spezielle Business-Browser braucht, die dann sicherer sind als andere und ob sie um das Chaos besser drum herum navigieren können, ist noch nicht so ganz klar. Dazu gab es verschiedene Meinungen.

Letztendlich das Thema „Bring Your Own Device“. Device Management war für mich der spannendste Punkt, da noch einmal sehr deutlich herausgehoben wurde, dass „Buy Your Own Device“ oder „Bring Your Own Device“ nicht nur heißt, dass ein Gerät in der IT-Umgebung ankommt. Mit dem Gerät kommt ein ganzer Software-Stack an. Es kommen alle möglichen Softwaren an, die die Nutzer selber gekauft, selber entwickelt oder selber aus dem Appstore heruntergeladen haben. Wie man die Apps auch noch unter Kontrolle bringt, selbst wenn man vielleicht verstanden hat, wie man ein iPhone oder Android-Phone in die unternehmensweite IT-Sicherheit einbindet, ist noch einmal eine ganz eigene Aufgabe für sich.

Haftung war ein Thema. Hilft Haftung, Sicherheit besser zu verankern? Hier stand vorher noch „analog zur Financial Service Industry“ in der Frage. Der ganze Workshop hat allerdings nicht ein einziges Mal Bezug auf die „Financial Service Industry“ genommen. Vielleicht liegt es daran, dass wir der nicht so über den Weg getraut haben. Das ist meine These an der Stelle.

Es hat sich herausgestellt, dass man, um Haftung wirklich durchsetzen und umsetzen zu können, ein gemeinsames neues Rechtsverständnis braucht. Ist das für neue Anwendungen in dem Maße gegeben oder kann man auch mit dem gegenwärtigen Rechtsverständnis

zumindest für ein paar klassische Anwendungen etwas erreichen? Auf wen will man eigentlich finanziellen Druck machen mit Haftung? Speziell bei Endnutzern war das so eine Frage. Muss man die da voll einbeziehen? Muss man die davon völlig ausnehmen? Irgendwo dazwischen? Das ist zumindest eine Frage, über die man noch weiter nachdenken muss, denn wie gesagt, bei diesen Themen „Bring your own Device“ and „Bring your own Software“ gibt es natürlich Kollisionen damit, Lizenzbedingungen der Software durchzusetzen. Wer ist denn wirklich schuld, wenn da eine Bedingung verletzt wird?

Was als Punkt blieb, war, dass letztendlich hinreichende Sicherheitsniveaus nötig sein werden, um überhaupt Versicherbarkeit hinzukriegen. Über diesen Hebel wird einiges kommen, was Einfluss nehmen wird auf die Unternehmens-IT und deren Sicherheit.
Was sind die „Lessons Learned“ und die Beiträge, die vielleicht die Cyber Security Strategie verwenden kann, wenn sie es nicht vorher schon wusste? Zentral ist, Nutzer abzuholen, bei dem, was sie tun. Auch ihre unterschiedlichen Bedarfe zu akzeptieren, und auch letztendlich, die Awareness zu schaffen.

Verschlüsselung ist zwar ein Klassiker, aber immer noch besonders wichtig. Bei der Cloud geht es speziell darum, den Zugang zu schützen. Einerseits, wie gesagt, bei Authentifizierung nicht nur Passwörter zu haben und andererseits – wir haben es HTLM5-Chaos genannt – das ganze Chaos mit den verschiedenen Zugangsprotokollen, Webprotokollen usw., zu ordnen bzw. zur Not da doch noch mal einen Neuanlauf zu machen oder etwas besser zu entwickeln, denn, was Jörg Schwenk an Schwachstellen vorgeführt hat, war schon ein erhebliches Problem.

Proaktive Sicherheit war ein Thema: Analysetools und Schwachstellen vor dem Schadfall zu identifizieren führt natürlich dazu, dass alles Mögliche vorweg angeguckt wird, bevor man weiß, ob es überhaupt einen Schaden gibt. Und totale Überwachung hilft auch nicht. Das ist ein Spannungsfeld, aber man muss das Thema auf jeden Fall ansprechen.

Virtualisierung einzelner Anwendungen kann pragmatisch helfen. Das war einer der Ratschläge nach dem Motto, „Was machen Leute, die sich mit sowas auskennen, wenn sie versuchen, ihre eigenen Rechner zu schützen?“. Lieber drei virtuelle Maschinen auf dem Rechner haben als eine, weil, wenn eine dieser virtuellen Maschinen von einer sogenannten Drive-by-Attacke oder Ähnlichem auf’s Kreuz gelegt wird, ist wenigstens nicht gleich der ganze Rechner mit all seinen Anwendungen „verloren“.

Insgesamt wird Sie nicht wundern, dass, wenn hier ein Professor steht, dass dann auf der Folie steht: „Hoher Forschungs- und Entwicklungsbedarf“. Das kam aber nicht nur von mir. Das kam von allen Leuten aus dem Raum.

Prof. Eckert:
Ganz herzlichen Dank. Ich denke, das war eine sehr gute Zusammenfassung dieser Dinge. Ich habe auch Informationen gehabt, dass in dem Workshop viele Aspekte diskutiert wurden. Das jetzt so zusammengetragen zu haben, ist wirklich noch einmal sehr hilfreich. Ich möchte jetzt zum dritten Workshop überleiten und vielleicht auch schon das aufgreifen, was Herr Rannenberg gerade gesagt hat: die Manager sind häufig neuralgische Punkte. Vielleicht könnten die Compliance Anforderungen, dass sie nämlich mit einem Bein im Gefängnis stehen, wenn sie sich nicht vernünftig verhalten, da helfen. Aber ich möchte den Ergebnissen nicht vorgreifen. Könnten Sie, Herr Geschonnek, bitte kurz und knapp berichten?

Herr Geschonneck:
Die Antwort wäre, es bleibt schwierig. Wir haben den Workshop so gestaltet, dass wir zwei technologische Vorträge gehabt haben, einmal von Herrn Lotz von SAP Research. Der andere Vortrag war von Herrn Köhler von RSA Deutschland, ergänzt durch einen Initiativvortrag von Frau Prof. Tinnefeld von der Hochschule in München. Das war erst einmal etwas sehr technologisch gestartet, weil der Titel doch eher non-technologisch ist. Aber es wurde allen Teilnehmern eigentlich klar, dass die Technik, die wir alle so schön entwickeln – und wir haben zwei sehr schöne Anwendungsbeispiele, sowohl von RSA als auch von SAP gesehen -, eigentlich nur so weit funktioniert, solange die Organisation dahinter alles im Griff hat. Die beiden Beispiele waren sehr eindrucksvoll. Herr Köhler hat aus eigenem Erfahren berichtet, was passieren kann oder welche Situation auftreten kann, wenn man selber gehackt wird oder wenn ein Unternehmen geschädigt wird. Herr Lotz hat anhand einer komplexen Krisensituation dargestellt, wie man durch intelligente Datenverarbeitung Mitarbeiter sicher nach Hause bringen kann. Dadurch, dass wir uns mit Compliance beschäftigen, werden viele von Ihnen sofort merken: Mitarbeiterdaten ist ein kritisches Feld. Wie gehen wir damit um? Da ist dann Frau Prof. Tinnefeld eingesprungen und hat uns etwas über das Thema Mitarbeiterdatenschutz erzählt. Wir sind mit einigen Fragen in den Workshop gestartet, nämlich welche Fragen oder welche Vorgaben im Rahmen von IT Compliance zu beachten sind? Damit haben wir eigentlich schon die Frage beantwortet, ob welche zu beachten sind. Natürlich sind Fragen zu beachten.

Die Herausforderung bei der Umsetzung: Wo besteht gesetzgeberischer Handlungsbedarf? Auch das ist eine wesentliche Frage, die wir dort versucht haben zu klären. Was können wir mit der Haftung machen? Auch hier, ähnlich wie in dem Workshop davor, Haftungsrisiken minimieren. Wie kann der finanzielle Rahmen aussehen? Wir haben auch die Anregung von Frau Prof. Eckert mitgenommen: Rettet uns eine Zertifizierung? Wir haben das etwas spitz formuliert und mit in den Workshop genommen. Die wesentlichen Ergebnisse waren: Interessanterweise hatten wir einen Konsensworkshop, wir waren alle gleich kritisch gegenüber Dingen, die noch zu tun sind und haben eigentlich relativ konsensual diskutiert. Wichtige Frage „tone from the top“, wesentlicher Erfolgsfaktor.

Wir haben eine Folie gesehen mit den klassischen Silostil Unternehmen. Existieren Management, Organisation, Technologie und noch ein viertes Silo? Es wurde dargestellt, wie eigentlich diese Bereiche miteinander interagieren in einem Unternehmen und dass Technologie ohne Organisation genau so wenig erfolgreich sein kann wie Organisation ohne Technologie. Das ist eigentlich der wesentliche Punkt, den wir dort identifiziert haben. Es muss alles miteinander harmonieren. Wir können nicht eine technische Lösung einführen, die irgendwo bei einer Bedrohung den Schalter umlegt, etwas protokolliert oder nicht protokolliert oder einen Nutzer aus dem Netzwerk schmeißt oder irgendwelche Gegenmaßnahmen, einen Gegenangriff startet ohne überhaupt zu wissen, ob das das Unternehmensziel ist. Wollen wir das überhaupt? Welches Risiko wollen wir eigentlich eingehen? Es hilft auch nicht, wenn das Management sich bewusst fahrlässig gegen Compliance Regeln verhält, also mit Mitarbeiterdaten fahrlässig umgeht, Überwachungsmaßnahmen startet, die es eigentlich nicht starten sollte, auch gegen Sicherheitsmaßnahmen agiert. Wir haben das iPhone Beispiel gerade aus einem Workshop gehört. Wir konnten es in unserem Workshop an anderen Beispielen sehr stark nachvollziehen.

Silodenken ist sehr wichtig. Die Frage, die dann auch durch die Vertreter aus Forschung und Lehre formuliert wurde: Haben wir eigentlich die richtig ausgebildeten Personen, um zwischen den Silos zu vermitteln? Welcher Skill-Level muss eigentlich ein Manager heute haben, um den Compliance Anforderungen gerecht zu werden oder auch zu formulieren, was er möchte? Welchen Skill-Level muss ein IT-Verantwortlicher haben, um zu verstehen, was das Management möchte. Und wie müssen die Personen, die in dieser Sandwich-Position dazwischen sind, ausgebildet sein? Also, die Compliance Officer, die Informationssicherheitsverantwortlichen, alle die, die Compliance Funktionen wahrnehmen? Das war eine spannende Diskussion und ist auch, glaube ich, mit als Auftrag an die Teilnehmer gegangen.

Zum Thema Datenschutz haben wir uns natürlich auch dem Thema Cloud, Cloud Computing, gewidmet. Es war eine von allen getragene These, dass gerade der Mittelstand und die kleinen mittelständischen Unternehmen sich in die Cloud Computing Technologien retten, weil sie versuchen Kosten zu sparen, dabei aber die komplexen Compliance Herausforderungen, die auf sie zukommen, möglicherweise übersehen oder auch die Risiken, die dann zu Schäden führen können, übersehen. Da ist die Normvielfalt derzeit noch zu uneinheitlich. Als Beispiel wurde das Thema Auftragsdatenverarbeitung aus dem Datenschutz genommen, dass dieses Konstrukt heutzutage nicht mehr sinnvoll sein kann, um die komplexen Daten- und Prozessströme im Rahmen des Cloud Computings zu beherrschen.

Angemahnt auf die Frage „Wo besteht Handlungsbedarf seitens des Gesetzgebers?“ wurde das Thema Sanktionen angesprochen. Frau Prof. Tinnefeld hat vom Entwurf einer Datenschutzverordnung berichtet, die eine Strafe vorsieht von ein bis zwei Prozent des Jahresumsatzes des betroffenen Unternehmens pro Fall oder ersatzweise eine Million Euro. Wenn Sie vergleichen, was Ihnen droht, wenn Sie gegen das Bundesdatenschutzgesetz verstoßen, 350.000 Euro, sind das Dimensionen, die durchaus dazu führen könnten, auch Geschäftsführer, Verantwortliche, dementsprechend auch in Datenschutz- und Datensicherungsmaßnahmen zu investieren, weil einfach ein Verstoß kein Kavaliersdelikt mehr bei diesen Sanktionen sein kann.

Das war abschließend der Konsens. Wir sind zum Schluss relativ gut in Fahrt gekommen, als wir diese ganzen Themen diskutiert haben, aber dann war die Zeit um. Ich möchte noch auf Frau Kollegin Scheben hinweisen, die als Datenschutzexpertin den Workshop mit geleitet hat.

Prof. Eckert:
Vielen Dank, Herr Geschonneck!

9 PODIUMSDISKUSSION

Wie kann die Cybersicherheitsstrategie der Bundesregierung operativ in der Wirtschaft umgesetzt werden?

Moderation: Prof. Dr. Claudia Eckert, TU München, Fraunhofer AISEC
Prof. Dr. Jörg Eberspächer, TU München

Teilnehmer: Referenten des Tages

Prof. Eberspächer:
Dann starten wir die Diskussion und ich darf Sie im Auditorium bitten, Ihre Fragen an das Podium zu richten, ein Statement abzugeben oder auch an die Workshops, an denen Sie nicht teilgenommen haben, eine Botschaft zu richten. Frau Prof. Spiekermann bitte!

Prof. Spiekermann, Wirtschaftsuniversität Wien:
Mir hat sehr gut gefallen: Daten müssen sich selbst schützen. Herr Prof. Rannenberg, können Sie das näher erklären? Was könnte das bedeuten?

Prof. Rannenberg:
Das hatte im Workshop verschiedene Wurzeln. Eine war Rights Management. Aber vielleicht bevor ich die einzelnen Details erkläre, noch einmal der Hintergrund der Debatte: Der ergab sich aus der Perimeterdiskussion heraus. Wir hatten festgestellt, wie es herkömmlich ist: Firewalls schützen einen Perimeter, also eine Umgebung um das Unternehmen herum, und innen drin ist dann alles sicher. Das wird, je mehr Internetanbindungen ein Unternehmen hat, eine immer löchrigere Schutzmaßnahme. Darum ist die Idee gewesen, zu sagen: „Okay, wir haben alle möglichen Daten im Unternehmen und können uns nicht mehr darauf verlassen, dass sie im Unternehmen sicher sind. Sie müssen für ihre eigene Sicherheit sorgen." Das erste Stichwort, das dann kam, hat es vor zehn Jahren schon einmal gegeben und hieß „Rights Management" oder „Digital Rights Management". Das ist oftmals auch eher verstanden oder missverstanden worden auf das Thema hin: „Wie schütze ich Hollywood oder andere Entertainment Inhalte dagegen, dass jemand sie kopiert und damit Geld verdient?" Man kann aber allgemein sagen, dass es darum geht, Daten einzeln zu schützen, so wie sie da sind, und die entsprechenden Rechte so zu setzen, wie man sie braucht, und dann auch sorgfältig darüber nachzudenken, welche Rechte man wie setzt. Das ist aber nicht trivial, sondern bleibt eine Aufgabe, die natürlich mit der Komplexität einer Organisation noch wächst. Und da muss man mehr tun. Das kann man mit Rights Management oder Digital-Rights-Management-Ansätzen unterstützen, indem man sagt: „Wir geben den Leuten mehr Möglichkeiten festzulegen, wer welche Daten wann verwenden darf." Man kann dann einen Ansatz verfolgen wie „Sticky Policies". Das heißt dann, an den Daten klebt jeweils eine Regel, wer sie eigentlich wie verwenden darf. Man kann sich das so vorstellen, dass jedes Datum oder jeder Datensatz seinen eigenen Perimeter bekommt. Das ist ein Perimeter auf der nächst kleineren Ebene, man kann auch „Umschlag" sagen. Das Thema „Trusted Platform Modules" bzw. der Trusted Computing Group ist in dem Zusammenhang auch noch einmal genannt worden. Das ist natürlich auch eine relativ aufwändige Geschichte. Dabei ist die Idee, die Durchsetzung der Schutzmaßnahmen gleich noch im Betriebssystem und der Hardware des jeweiligen Rechners zu verankern. Das sind die Themen, die unter dem Stichwort: „Daten müssen sich selbst schützen", letztendlich gebündelt worden sind. Ich frage einmal bei unseren sehr aktiven Workshop-Teilnehmern, ob ich etwas vergessen habe?

Prof. Eberspächer:
Gibt es noch Kommentare zu dem Vorschlag von hier aus dem Podium?

Prof. Rannenberg:
Das funktioniert auf den ersten Blick schön. Aber es bleibt die Schwierigkeit, die Policies jeweils so festzusetzen. Und es ist natürlich auch nicht trivial durchzusetzen, dass die Umschläge um die Daten auch respektiert werden. Das ist das Problem all dieser Ansätze.

Prof. Eckert:
Es hat ja durchaus einen Grund, dass es sich bis jetzt nicht durchgesetzt hat. Das kommt nicht von ungefähr. So ganz einfach, wie das Herr Rannenberg sehr schön dargestellt hat, ist die Technik einfach nicht. Aber es gibt Ideen. Das war eigentlich die Antwort auf Ihre Frage. Es gibt eine Vielzahl von Ansätzen, die man da verfolgen könnte. Ob das der Weisheit letzter Schluss ist, muss man noch mal sehen.

Prof. Eberspächer:
Herr Dr. Hultzsch bitte!

Dr. Hultzsch:
Ich habe in zwei Berichten, indirekt auch bei Herrn Rannenberg, das Thema Cloud gesehen. Wenn wir zurückschauen, haben wir mit unseren Sicherheitsanstrengungen über das Netz Gewaltiges erreicht. Wenn wir uns vergleichen mit der Vor-Internet- und Kommunikationszeit, wo man mit Unterschrift oder Stempel Sicherheit generierte und de facto ohne Standards arbeitete. Insofern können wir stolz sein, dass es da ist, selbst wenn es an ein paar Stellen Fraud und so etwas gibt. Bei Herrn Fromm und bei der dritten Gruppe ist das Thema Cloud als Vision, als Notwendigkeit in den Vordergrund gestellt worden, am stärksten wohl bei der dritten Gruppe. Die Frage ist jetzt tatsächlich, wie wir diese Sicherheitsaspekte in der Cloud erreichen. In der gegenwärtigen Welt haben wir eine Gruppe und eine Person oder so etwas, die mit irgendeiner anderen Struktur arbeitet, auch wenn das über Netz relativ flexibel hin- und hergeht. Insofern können wir die Identifizierung auf diese Person oder Gruppe konzentrieren. Aber wenn wir in die Cloud gehen, wo wir dann viele Punkte, also Internet of Things usw., miteinander kommunizieren, müssen wir dazu kommen, und ich weiß darauf keine Antwort, dass wir die einzelnen Transaktionen in unserer Cloud mit einer Identität ausstatten, um ein gewisses Maß an Sicherheit, das Äquivalent ist zu den heutigen oder vielleicht zukünftigen Anforderungen, zu erreichen. Also, eine Forderung an uns alle. Ich glaube, dass dies ein Diskussionspunkt sein könnte, über den wir sprechen müssen.

Prof. Eberspächer:
Danke schön. Bitte schön. Direkt dazu?

Herr Köhler:
Die Frage passt ganz gut an Herrn Sieber. Sie hatten heute Morgen einen sehr guten Überblick gegeben, wie der Trend ist, wie wir die regulatorischen Anforderungen ändern müssen. Sie hatten auch den Begriff Deep Packet Inspection erwähnt. Der ist für mich sehr spannend, weil der Angriff auf RSA eigentlich nur bekannt wurde, weil wir einen kompletten Netzwerkstream aufgenommen haben. Das konnte man in den USA wunderbar machen. Das geht hier nicht so einfach. Das heißt, wir können mit solchen Technologien schon Angriffsszenarien erkennen und präventiv werden. Aber das passt natürlich überhaupt nicht mit dem Datenschutz zusammen. Für mich wäre interessant, was für Modelle oder was für gesetzliche Voraussetzungen sehen Sie, um solche Technologien in Zukunft vielleicht einmal anwenden zu können?

Prof. Eberspächer:
Vielen Dank. Herr Sieber, Sie waren direkt gefragt.

Prof. Sieber:
Die Deep Packet Inspection habe ich im Kontext mit den Sperrverfügungen als Frage angesprochen. Sperrverfügungen im Internet greifen in das Telekommunikationsgeheimnis ein, sie sind deswegen und aus verschiedenen anderen Gründen problematisch, und sie funktionieren zumindest derzeit nicht gut. Unter dem Stichwort Deep Packet Inspection stellen sich dabei für mich zwei Fragen. Zum einen: Kann man im Internet mit Deep Packet Inspections in Echtzeit eine Inhaltskontrolle der übermittelten Daten vornehmen, z.B. ob kinderpornografische Bilder mit einem speziellen Hashwert übermittelt werden. Im Anschluss an diese technische Frage stellt sich dann die weitere juristische Frage: Ist es möglich, dass derartige Kontrollen einer Maschine so vorgenommen werden, dass das Fernmeldegeheimnis nicht verletzt wird? Es geht damit um die Frage, ob die technische Entwicklung von Deep Packet Inspection die Prämisse verändert, so dass Inhaltskontrollen im Internet technisch möglich und sinnvoll werden. Ich selbst bin insoweit skeptisch, weil Sperrverfügungen auch weitere Nachteile haben, und weil wir keine Totalkontrolle im Internet wollen. Aber die Frage muss gestellt und geprüft werden. Eine weitere wichtige Frage ist, ob man mit Deep Packet Inspections typische Angriffsszenarien und die Kommunikation in Botnetzen oder ähnlichen Datenverkehr abfangen kann. Auch insoweit geht es darum, ob technische Weiterentwicklungen die bisherigen Szenarien und die rechtlichen Regelungen ändern.

Prof. Eberspächer:
Vielen Dank. Das Thema wird ja auch im Zusammenhang mit Netzneutralität ganz heiß diskutiert und da sieht man auch den Trade Off zwischen der Freiheit, der Konnektivität und dem Schutz der Daten. Ich glaube, da würden sich manche sehr wundern, wenn wir das plötzlich massiv einführen würden. Aber vielleicht gibt es ja Lösungen, wie Sie sie gerade gewünscht haben, die trotzdem noch nicht alles offenlegen, was der Mensch kommuniziert. Nächste Frage, bitte sehr!

Herr Wöhr, Kabel Deutschland:
Mein Name ist Peter Wöhr von Kabel Deutschland, wohlgemerkt nicht Kabel 1 sondern Kabel Deutschland, die mit den Glasfaser- und Kupferkabeln. Ich hätte eine Frage an Herrn Schallbruch. Aus Ihrem sehr informativen Vortrag habe ich entnommen, dass Sie durchaus einige konkrete Schritte planen, um auch die Telekommunikationsanbieter noch ein Stück mehr in die Pflicht zu nehmen, was die Erkennung und Absicherung der Kundenaktivitäten in der Netzinfrastruktur betrifft. Das geht beispielsweise in Richtung Deep Package Inspection, das heißt, neben den diversen Pflichten, die die Netzbetreiber, wie wir als Kabel Deutschland, heute schon haben bzgl. Auskunftsverfahren und Ausleitung und ähnlichem. Ist da eine gewisse Strategie dahinter, sozusagen auch die Netzbetreiber mittel- und langfristig mehr in die Pflicht hinsichtlich auch inhaltlicher Überwachung des Traffics auf den Verkehrswegen zu nehmen? Also, gerade so wie ein Mautstraßenbetreiber die Mautstraße überwachen soll? Oder wie ist die Strategie der Bundesregierung dahinter? Das wäre meine Frage.

Herr Schallbruch:
Ich glaube, die Frage muss man auf drei Ebenen beantworten. Diejenigen, die die Menschen mit dem Internet verbinden, tragen ein Stück weit Verantwortung dafür, wie sicher sich der Einzelne im Internet bewegt, weil sie diejenigen sind, die einem diese Dienstleistung „Internet-Zugang“ verkaufen. Wir haben die Erwartung – und das ist auch das, was wir im Augen-

blick prüfen –, dass eine solche kostenpflichtige Dienstleistung ein Mindestsicherheitsniveau umfassen muss. Das ist bei vielen Providern schon der Fall. Aber das kann durchaus noch ein Stück weiter gehen, wenn es etwa darum geht, dass Provider erkennen, dass aus bestimmten Adressbereichen von Providern heraus Beteiligungen an laufenden Denial of Service Attacks Angriffen erfolgen. Dann sollte der Provider unmittelbar seine Kunden ansprechen und warnen. Wie gesagt, das machen einige Provider bereits, aber nicht alle. Das zweite ist ein Stück weit die Frage, dass die Provider ihren Kunden gegenüber transparente Sicherheitsangebote machen, die die Kunden dann möglicherweise vielleicht auch dazu buchen können. Das ist heute schon häufig der Fall. Da gibt es ein Sicherheitsplus-Paket. Dazu kann dann auf Kundenwunsch auch gehören, dass vielleicht jemand sagt: Ich möchte, dass der Provider schaut, ob meine Kommunikation mit irgendwelchen bekannten Command- und Kontrollservern läuft, um mich in so einer Situation zu warnen. Wenn das auf Wunsch des Kunden und im Rahmen des Vertrags zwischen dem Kunden und dem Provider erfolgt, ist nichts dagegen einzuwenden, denn das ist keine Überwachung der Internetkommunikation. Die dritte Ebene geht ein bisschen in die Richtung, die Herr Prof. Sieber eben schon beantwortet hat. Die Frage, dass die Provider auf irgendeine Art und Weise verpflichtet sind, in die Inhalte der Kommunikation hineinzuschauen, um bestimmte Arten der Kommunikation zu verhindern oder zu überwachen. An dieser Stelle planen wir keine Veränderungen des geltenden Rechts.

Prof. Eckert:
Ich möchte auch ganz gern eine Frage dazwischen schieben. Ich möchte gern noch einmal etwas aufgreifen, was an Handlungsempfehlungen aus dem Workshop gekommen ist. Das würde ich ganz gern zurückspiegeln auf das Plenum. Herr Fromm, Sie haben als eine Handlungsempfehlung gesagt, dass Sie gern die Selbstbestimmung, die Selbstbestimmtheit des Nutzers haben. Der soll die Wahlmöglichkeit haben. Da wäre jetzt für mich eine Frage an Herrn Schneider und auch an Herrn Preuß als Vertreter von Unternehmen, aber auch an die Herren Schallbruch und Helmbrecht, als Regulatoren, Umgebungshersteller. Was kann man denn hier eigentlich technologisch zur Verfügung stellen, dass man auch eine informierte Wahl treffen kann? Und was kann man über regulatorische Maßnahmen machen, damit der Bürger auch wirklich eine für ihn vernünftige Wahl treffen kann? Wenn man das schon fordert, müsste man das gegebenenfalls begleiten.

Herr Schneider:
Was wir heute sehen, ist, dass Telekommunikationsunternehmen zunehmend Sicherheitsdienstleistungen anbieten, sowohl an ihre Privatkunden als auch an Unternehmenskunden. Da ist immer eine Prämisse sehr wichtig, die Herr Schallbruch gerade auch erwähnt hat: Dass im Endeffekt der Benutzer entscheiden kann, was kontrolliert wird, und damit vermieden wird, dass in die Information reingeschaut wird und da Sachen gemacht werden, die nicht erlaubt sind. An der Stelle ist sehr wichtig, dass der Benutzer sagt, was er möchte und er dann entsprechend abgesichert wird. Vielleicht noch einen zweiten Punkt dazu: Für die Telekommunikationsunternehmen sind Sicherheitsdienstleistungen ein Zusatzgeschäft. Das hat natürlich Grenzen, weil es für die Telekommunikationsunternehmen nur so weit Sinn macht wie Kunden bereit sind dafür zu bezahlen. Was wir heute sehen und was vielleicht auch ein Paradoxon ist, ist, dass auf der einen Seite Kunden, also Privatpersonen und Unternehmen, weniger bezahlen möchten für Telekommunikationsleistung. Auf der anderen Seite kostet Security natürlich auch wieder Geld, aber ohne Sicherheitsvorkehrungen steigt das Risiko für wirtschaftliche Schäden bei Unternehmen oder Privatpersonen. Man muss sich in der Zukunft Gedanken machen , wie man erreicht, dass man zwischen Regulierung und Incentivierung an der Stelle sicherstellt, dass auch genügend Geld zur Verfügung steht, das entsprechend investiert werden kann. Wenn man es weltweit vergleicht, und ich bin weltweit

unterwegs, ist Deutschland aus meiner Sicht auf einem sehr guten Weg und auch die deutschen Telekommunikationsunternehmen investieren wirklich einen signifikanten Anteil in die Infrastruktur, um sichere Dienstleistungen anzubieten. Ich kann Ihnen sagen, dass es in anderen Ländern teilweise deutlich schlechter aussieht. Das heißt aber nicht, dass man das nicht kontinuierlich weiter angehen muss.

Prof. Eckert:
Herr Schallbruch, könnte eine Incentivierung auch eine Steuererleichterung sein?

Herr Schallbruch:
Auf die Idee kommt man natürlich immer. Man könnte alles Mögliche durch Steuererleichterung fördern. Man sollte nicht zuerst auf Steuererleichterungen schauen, sondern darauf, dass hier letztlich ein Geschäftsmodell vorliegt. Wenn man sich die Umfragen anschaut, wird dieses Geschäftsmodell „Sicherheit" auch nachgefragt, so dass ich zunächst einmal davon ausgehe, dass Unternehmen ein Interesse daran haben müssen, ihren Kunden ein entsprechendes Angebot zu machen. Ich weiß von den Unternehmen aus den Sicherheitsabteilungen, dass sie in ihre Produktentwicklungsabteilungen auch hinein kommunizieren, was an zusätzlicher Sicherheit im Zweifel erforderlich sein wird, was sie in ihren Honeypots alles feststellen, was sie in ihren Langfrist-Untersuchungen alles beobachten. Da sollte jedes Unternehmen klug genug sein, intelligente Sicherheitsprodukte in ihre Leistung zu integrieren. Da muss nicht der Gesetzgeber kommen und mit Steuererleichterungen winken – der Wettbewerb kann hier vielleicht viel bessere Incentives setzen.

Prof. Eberspächer:
Bevor Herr Dr. Nasko an die Reihe kommt, muss ich Sie doch noch ergänzend fragen, welche Bedeutung es dann für Sie hat, dass, wie ich höre, über 50% der deutschen TK-Infrastruktur aus China kommt?

Herr Schallbruch:
Also, die Zahl kenne ich nicht, dass 50% aus China kommt.

Prof. Eberspächer:
Aber sagen wir mal, ein substantieller Wert.

Herr Schallbruch:
Ich finde es eine unglückliche Entwicklung, dass wir in Europa in manchen Technologiebereichen, die sicherheitstechnisch relevant sind, mittel- und langfristig – bei manchen Themen sogar heute schon – nicht mehr in der Lage sind, selbst zu entwickeln, zu produzieren und vor allen Dingen auch zu beurteilen, was in den Geräten eingebaut ist. Wir wissen gerade im Bereich der Netzwerktechnik, dass es durch nachträgliche Analysen nicht möglich ist herauszufinden, ob das Gerät versteckte Funktionalitäten hat. Das ist eine für uns problematische Entwicklung, weswegen wir in der Cyber-Sicherheitsstrategie einen Punkt haben „vertrauenswürdige Komponenten und Hersteller fördern". Mein früherer Minister hat das immer mit der Überschrift „technologische Souveränität" überschrieben, und ich weiß auch, dass innerhalb der EU - Kommission darüber nachgedacht wird, unsere Forschungs- und Entwicklungsmittel und die regulatorischen Rahmenbedingungen so zu setzen, dass die aus Sicht der Cybersicherheit wichtigen Bereiche in Europa erhalten oder da, wo sie verloren sind, vielleicht wieder aufgebaut werden.

Prof. Eberspächer:
Vielen Dank. Jetzt Herr Dr. Nasko.

Dr. Nasko:
Ich war viele Jahre in der Computerbranche tätig und habe heute wieder gelernt, dass es sehr schwierig, vielleicht sogar unmöglich ist, eine absolute Sicherheit zu gewährleisten, wie in anderen technischen Gebieten übrigens auch. Vor allem im Workshop 2 habe ich miterlebt, wie Herr Prof. Schwenk uns erläutert hat, was alles getan werden müsste, um die Sicherheit im Internet wesentlich zu verbessern. Das war so kompliziert, dass ich zweifle, ob das irgendwann wirklich in die Tat umgesetzt werden kann. Deswegen frage ich mich, ob es eigentlich überhaupt notwendig ist, alle Informationsflüsse diesen hohen Sicherheitsanforderungen zu unterstellen. Wenn man einen Termin mit dem Zahnarzt macht oder derlei Dinge, dann genügt doch der Sicherheitslevel, den es heute gibt, allemal. Wenn aber jetzt, vom Unternehmen aus betrachtet, sagen wir mal ein Preisnachlas für ein Großprojekt, das Siemens in Australien bearbeitet mit dem Stammhaus abgestimmt werden muss, dann ist es in der Tat wichtig, dass die Kommunikation zwischen dem Stammhaus und der Tochtergesellschaft in Australien so sicher ist, dass diese Information nicht in falsche Hände geraten kann. Also, meine Frage lautet: Kann man nicht darüber nachdenken, dass man verschiedene Sicherheitslevel einführt und nur wirklich relevante Daten den hohen Sicherheitsanforderungen unterwirft.

Prof. Eberspächer:
Ja, zuerst Herr Schwenk. Sie sind angesprochen.

Prof. Schwenk:
Ich möchte hier ein positives Beispiel geben, das ich immer wieder gern zitiere, nämlich die deutschen Banken, die es ja geschafft haben, genau zwischen sicherheitskritischen und unkritischen Daten zu differenzieren. Sie haben einen sicheren Kanal für die wirklich relevanten Informationen hergestellt, die Transaktionsdaten, die entweder per smsTAN- oder per ChipTAN-Verfahren gesichert werden. Der ganze Rest bleibt ungesichert. Das ist schon ein schöner Ansatz, den man mal weiterdenken müsste, dass man nämlich genau die Daten schützt, die für das eigene Wirtschaften essentiell sind und gar nicht versucht, die Welt zu retten im großen und ganzen, sondern nur das eigene Geschäftsmodell. Hier hat man wahrscheinlich auch bessere Chancen, als wenn man versucht, das ganze Internet sicher zu machen.

Prof. Eberspächer:
Wobei jeder aus seinem eigenen Umfeld weiß, wie unterschiedlich dasselbe Datum gewertet wird von einem Moment auf den anderen! Herr Kohlhammer mit der nächsten Frage!

Dr. Kohlhammer:
Ich habe die Frage im Workshop 2 schon einmal gestellt, möchte sie aber jetzt noch einmal stellen, weil Sie, Herr Schallbruch, nicht im Workshop 2 waren. Wenn ich höre, wie aufwendig letzten Endes Sicherheit ist, die wir zu betreiben haben, stellt sich mir die Frage, warum man nicht wie bei GSM gehandelt hat, wo sich die Europäer wirklich zusammengetan und für die Entwicklung eines Standards entschieden haben? Warum hat man nicht auch bei der gesicherten Kommunikation so agiert und da will ich gar nicht auf die Auseinandersetzungen in Workshop 2 eingehen, ob jetzt Email noch Zukunft hat oder nicht oder ob es etwas anderes geben wird? Darauf kommt es nämlich gar nicht mehr an. Warum hat man sich nicht wieder zusammengetan und gesagt, dass man gemeinsam eine Lösung macht? Man hätte ganz viel Geld sparen können und vor allem schnelle Lösungen haben können, denn – und da werden Sie mir zustimmen – eine Lösung, wie die Email endet ja nicht an den Grenzen. Für das Internet gibt es keine Grenzen mehr.

Herr Schallbruch:
Im Gegensatz zur Regulierung entstehen Standards ja nicht durch europäische Beschlüsse, dadurch dass Regierungen einen Standard verabreden, sondern typischerweise dadurch, dass Unternehmen, Wissenschaftler, vielleicht auch einzelne Behörden um die beste technische Ausgestaltung ringen. Weil sie De-Mail erwähnt haben: das ist fünf Jahre her. Damals haben wir zu der Frage, wie wir sichere elektronische Kommunikation, die auch Rechtsverbindlichkeit erlangen kann, herstellen können, festgestellt, dass es Standards gibt, auf die wir aufbauen können, Kommunikationsstandards, Sicherheitsstandards, Verschlüsselungsstandards, Zertifikate usw., was man alles verwenden kann. Gleichzeitig gab und gibt es keinen Standard für das gesamte Thema. Daher standen wir vor der Wahl, eine abstrakte europäische Normungsdiskussion zu führen oder ein System zu entwickeln, das wir in die europäische Diskussion hineinbringen können. Wir haben uns für den zweiten Weg entschieden, weil das im Allgemeinen der erfolgversprechendere Weg ist. Und wir haben insofern unser Projekt auch schon seit drei Jahren in ein europäisches Projekt, was von der Kommission gefördert wird, SPOCS, eingebracht, um die Diskussion über sichere elektronische Kommunikation in Europa mit einem deutschen Beispiel zu befördern. Dieses Beispiel, die De-Mail, gibt es jetzt, sie ist mittlerweile rechtlich geregelt und auch praktisch verfügbar. Das wird diese Diskussion befördern und ich prophezeie auch, dass, wenn ein europäischer Standard kommt, wir unser System an der einen oder anderen Stelle ändern müssen, gleichwohl aber unseren Ansatz eingebracht haben. Die Schwierigkeit, die wir bei vielen Sicherheitsthemen im Augenblick haben, ist, dass es nicht so einfach ist wie bei GSM, wo es wenige Player gab, die doch ganz überwiegend irgendwo staatlich beeinflusst waren, die sich zusammensetzen konnten und eine solche Lösung entwickeln. Wenn Sie nur einmal das Cloud-Thema im Vergleich dazu anschauen, würde man nicht mit einer Vorgehensweise wie bei GSM vorgehen. Deshalb wählen die auch dort eine andere Vorgehensweise. Das BSI hat gemeinsam mit dem Gesamtverband der Deutschen Versicherungswirtschaft vereinbart, dass wir anhand der Cloud, die die Versicherungswirtschaft betreibt, in eine Zertifizierung von Cloud Services hineingehen, um an einem konkreten Projekt die Kriterien zu entwickeln, die Schutzprofile zu entwickeln, um dann auch allgemeine Zertifizierungsangebote für Cloud Services zu machen. Das wird dann zwar nicht den ganzen Markt abdecken aber einen Teil des Marktes. Wir wissen auch, dass das dann in die europäische Diskussion gebracht werden muss. Aber wir haben nicht die Möglichkeit abzuwarten, und dann in einem halben Jahr einen europäischen Standard zu erwarten, weil solche Prozesse mehrere Jahre dauern.

Prof. Eberspächer:
Ganz so einfach war es ja auch im Mobilfunk nicht, aber man hat es geschafft. Ich weise darauf hin, dass GSM eine völlig europäische Entwicklung war, aber die neueste Generation namens LTE sogar global standardisiert wurde. Da gibt es also globale Übereinkünfte, was durchaus ein Wunder ist angesichts des Wettbewerbs über die Erdteile hinweg. Ich finde, es ist schon ein schönes Beispiel, wie das im Mobilfunk funktioniert.

Prof. Thielmann:
Ich habe eine ganz andere Frage an Herrn Sieber. Sie sind Jurist und Experte auf dem Gebiet des Datenschutzes und des Identitätsschutzes, wie wir heute Vormittag sehr eindrucksvoll gehört haben. Meine Frage ist: Wie weit sind unsere Juristen im Feld draußen, die Staatsanwälte, die Rechtsanwälte, die Richter usw. mit diesen Themen vertraut, so dass sie im Konfliktfall auch tatsächlich tätig werden können und gibt es dafür einen Ausbildungsbedarf?

Prof. Sieber:
Das ist in allgemeiner Weise schwer zu beantworten. In den letzten Jahren hat sich jedoch einiges getan nicht so sehr beim flächendeckenden Wissen aller Ermittlungsbeamten,

Staaanwälte und Richter, aber doch im Bereich von Spezialzuständigkeiten. Insbesondere im Bundeskriminalamt und in den Landeskriminalämtern gibt es spezialisierte und sehr kompetente Einheiten. Gutes Fachwissen ist auch bei einzelnen spezialisierten Staatsanwälten vorhanden. Wir sehen Fortschritte, wollen aber selbstverständlich mehr. Der Entwicklungsprozess hat aber sicher schon seit längerem begonnen.

Prof. Eckert:
Herr Rannenberg wollte auch noch etwas dazu sagen.

Prof. Rannenberg:
Noch mehr zu der Frage von GSM. Ich freue mich immer, wenn GSM gelobt wird, schließlich bin ich Mobilkommunikationsprofessor. Aber ich habe im Workshop 2 ja eine Moderatorenrolle gehabt. Deshalb habe ich dazu nichts gesagt. Ich denke, aus dem GSM Beispiel könnten wir tatsächlich noch mehr lernen als wir gegenwärtig lernen. Es sind aber noch zwei Facetten wichtig, neben dem Mobilkommunikationsmarkt, soweit es denn schon überhaupt ein Markt war, da die Player doch relativ reguliert waren. Die Standardisierung von GSM hat eingesetzt bevor es überhaupt digitale Mobilkommunikation im Markt gab, mindestens in Europa und auch anderswo, und auch, bevor Mobilkommunikation überhaupt ein Massenmarkt war. Da gab es zwar einige Vorläufertechnologien, aber die waren mit relativ kleiner Marktausprägung da. 2005 hat man angefangen, Email zu standardisieren. Das war 18 Jahre nachdem ich − und ich bin noch einer der späteren Email-Nutzer − meine erste Email geschrieben habe. Das war nämlich schon 1987. Es hat schon Leute gegeben, die in den 70er Jahren Emails geschrieben haben. Wenn wir so einen Erfolg wie bei GSM wieder hinkriegen wollen, der sich in vieler Hinsicht rentiert hat, auch strategisch vielleicht im Sinne von Rückgewinnung von Technologien oder aus europäischer strategischer Sicht, Gewinnung von Technologien, dann müssten wir uns jetzt eigentlich sehr genau angucken, was die Dinge sind, die in 10 bis 15 Jahren kommen werden. Wir müssen den Mut haben da jetzt zu investieren, in die Entwicklung dieser Dinge, in die vorlaufende Standardisierung dieser Dinge und natürlich vorweg in die Überlegung, was das Nutzungsszenario dafür ist. Ich habe vielfach erlebt, dass Leute meinten, dass zukunftsorientierte Standardisierung keinen Sinn macht. Standardisierung darf nur das standardisieren, was im Markt schon da ist. Damit bekommt man einen GSM Erfolg nicht hin. Wenn wir etwas erreichen wollen, müssen wir das GSM Beispiel deutlich ernster nehmen als wir es vielleicht bislang genommen haben, was aber auch wieder heißt: bei der Standardisierung in die Zukunft zu schauen.

Herr Schneider :
Ich möchte vielleicht auch noch etwas hinzufügen. GSM klingt immer so ein bisschen nach Vergangenheit. Heutzutage führen wir den 4G Standard ein, Long Term Evolution. Auch im Telekommunikationsbereich findet sehr viel Standardisierung statt, weil einfach die Netze insgesamt weltweit funktionieren müssen. Und auch in dem Bereich ist Security Teil der Standardisierung. Bei den Themen, die ich heute Morgen erklärt habe, wie dieser Zugang geschützt wird, sind viele dieser Elemente heute in einem Standard mit enthalten. Die meisten Telekommunikationsunternehmen implementieren auch diese Security Elemente. Ein Problem ist natürlich, dass diese Infrastruktur auch über sogenannte Over the Top Player genutzt wird, die wiederum Dienste anbieten, die dann aber nicht den Telekommunikationsstandards oder Reglementierungen unterliegen, weil diese Player keine Operator oder Carrier sind sondern generelle Wirtschaftsunternehmen, die deutlich geringere Anforderungen an solche Themen haben. Sprich: da, wo das Standardisierungsthema gemacht wird, wird die Security auch oft eingebracht. Aber es gibt auch viele Bereiche, die heute nicht standardisiert sind und einfach noch Schwachstellen darstellen, woran aber auch kontinuierlich gearbeitet wird.

Dr. Jäger, Uniscon München:
Daran möchte ich anknüpfen: Wie Herr Schneider richtig sagte, kommen die Bedrohungen nicht von den Übertragungs- oder Transportprotokollen, sondern finden auf der Applikationsebene statt. Sprechen wir also heute von Facebook und Google und die Angriffe auf die Privatsphäre – was wir im Internet Privacy nennen – dann interessiert uns nicht die großartige Kommunikation, die man mit Social Networks haben kann oder was man alles mithilfe der Suchmaschinen findet. Wir sprechen über Geschäftsmodelle. Über die Geschäftsmodelle, auf denen Facebook oder Google basieren. Wenn wir 10 Jahre oder mehr nach vorne schauen, werden wir hier einen massiven Wandel beobachten. Durch die Transparenzmaschine „Internet" werden die Menschen diese Modelle durchschauen. Ähnlich wie die Entwicklung der Umweltschutzbewegung in den 70er und 80er Jahren, als Experten schon früh erkannt haben, dass die Natur Hilfe braucht. Erst mehrere Jahrzehnte später ist es zu einem Konsens in der Gesellschaft geworden, dass Umweltschutz ein Erfordernis ist. Mit Privacy wird es nicht viel anders sein. Und Deutschland hat im Bereich Datenschutz eine langjährige Tradition, die es in wirtschaftliche Innovationen stecken kann. Hier nun liegt Deutschlands Chance: Wir könnten maßgeblich zur Weiterentwicklung des Internets beitragen, endlich signifikant am IT-Markt mitmischen.

Prof. Eberspächer:
Hoffen wir es! Die nächste Wortmeldung.

Dr. Kobylinski, incapptic GmbH:
Ich glaube, man kann Security nicht grundsätzlich und schon gar nicht staatlich standardisieren. Dafür ändern sich die Anforderungen viel zu schnell. Ich bin da mehr bei Herrn Schallbruch. Die Absicherung der Netze ist ein Thema für die Carrier. Für sie kann es ein Geschäftsmodell sein, so etwas als zusätzliche Leistung anzubieten. Das liegt eigentlich auf der Hand und wird teilweise schon gemacht. Meine Überzeugung ist allerdings, dass wir es hier in Deutschland mit der Regulierung übertreiben. Die Einführung neuer Geschäftsmodelle scheitert viel zu oft, weil zu einem sehr frühen Zeitpunkt Betriebsräte involviert werden müssen und irgendwelche antiquierten Gesetze greifen, die ihren Ursprung in den Anfängen der Industrialisierung haben. So werden Innovationen verhindert. Das durch zusätzliche staatliche Regulierung in Sachen Security heilen zu wollen, halte ich für absurd.

Prof. Sieber:
Wir haben sicher viele reformbedürftige Vorschriften, jedoch sehe ich keine grundsätzlich antiquierten Regulierungsmodelle. Vor zehn Jahren konnte man den deutschen Datenschutz vielleicht noch für überzogen halten. Wenn man aber jetzt sieht, was im privaten Sektor an Daten gespeichert wird und was an Daten zusammengeführt wird, so muss man die Notwendigkeit des Datenschutzes anerkennen. Viel von dem, was Orwell vorausgesehen hat, finden wir heute im privaten Sektor in neuen Geschäftsmodellen zur Monetarisierung von Daten. Wir müssen in diesem Bereich deswegen heute eher darüber nachdenken, wie wir unsere Datenschutzregelungen effektiver durchsetzen können. Für die Probleme der Globalisierung und Internationalisierung haben wir noch keine gute Lösung gefunden. Staaten mit dem niedrigsten Schutzniveau setzten Standards, es kommt zu einer Verlagerung von Aktivitäten in diese Staaten und deren Standards setzen sich dann durch. Wir sollten daher darüber nachdenken, wie wir unsere europäischen Standards weltweit besser durchsetzen können Wenn ich mir ansehe, wie die USA ihre Ansprüche auf Herausgabe von Steuerdaten gegen die Schweiz durchsetzen, so halte ich das zwar nicht für beispielhaft. Möglicherweise kann man aber durch wirtschaftliche Sanktionen Druck auf Unternehmen ausüben, die hier in Deutschland Geschäfte machen, um gewisse Standards durchzusetzen. Wir müssen uns diesen globalen Problemen stellen. Entsprechendes gilt für neue Public Private Partnerships. Auch hier sehe ich neue Ansatzmöglichkeiten.

Prof. Eberspächer:
Sie haben noch eine Ergänzung.

Dr. Kobylinski:
Ich würde das gern an einem banalen Beispiel aus meiner persönlichen Lebenswelt als frisch gebackener Start-up Unternehmer illustrieren. Ich finde es, mit Verlaub, völlig absurd, dass ich in Deutschland einen Anwalt konsultieren und seitenweise AGBs publizieren muss, sobald ich auch nur eine ganz einfache Webseite online stellen will. Das ist heutzutage ein Standardvorgang und wenn hier noch so viel Klärungsbedarf besteht, ist das für mich ein Versagen des Gesetzgebers. Zusammen mit der Diskussion über die Notwendigkeit und Beschaffenheit eines Impressums auf Facebook ist das doch nur ein Arbeitsbeschaffungsprogramm für Anwälte. Und macht uns ganz sicher nicht innovativer.

Prof. Eckert:
Herr Schallbruch, Sie wollten auch noch etwas dazu sagen.

Herr Schallbruch:
Ja, das passt jetzt gut, weil ich Ihnen da beitreten möchte und, was ich ungern tue, Ihnen Herr Sieber wirklich widersprechen möchte, gerade was den Datenschutz angeht. Wir haben hier gerade eine Diskussion über europäisches Datenschutzrecht. Die Kommission hat einen Vorschlag vorgelegt. Und da wird immer gesagt, dass wir das deutsche hohe Schutzniveau erstens erhalten und zweitens möglichst flächendeckend umsetzen müssen. Ich bin aber gar nicht sicher, ob wir mit unserem Datenschutzrecht – was den privaten Sektor angeht – überhaupt noch zukunftsfähig sind. Ich habe wirklich Zweifel daran, ob unser Datenschutzrecht, so wie es für das Verhältnis Bürger-Staat konstruiert und auf den gesamten privaten Bereich übertragen wurde, die anstehenden Probleme des Internets überhaupt noch lösen kann. Zum einen haben wir im Internet eklatante Persönlichkeitsrechtverletzungen, denen wir mit dem Mittel der Einwilligung nicht zu Leibe rücken können: dass man irgendwo einmal eingewilligt hat bei Facebook oder Google oder iTunes und dann Monate später ganze Adressbücher irgendwohin geladen werden, plötzlich biometrische Gesichtserkennungsverfahren eingesetzt werden usw., ohne dass der Nutzer das irgendwie zu irgendeinem Zeitpunkt vernünftig erkennen konnte, dass das möglicherweise einmal von der Reichweite seiner Einwilligung erfasst sein soll. Das finde ich sehr problematisch, wird aber von unserem Datenschutzrecht kaum erfasst und auch nicht von dem Vorschlag, den die EU-Kommission jetzt gemacht hat. Auf der anderen Seite haben wir Start-up Unternehmen wie Ihres zum Beispiel, die Daten verarbeiten und wo es in endlicher Zeit kaum möglich ist, eindeutig aus dem Datenschutzrecht herauszulesen, ob diese Datenverarbeitung wirklich zulässig ist. Weil unser Datenschutzrecht eben kompliziert ist, weil es auf das einzelne Datum abhebt, auf die einzelne Datenverarbeitungsphase usw. Wenn man sich dann z.B. eine iPhone-App anschaut, wo die App noch mit einem Anbieter im Internet zusammenwirkt und wo der Betriebssystemhersteller Apple und der Telekommunikationsanbieter ebenfalls eine Rolle spielen. Diese Datenverarbeitung dort rechtlich zu bewerten, fällt schwer. Und die Datenschutzbeauftragten sagen auch, dass sie das erst etwas grundsätzlicher beurteilen, weil sie den Fall auch nicht ganz genau an den Buchstaben des Rechts lösen können. Deshalb halte ich es für wichtig, dass wir uns wieder mehr an dem Grundgedanken des Persönlichkeitsrechtschutzes orientieren und nicht so sehr an dem Formalismus einzelner Datenverarbeitungsvorgänge. Ich glaube, dass wir daher jetzt auf europäischer Ebene noch eine schwierige Diskussion haben werden. Und wir sprechen uns hier nicht dafür aus, das Schutzniveau abzusenken, sondern, anders als die Kommission uns sozusagen unterstellt, dass wir besser differenzieren, um die wirklich harten Fälle zu erfassen und die alltägliche Datenverarbeitung, dass ein Mensch Daten von seinen Freunden beispielsweise auf seinem Smartphone im Kontaktbuch hat, nicht unter strenge Einvernehmensregelungen fallen zu lassen.

Prof. Sieber:
Dieser besseren Differenzierung widerspreche ich nicht.

Herr Schallbruch:
Wunderbar.

Prof. Sieber:
Das deutsche Recht ist durch seine Kleinteiligkeit und Genauigkeit oft überreguliert. Dies zeigt sich deutlich bei den Datenschutzstrafvorschriften, die immer weiter und weiter auf andere Datenschutzvorschriften verweisen. Im Ergebnis wird dadurch praktisch auch das gesamte Datenschutzrecht sanktionsbewehrt. Jeder Verstoß fällt letztlich unter eine Straf- oder Bußgeldvorschrift. Aber um das herauszufinden, muss man sich durch eine Verweisung zur anderen durchfinden. Das ist in der Tat viel zu kompliziert. Wir brauchen knappe Regelungen, die sich auf die wirklich gravierenden Fälle konzentrieren.

Prof. Eberspächer:
Jetzt war da Herr Schöne.

Prof. Eckert:
Kann ich gerade noch mal eine Nachfrage stellen? Es war doch eine ganz klare Forderung auch von dem Kollegen gerade, doch auch das deutsche Datenschutzrecht ein bisschen zurückzuschrauben. Jetzt haben Sie, Herr Sieber, heute Morgen dargestellt, dass jetzt gerade eine Novellierung in Arbeit ist. Wie gehen Sie denn mit solchen Anregungen jetzt um? Nehmen Sie das mit rein in den Novellierungsprozess, diesen auch mal zu entrümpeln? Darüber nachzudenken, wo vielleicht zu starke bürokratische Hürden drin sind, die gar nicht das bringen, was wir uns dahinter vorstellen? Werden solche Stimmen wie jetzt gerade Einzelstimmen, die sicherlich mehrheitlich da sind, auch erfasst und aufgenommen?

Prof. Sieber:
Heute Morgen habe ich mich mit den strafrechtlichen Fragestellungen beschäftigt. Meine Forderung dazu ist, dass wir uns auf die krassen Fälle beschränken und nicht flächendeckend kriminalisieren. Die langen Listen im Datenschutzgesetz mit den Verweisungen sind unverständlich. Von dieser Verweisungsabhängigkeit möchte ich deswegen gern wegkommen. Ich würde das Datenschutzstrafrecht gern auf die krassen Fälle konzentrieren, das Strafrecht aber in diesem Bereich dann auch wirklich durchsetzen.

Prof. Eckert:
Schon wirklich ein Entrümpeln und Fokussieren?

Prof. Sieber:
Fokussieren, ja. Das ist die alte Funktion vom Strafrecht als ultimo ratio, d.h. als letztem Mittel. Strafrecht soll die gravierenden Fälle erfassen und nicht flächendeckend kriminalisieren.

Prof. Eckert:
Wann dürfen wir damit rechnen, dass wir dann auch unter dieser Novellierung leben? Gut. Warten Sie noch ein bisschen mit dem Start-up!

Prof. Eberspächer:
Herr Schöne!

Herr Schöne, Pressebüro Schoenetexte:
Ich möchte kurz vor Ende noch einmal auf die Sicherheit zurückkommen. Cloud ist auch auf dieser Konferenz ein großes Thema gewesen und wird seit ungefähr zwölf Monaten heftig als die neueste Supersau durch die IT getrieben, die alle Probleme lösen soll. Sie stellt uns aber vielleicht noch vor große Herausforderungen. Es wird nämlich z.B. jetzt diskutiert, was wäre, wenn sich ein großes Rechenzentrum mit 100 Firmen und hunderten von virtuellen Servern eine Malware einfängt? Diese Malware purzelt runter von den virtuellen Servern auf den realen Server, vergiftet das ganze Rechenzentrum und schießt die ganzen anderen 100 Firmen ab. Diese theoretischen Überlegungen gibt es bereits. Eine praktische Umsetzung kenne ich noch nicht. Die Frage wäre: Wann glauben wir, sehen wir so etwas in der Realität und was sagen die Juristen dazu? Wer haftet in solch einem Fall?

Prof. Eberspächer:
Ja, wer haftet?

Prof. Eckert:
Die Frage war: Was sagen die Juristen dazu?

Prof. Eberspächer:
Die Frage gilt ja auch für den Trend der Virtualisierung. Die Netze werden ja zunehmend virtualisiert. Wie viel Abschottung gibt es da noch?

Prof. Rannenberg:
Also, vielleicht kann ich dazu als Nichtjurist dazu einen kleinen Ausflug machen. Ich will jetzt keine Namen nennen, was es so an großen Anbietern von Public Clouds gibt. Es gibt ein Beispiel, wenn Sie sich die AGBs eines großen Anbieters anschauen, der auch im Versandhandel unterwegs ist, wissen Sie ja, dass alles über das Internet geht und Angriffe aus dem Internet schließt der Anbieter aus der Haftung aus. Ich denke mal, dass das eher die Frage ist.

Prof. Eckert:
Ich hatte Herrn Lotz genötigt, kurz Stellung zu nehmen, aber er will erst noch einmal kurz nachdenken. Die SAP ist ja auch ein Cloud Anbieter und kann etwas dazu sagen, wie man mit z.B. Virtualisierungskonzepten usw. hierzu technische Lösungen bereitstellen kann.

Prof. Veit, Universität Mannheim:
Ich setze mich mit eBusiness und eGovernment seit längerem auseinander. Wir, Herr Picot, Herr Krcmar, Herr Kagermann, einige andere und ich, haben vor einiger Zeit, im Herbst letzten Jahres, ein Papier zum Thema „Harmonisierte Cloud – Infrastrukturen in Europa“ geschrieben und haben darin von der Bunderegierung letztendlich auch gefordert, eine Förderung zu dem Themengebiet aufzulegen. Der Grund ist, dass wir der Auffassung sind, dass sich in dem Markt der Cloud-Anbieter relativ schnell Lock-In-Situationen ergeben. Sie haben gerade einen großen Versandhändler genannt, der in diesem Bereich eine solche Situation hergestellt hat. Aber auch andere bieten Dienste an, von denen normalerweise die Mehrzahl nicht in Europa angesiedelt sind, sondern irgendwo anders auf der Welt und damit physisch die Daten dorthin verschieben mit für das deutsche und europäische Recht letztlich nicht abschätzbaren Folgen für diesen Datenbestand. Die Frage ist: Sehen Sie die Notwendigkeit infrastrukturell Anreize zu schaffen oder auch regulatorische Möglichkeiten zu schaffen, dass hier solche Anbieter entstehen? Gründe dafür, dass diese hier eben derzeit nicht entstehen, sind zum Teil meines Erachtens gerade darin zu finden, dass es einfach sehr komplex ist, in Deutschland einen solchen Dienst aufzusetzen im Gegensatz zu anderen Rechtsräumen. Wie sehen Sie das?

Prof. Eckert:
An wen war die Frage?

Herr Schallbruch:
Wir haben in der Bundesregierung, federführend durch das Bundesministerium für Wirtschaft und Technologie, ein Programm „Trusted Cloud“ dazu aufgelegt, was sehr intensiv in den IT-Gipfelprozess eingebettet ist, wo sich drei von sechs Arbeitsgruppen des IT-Gipfels mit dieser Frage beschäftigt haben und in diesem Programm entwickeln wir gerade a) Anforderungen und b) Realisierungsmöglichkeiten für sichere Cloud-Angebote. Wir haben als Sicherheitsverantwortliche durch das Bundesamt für Sicherheit und Informationstechnik schon vor einem Jahr ein Papier zu Sicherheitsanforderungen beigesteuert, haben das zur Diskussion gestellt und breit abgestimmt und im Übrigen mit dem Forschungs- und dem Wirtschaftsministerium auch vereinbart, dass wir jetzt im BSI überlegen, zu einer Zertifizierung für Cloud-Dienste zu kommen. Was wir gegenwärtig nicht planen, ist ein staatliches Cloud-Angebot.

Prof. Eckert:
Herr Lotz möchte gerade noch mal auf die technischen Aspekte von Cloud und die Frage von vorhin Stellung nehmen und auch Herr Köhler möchte noch einmal Stellung nehmen.

Herr Lotz:
Ich beuge mich jetzt dem Druck von Frau Eckert und sage doch etwas zum Thema Cloud. Ich teile eine ganze Reihe der Bedenken, die hier geäußert worden sind, insbesondere natürlich auch, was die Fragen hinsichtlich der Verteilung von Verantwortlichkeit und damit auch Haftungsfragen in einer verteilten Infrastruktur betrifft. Das hat auch zur Folge – wir sehen das derzeit bei unseren Kunden -, dass diese noch nicht so weit sind, den Weg in eine öffentliche Cloud zu gehen. Wir nutzen daher Cloud derzeit in erster Linie als eine Technologie, die es uns erlaubt, zu günstigen Konditionen Kunden Applikationskapazität zu bieten. Das heißt also, wir nutzen Cloud Technologie, um ein On-Demand-Angebot zu machen. Um den nächsten Schritt zu gehen, beispielsweise hin zu SAP-fremden Betreibern einer on Demand Lösung von SAP-Lösungen, müssen wir einen Sicherheitsstandard vorantreiben. Was Herr Schallbruch eben erwähnt hat im Hinblick auf Trusted Cloud, liegt uns natürlich auch am Herzen. Wir haben etwa eine Initiative in die Wege geleitet, deren Ziel es ist, etwas wie einen „Gold-Standard“ für Trusted Cloud europaweit einzuführen. Das sehen wir als den richtigen Weg. Ich möchte aber auch gleichzeitig anmerken, dass hier noch einige Forschungsfragen zu bewältigen sind, mit denen wir uns derzeit beschäftigen, wo aber Lösungen noch nicht vorhanden sind. Ein Beispiel ist Zertifizierung. Wie können wir Zertifizierungsschemata etablieren, die mit diesen verteilten Infrastrukturen umgehen können? Kurz gesagt: die Common Criteria können das heute noch nicht. Hier müssen wir einfach weiter investieren, um dann schließlich diesen Schritt in eine weiter verteilte Umgebung gehen zu können.

Herr Köhler:
Ich glaube, das müssen wir noch differenzierter sehen. Wir haben ein Public Cloud. Wir haben eine Private Cloud. Wir haben die Hybrid Cloud. Das Problem ist, dass in den meisten Unternehmen, die in die Cloud gehen wollen, diese Thematiken gemixt werden und je nachdem, was für eine Beratung sie erhalten, ist die Frage, was für Applikationen für welche Cloud überhaupt adäquat sind. Was wir so sehen, ist, dass es eine sektorale Cloud geben wird. Nehmen wir mal die Automobilzulieferer. Die kennen ihre Prozesse. Die kennen auch die Gesetzmäßigkeiten, die sie abwägen müssen. So ein Cloud Anbieter, der speziell für dieses Segment etwas aufbaut, kann das kostengünstig machen. Wenn ich mir jetzt aber alle

anderen Sektoren dazu nehme, wird es schwieriger, diese Zuordnung, dieses Mapping von Compliance Vorschriften auf die Prozesse zu machen, wird Ihnen keiner so 'out of the box' geben können. Von daher glauben wir schon, dass die Standardisierung auch eine Marktfrage ist. Dafür gibt es ein wunderschönes Beispiel, die Cloud Security Lines, die sich aus einem losen Bund von großen und kleinen Unternehmen entwickelt. Mittlerweile arbeiten global 80.000 in diesem Verbund mit. Es gibt sie in den USA, in Deutschland. Plötzlich wird aus diesem losen Cloud Security Alliance Standard ein Interesse und wandert so langsam in die ISO Norm Richtung hinein. Da ist es vernünftiger zu sagen, dass man früh genug in diesem losen Zusammenhang erst mal mitarbeitet, um diese Standards Ideen mit zu entwickeln, weil momentan die meisten Technologien aus den USA kommen und nicht aus Europa. Deswegen schwappt es eher hier herüber und es ist nicht so wie Kai Grassie sagt, wir haben nicht so die Zeit, diese 10, 15 Jahre vorzudenken, sondern die ganzen Cloud Technologien entwickeln sich jetzt. Das ist rapid Innovation. Und wir müssen jetzt mit daran arbeiten und gucken, was sich vielleicht in zehn Jahren um die Cloud herum entwickelt.

Prof. Rannenberg:
Die 15 Jahre vorlaufende Standardisierung bezog sich nicht auf die aktuellen Sicherheitsprobleme bei und mit Cloud Computing. Dafür muss man schon jetzt etwas tun, bzw. man hätte in den letzten 15 Jahren, seit sich verteilte Anwendungen, die wir jetzt Cloud Computing nennen, ankündigt, etwas tun müssen. Das ist klar. Aber was wir halt machen müssen, wenn wir wieder diesen Vorsprung, der uns bei GSM wirtschaftlich stark gemacht hat, erreichen wollen, ist für 15 Jahre voranzudenken und zu überlegen, was dann da ist. Bei GSM ist uns das ja auch geglückt. Oder wir sagen, es geht gar nicht mehr und vergessen den Forschungsstandort Deutschland bzw. Europa. Aber es geht ja schon. Nur muss man wirklich Mut haben, darüber nachzudenken, was in 15 Jahren relevant werden könnte und wie die Sicherheitsmaßnahmen dafür zu machen sind. Das ersetzt nicht, jetzt mit den Problemen beim Cloud Computing umzugehen, ist aber für die Zukunft nötig.

Dr. Harlander, GeNUA mbH:
Ich muss leider noch einmal auf das Thema vorher zurückkommen, nämlich auf die Frage, welches Niveau von Datenschutz wir eigentlich brauchen. Herr Schallbruch, Sie haben sich ein bisschen beklagt über die etwas weich gespülte Vorlage der Kommissarin Kroes auf EU-Ebene. Herr Helmbrecht, nun ist es ja so, dass Sie die Frau Kroes beraten mit Ihrer Agentur. Meine Frage ist: Stammt diese Vorlage etwa aus Ihrem Haus? Und wenn sie aus Ihrem Haus stammt, meine zweite Frage: Ist es so, dass das eine inhaltliche Position ist, die innerhalb der ENISA erarbeitet wird oder stehen Sie als europäische Agentur auch in dem Konflikt, dass sie quasi 27 Meinungen einigermaßen konsensfähig unter einen Hut bringen müssen, um dann einen politisch durchsetzbaren Vorschlag in der Kommission zu erstellen?

Prof. Helmbrecht:
Zur Klarstellung: Es gibt Kommissarin Neelie Kroes, die das Portfolio Mediengesellschaft, " Digitale Agenda" verantwortet und Frau Reding ist als Kommissarin dafür zuständig, was alle juristischen Belange betrifft. Insofern heißt auch die Generaldirektion DG INFSO bei Frau Kroes und DG JUSTICE bei Frau Reding. Ein Gesetzentwurf stammt immer aus der Feder, wir würden hier sagen, eines Ministeriums. Das heißt also, aus der Feder eines Referates in einer Generaldirektion. Im Prinzip sind die europäischen Gesetzgebungsprozesse ähnlich wie die bei der Bundesregierung. Es gibt ein federführendes Kommissariat, eine federführende Generaldirektion und dort gibt es ein Referat, das zuständig ist und aus dessen Feder stammt das. Darüber wird dann innerhalb der Kommission abgestimmt. Insofern waren wir daran nicht beteiligt. Ich will es aber noch ergänzen. Es ist so, dass Sie auf europäischer Ebene auch den EDPS, European Data Protection Supervisor, haben, der

es am Ende als Aufsichtsbehörde umsetzen muss. Wir sind eine Agentur, die mit dem EDPS in dem Sinne zusammenarbeitet, ihn unterstützt und in Artikel 29 Arbeitsgruppe, in der die Datenschützer organisiert sind, und wir eher in diesem IT Privacy Bereich tätig sind.

Prof. Spiekermann, Wirtschaftuniversität Wien:
Herr Helmbrecht, Sie haben gesagt, New Currency Personal Data, unsere persönlichen Daten werden zu einer neuen Währung. Gleichzeitig stellt im Prinzip das gesamte Podium fest, dass der neue Datenschutzverordnungsvorschlag eigentlich zu kurz greift und nicht wirklich an die Probleme herangeht. Jetzt wird schon seit Jahren in den USA die Idee diskutiert, ob man nicht persönliche Daten mit Eigentumsrechten belegen sollte. Also, wir sind Eigentümer unserer persönlichen Daten und wir geben möglicherweise Firmen Nutzungsrechte an diesen Daten. Meine Experimente an der Wirtschaftsuni haben gezeigt, auf Basis einer Befragung von 1.500 Facebook Usern, dass in der Tat, wenn man Leuten bewusst macht, dass es da einen Markt gibt und sie Eigentumsrechte bekommen, sie plötzlich viel bewusster mit ihren Daten umgehen, diese vielmehr wertschätzen, sich also zu tatsächlich rationalen Marktakteur entwickeln. Zumindest geht es in die Richtung. Die Frage, die ich jetzt an das Podium und insbesondere an Herrn Sieber habe, ist: Ist das denkbar?

Prof. Helmbrecht:
Wenn ich da anfange, würde ich sagen, denkbar ist vieles. Ich möchte ein paar Aspekte einbringen, worin die Schwierigkeiten liegen, was man berücksichtigen muss und ob man dahin kommt. Wir haben vor kurzem eine Studie veröffentlicht, die heißt „Monetarisierung von personenbezogenen Daten " und wir haben Laborstudien durchgeführt, ca. 2.000 Menschen befragt. Das Interessante ist, wenn in den Geschäftsbedingungen bewusst gemacht wird, wie das Datenschutzniveau ist, also der Kunde aufmerksam gemacht wird, dann ist der Kunde bereit, den Provider zu wählen, der weniger Daten sammelt oder mehr für den Datenschutz tut. Es gibt sogar eine kleine Bereitschaft dafür zu bezahlen. Das ist nicht ganz so gut ausgeprägt, und das muss man vielleicht noch weiter untersuchen. Aber die Botschaft ist: Wenn Kunden deutlich ist, was mit Daten passieren kann und wenn jemand sagt, dass er sorgfältiger mit Daten umgeht, kann das zum Wettbewerbsvorteil werden. Der andere Punkt ist der, dass wir wissen, vielleicht nicht bewusst, aber eigentlich wissen könnten, dass wir mit unseren Daten bezahlen. Das heißt, wenn ich eine Location Based Service Anwendung als App auf meinem Smartphone habe, dann weiß ich doch, wenn ich die Geschäftsbedingungen angeklickt habe, sonst kann ich die App nicht runterladen, dass ich meine personenbezogenen Daten abgebe. Und dafür bekomme ich eine Dienstleistung. Es wird nicht so transparent gemacht. Aber ich weiß heute, und so gehe ich persönlich damit um, dass ich mit jeder App, die ich herunterlade, meine Daten abgebe. Die sind verloren. Da kann ich heute nichts dagegen tun. Das kann ich nicht einklagen. Aber ich freue mich, wenn ich die Dienstleistung bekomme. Das ist doch ein Geschäft.

Prof. Sieber:
Ich wäre mit Ihrem Modell einverstanden, wenn es dem Kunden wirklich transparent gemacht würde. Und da liegt mein Anliegen: Dass der Kunde zumindest grob erfährt, was mit seinen Daten gemacht wird. D.h., dass er die Daten bewusst und in Kenntnis der relevanten Umstände hergibt. In der gegenwärtigen Praxis weiß der Nutzer jedoch oft nicht, was mit seinen Daten gemacht wird. Dagegen wendet sich meine Kritik.

Prof. Helmbrecht:
Wir sind uns im Prinzip wahrscheinlich einig. Die Problematik besteht darin, dass wir in vielen Fällen unbewusst wissen, welche Gefahren wir eingehen. Wenn wir manchmal darüber reden, wie junge Leute mit sozialen Netzwerken umgehen, dann nehmen Sie zum

Vergleich auch ein Beispiel aus dem klassischen realen Leben: Wochenende, Landbevölkerung, Landjugend, Discobesuch. Jeder weiß, dass Schnellfahren bei Regen, wenn ich aus der Disco komme, gefährlich ist. Wir stellen Bilder von kaputten Autos hin und trotzdem fahren die Jugendlichen so, obwohl sie es wissen. Sie wissen es wahrscheinlich in dem Moment, wo sie aus der Disco herauskommen. Eigentlich müssten sie es wissen und eigentlich müssten sie auch wissen, was sie in den sozialen Netzwerken machen. Wir versuchen ihnen das ja beizubringen. Vielleicht ist die Frage, warum das Awareness Raising nicht so funktioniert, wie wir das eigentlich wünschen.

Prof. Spiekermann, Wirtschaftsuniversität Wien:
Ja, ich frage Sie aber noch einmal. Eigentumsrecht an persönlichen Daten ist doch ein anderes Rechtskonstrukt. Das ist ja etwas ganz anderes. Was mich eben interessieren würde, ist: Ist es juristisch denkbar, umsetzbar, vorstellbar, dass wir so etwas bekommen? Herr Sieber, Sie sind der Jurist.

Prof. Sieber:
Der Eigentumsbegriff kommt aus dem Recht der körperlichen Gegenstände. Eigentum bedeutet: Ich darf mit einem körperlichen Gegenstand machen, was ich will und ich darf alle anderen von der Nutzung dieses Gegenstandes ausschließen. Dieses Eigentumskonzept passt jedoch nicht für Daten und Informationen. Informationen sind zunächst einmal ein öffentliches Gut. Die darf jeder andere auch benutzen. Er kann sich dabei oft auf den Grundsatz der Informationsfreiheit berufen. Um andere im Einzelfall auszuschließen, sind Gegengründe und eine Interessensabwägung erforderlich. Das ist nicht so einfach wie beim Sacheigentum. Wir brauchen daher für Daten eigenständige Konzepte.
Ein entsprechendes Gegenrecht kann sich etwa aus dem Persönlichkeitsrecht ergeben, das mit dem Recht auf Informationsfreiheit abgewogen werden muss. Bei personenbezogenen Daten kann es deswegen auch entscheidend sein, ob der Betroffene der Datennutzung zustimmt. Dabei müssen allerdings die Bedingungen, unter denen zugestimmt wird, fair sein. Die Menschen müssen wissen, in was sie einwilligen. Wenn sie Daten dann bewusst und in Kenntnis der maßgeblichen Umstände freigeben, so müssen sie sich jedoch in der Regel daran festhalten lassen. Vielleicht kann man ihnen dann noch mit dem Recht auf Vergessen helfen und mit entsprechenden Widerrufs- und Löschungsrechten. Auch das zeigt aber, dass das das Recht am eigenen Datum etwas anderes ist als das Eigentumsrecht an einer Sache.

Prof. Eckert:
Ich wollte eine kurze Anmerkung machen zum Recht auf Vergessen. Wir müssen ein bisschen aufpassen, wenn wir juristische Forderungen in den Raum stellen, was wir da technisch gegenhalten können. Was ist denn eigentlich Eigentumsrecht an Daten? Wem gehören denn die Daten, Verkehrsdaten? Gehören die dem Provider? Gehören die dem Anbieter? Gehören die mir? Wie mache ich denn das, wenn ich ein Foto mache von Ihnen allen? Wer ist der Eigentümer dieses Fotos? Das ist jetzt alles nicht ganz trivial. Oder auch jemanden zu identifizieren, technisch festzuhalten, wer eigentlich der Urheber von sowas ist. Und mit Recht auf Löschen kommen wir ganz in die Bredouille bei den digitalen Daten. Das von mir zu diesem Thema. Herr Köhler, gleich dazu?

Herr Köhler:
Bei diesen disruptiven Innovationen, das wird ein großer Stopper, weil ich mir nicht vorstellen kann, dass jemand ein Business Modell darauf aufbaut, wenn er plötzlich diese Dinge auch noch in sein Business Modell mit einrechnen müsste. Er hat heute schon Probleme mit seinen Standardinfrastrukturen Compliance herzustellen. Das würde voraussetzen, dass Sie

anfangen Daten zu klassifizieren. Und das im großen Spektrum kann ich mir nicht vorstellen, dass da noch ein Funken Innovation von einer Start up Company kommt, die eine tolle Idee hat und das versuchen will. Das funktioniert nicht.

Herr Schallbruch:
Wir haben die Frage auch diskutiert. Kann man sich bei Daten so etwas wie eigentumsähnliche Konstruktionen vorstellen? Wir lehnen das ähnlich wie Herr Sieber ab, weil wir uns in Kommunikationsverhältnissen befinden. Und wenn ich meine Daten entäußere, sind sie ein Stück weit weg. Ich kann auch nicht Liebesbriefe, die ich vor 20 Jahren geschrieben habe, unter Verweis auf einen Herausgabeanspruch zurückverlangen. Und ich werde die auch nicht zurückverlangen können, wenn sie denn vor 20 Jahren über das Internet geschrieben sein werden unter Verweis auf das Reding'sche Recht auf Vergessen, weswegen das juristisch nichts taugt. Als Anspruch, man sollte nicht immer alles auf alle Zeiten speichern, ist das vernünftig, also als politische Zielsetzung, aber als juristisches Konzept nicht. Wir haben vielmehr eine Abgrenzung und auch Abwägung zwischen unterschiedlichen Grundrechten. Und da gibt es eben Grundrechte der Kommunikations- und Äußerungsfreiheit und der Informationsfreiheit und die stehen eben Persönlichkeitsrechten gegenüber. Und es gibt Grundrechte auf wirtschaftliche Betätigung, die ein Start-up hat und die stehen eben auch anderen Rechten gegenüber. Deshalb glauben wir, weil wir inzwischen auch durch elektronische Kommunikation leben und handeln, dass wir da zu neuen Formen der Abwägung kommen müssen. Die heutige Methodik im Datenschutzrecht, erst einmal alles verbieten und einen Erlaubnisvorbehalt vorsehen, passt hierfür nicht mehr. Wenn informationstechnisches Äußern, Entäußern usw. der Normalfall ist, kann das nicht rechtlich abgebildet werden in einem Verbot mit Erlaubnisvorbehalten, sondern man muss eine neue Konstruktion finden.

Herr Konietzka:
Ich möchte dem jetzt Gesagten heftig widersprechen und zwar in der Hinsicht, dass wir schon in unserem Lebenslauf eine Menge Datenerfasser um uns herum haben. Zum Beispiel kennt unser Arzt unsere Krankengeschichte, es ist aber verboten, dass er sie veröffentlicht. Wenn ich mit der Polizei oder dem Gericht zu tun habe, ist ebenfalls eine Datenerfassung passiert und ich kann darauf hoffen oder bin sicher, dass es nicht veröffentlicht wird. Wenn ich im Krankenhaus war, ist die Krankenhausakte auch geheim. Oder wenn ich bei Ämtern oder Behörden bin, ist es genau das Gleiche, meine Daten werden erfasst, sie bleiben da und werden in einer Weise genutzt, wie das der Fall ist. Ich denke einmal, dass dieses traditionelle, analoge klassische Datenmodell, das ich darstelle ein Vorbild ist. Und ich bin damit einverstanden, wenn der Arzt, das Gericht oder der Arbeitgeber es nicht weitergibt, was für ein guter oder weniger guter Mensch ich bin. Wenn wir jetzt in der modernen Medienwelt die Möglichkeit haben, dass alles offen ist, dass die Schleusen gewissermaßen geöffnet werden, dann sind wir damit ja nicht mitgewachsen, sondern werden hineingezogen. Der Punkt ist jetzt, dass sich an diesem Datenmodell, das wir in klassischer Weise schon immer haben, das Internetrecht schleunigst orientieren sollte. Das ist die Auffassung, die ich jetzt habe und das ist das Modell, das man eigentlich diskutieren sollte gegen die Piraten und Ähnliche.

Prof. Eckert:
Herr Klumpp ist der Nächste.

Dr. Klumpp:
Die Eigentums- und Besitzfrage, das wissen Sie seit 1977, Herr Sieber, kann man fachlich objektiv nicht in der Öffentlichkeit diskutieren. Der Unterschied zwischen Eigentum und Besitz ist, dass ich sehr wohl Daten in einem Tresor lagern kann. Dann sind diese in meinem Besitz. Ansonsten gilt für Daten, Information und speziell das Wissen, dass es dieses nicht

„gebraucht“ gibt. Oder weiß jemand, ob es irgendwo „gebrauchtes Wissen“ zu verkaufen gibt? Ich wollte mich auf einen anderen Punkt im Podiumsgespräch beziehen, in dem wir im Leitbild alle zusammen weltweit völlig falsch gelaufen sind: Nämlich, dass wir gesagt haben, mit den neuen Techniken muss der Benutzer „medienkompetent“ fertig werden. Das sei auch die Verantwortung des Staates und der Gesellschaft. Ich nehme mich da nicht aus, denn ich habe als Anwendungspionier mit am lautesten geschrien, dass eigentlich alle als Pflicht einen Computerführerschein machen müssen. Nehmen wir den Fall hier im Saal. Da oben ist die Sprinkleranlage, die für den Fall, dass hier Feuer ausbricht, Wasser sprüht und einen Brand löscht. Warum machen wir eigentlich so etwas? Wir könnten doch alle in Fortbildungskursen lernen, dass gar kein Feuer entsteht, wenn man nirgendwo Feuer macht oder seinen PC überheizt. Die ganze Sprinkleranlage wäre also unnötig. Niemand würde aber auf diese Idee kommen, sondern sagen, es ist ein Erfordernis, einen Brandschutz insgesamt zu machen. Und jetzt bin ich noch einmal beim Nutzer und beim Nutzerschutz. Wir können tatsächlich vom Nutzer diese Dinge nicht verlangen, dass er überlegt, wo könnte was über mich gespeichert sein und was davon ist kritisch? Das bekommt er nicht zusammen. Wir sprachen vorher in der Pause über ein paar Fälle, in denen Leute plötzlich und nur per Zufall erfahren haben, dass irgendwelche Dinge über sie gespeichert sind. Das kann man nicht verhindern. Das heißt, hier ist der Ansatz. Da muss man einen „Nutzerschutz“, Datenschutz genauso wie Verfügbarkeit und Verbraucherschutz, als gesellschaftliche Aufgabe sehen. Damit will ich nicht sagen, dass nicht Fortbildungskurse im Sinne des Computerführerscheins u. ä. stattfinden sollen, aber auf jeden Fall auf Seiten des Staates und der Gesellschaft ist die Aufgabe, diese Schutzfunktion „Nutzerschutz“ insgesamt zu realisieren. Und daran müssen wir verstärkt arbeiten.

Prof. Eckert:
Vielen Dank, Herr Klumpp. War das jetzt eine Frage oder ein Hinweis?

Dr. Klumpp:
Das kommt auf Herrn Sieber an. Ich setze auch gern ein Fragezeichen dahinter.

Herr Philipeit:
Die Bilderkennung im Internet erlangt zunehmend an Bedeutung. An meinem eigenen Bild sehe ich ein noch höheres Eigentumsrecht als vielleicht an meinem Namen, meiner Straße, meiner Hausnummer. Ändert sich in Bezug auf das eigene Bild auf einem Digitalfoto etwas an Ihrer Aussage zum nahezu nicht vorhandenen Eigentumsrecht an persönlichen Daten, Herr Sieber? Und wenn sich da etwas ändern sollte, d.h. ich habe tatsächlich eine Art Eigentumsrecht an meinem Foto, dann hätten wir vielleicht sogar eine interessante flächendeckende Anwendung für den neuen Personalausweis. Wenn man das koppeln könnte, d.h. immer wenn mein Foto irgendwo erscheint, muss ich informiert werden und der Veröffentlichung zustimmen bzw. widersprechen können. Ich glaube, es wäre ein erster Schritt in die Welt der informationellen Selbstbestimmung im Netz. Die Digitalfotografie hat uns schon einmal einen Durchbruch gegeben bei der Durchdringung des PCs im älteren Semester. Die 60-, 70-Jährigen sind hauptsächlich durch die Digitalfotografie zum PC gekommen. Vielleicht können wir es schaffen, den neuen Personalausweis auch über so ein Instrument wie der Digitalfotografie in die Fläche zu bringen. Die Frage ist: Kann das Eigentum am eigenen Bild im Netz tatsächlich unter rechtlichen Aspekten geschützt werden? Dann könnten wir in die von mir beschriebene Richtungen weiter denken und investieren.

Prof. Sieber:
Mein Ausgangspunkt ist, dass diese Modelle und dieses ganze Denken mit dem Eigentum einfach nicht passen. Die entsprechenden Regeln sind für körperliche Gegenstände entwickelt. An körperlichen Gegenständen bestehen Ausschließlichkeitsrechte und die Übertra-

gung dieser Rechte auf Daten und Informationen ist schwierig. Meine Ausgangspunkt zu Verfügungsrechten an Information ist dabei grundsätzlich die Informationsfreiheit und die Meinungsfreiheit: Informationen müssen grundsätzlich frei sein. Allerdings gibt es – wie gesagt - Gegeninteressen, die dies verhindern.
Dies wird nicht nur an der vorhin von mir angesprochenen Frage nach Eigentumsrechten an personenbezogenen Daten deutlich. Es zeigt sich auch bei den Verfügungsrechten über sonstige Daten. Solche Verfügungsrechte erkennen wir nicht allgemein an, sondern nur in wenigen speziellen Bereichen, wie etwa bei den Patent- und Immaterialgüterrechten. Auch hier passt die Analogie zum Sacheigentum nicht. Das gleiche gilt auch für die jetzt angesprochenen Fotographien: Hier bestehen ebenfalls spezielle Regelungen im Urheberpersönlichkeitsrecht, z.B. das Recht am eigenen Bild, das aber wiederum Ausnahmen hat für Personen der Zeitgeschichte.

Herr Schallbruch:
Vielleicht kann ich da Herrn Sieber einmal beispringen. Was wir eben diskutiert haben, bezog sich auf das Verhältnis zwischen Menschen, die im Internet kommunizieren oder zwischen Ihnen und einem Unternehmen, das eine Dienstleistung anbietet. In dem Bereich, den Sie gerade aufgezählt haben, Krankenhaus, Polizei, Gerichte usw., - also in dem Verhältnis Bürger-Staat – haben wir in Deutschland eine gute Tradition, nämlich das bereichsspezifische Datenschutzrecht, das dort zu einer sehr spezifischen Abwägung kommt, wo auch z.B. sehr viel strengere Regeln im Gesundheitswesen, im Sozialgesetzbuch, im Steuerbereich gelten als beispielsweise bei Standesämtern. Das ist sehr fein austariert, und das wollen wir gern erhalten – unbeschadet aller europäischen Regulierungsüberlegungen, weil wir diese spezifischen datenschutzrechtlichen Abwägungen für vernünftig halten. In diesem Bereich – also dem Verhältnis Bürger zu Staat – passt auch das Verbot mit Erlaubnisvorbehalt. Für diesen Bereich hat das Bundesverfassungsgericht z.T. sehr detaillierte Voraussetzungen festgelegt. Hier wollen wir von der bewährten Systematik nicht abrücken.

Herr Helmbrecht:
Ich möchte die Punkte zusammenbringen und aus einem anderen Blickwinkel betrachten. Wenn wir jetzt, wie Sie sagten, Krankenhaus oder andere Daten betrachten und Sie hatten politisch auch einen Schwenker zur Piratenpartei gemacht, wenn wir über Gesichtserkennung reden, dann ist für mich die Frage: was diskutieren wir im Moment aus welcher Perspektive? Wir haben Herrn Schallbruch, der das aus der Perspektive der Regierung betrachtet. Was will man tun, um den Bürger zu schützen? Was will man weiterentwickeln? Wir haben das hier in Deutschland sehr gut im Griff Aber ich glaube, dass da ein Punkt fehlt. Das ist die gesamtgesellschaftliche Entwicklung aufgrund dieser Technologie. Und da geht es nicht darum, was wir hier in unserem beruflichen Umfeld oder im Generationsumfeld wünschen, sondern was die Gesellschaft macht. Und die Gesellschaft sind die Menschen, die Jugendlichen und die jungen Erwachsenen, die diese Technologie benutzen. Die Frage ist dann schon, wenn ich mir jetzt überlege und dann sage: Ich bin ein Junger und gehe vielleicht anders mit Arztdaten um. Und es sind auch andere dann da, die sagen: Ich bin mir zwar dessen bewusst, aber ich nutze diese Technologie, weil sie neue Geschäftsmodelle schafft. Die Frage ist, wie wir damit umgehen. Ich finde, es ist zu wenig, wenn man nur sagt, dass man da regulierend eingreifen muss und hier und da etwas tun muss, weil wir sonst einfach global davon überrollt werden. Bis zu einer gewissen Grenze können wir das in Deutschland machen. Wir können das juristisch angehen, Normen schaffen. Dann kommen andere Rechtssystem nach dem Case Law Prinzip, machen drei, vier Entscheidungen und es geht links herum. Und dann wollen wir das zusammenbringen. Nehmen Sie ein einfaches Beispiel: Fluggastdatenabkommen Europa - USA. Das können wir gut finden oder nicht. Es läuft so, wie der Mächtigere das vorgibt. Ich wollte einfach ein paar Stichpunkte bringen. Wir müssen uns bewusst werden,

dass in diesem globalen Spiel unsere deutschen Interessen und die Interessen unserer Altersgruppe in Zukunft doch etwas beschränkt sein werden.

Prof. Eckert:
Wir hatten noch eine Wortmeldung dort hinten, bevor wir langsam zum Ende kommen.

Dr. Stögmüller:
Ich bin Rechtsanwalt. Vielleicht darf ich kurz ein, zwei Anmerkungen aus der Praxis machen, weil wir jetzt doch in einen relativ juristischen Bereich abgedriftet sind, nämlich die Frage des Eigentums. In der Praxis ist es mir relativ egal, auf welche Anspruchsgrundlage, um einen juristischen Begriff zu benutzen, ich Ansprüche stütze. Es gibt eine Menge Regelungen, nach denen selbstverständlich auch künftig ein Arzt keine Patientendaten veröffentlichen darf. Es gibt viele Urteile, die sich mit Fragen der Nutzung personenbezogener Daten im Internet, mit Social Media Themen, mit dem Like Button von Facebook usw. befassen. Ich sehe aus der Praxis eher ein Umsetzungsproblem und nicht so sehr ein juristisches Problem darin, dass ich letztendlich, selbst wenn ich einen Titel erwirke, diesen möglicherweise nicht vollstrecken kann, weil ich das entsprechende Unternehmen nicht mehr zu fassen bekomme. Weil es möglicherweise insolvent gegangen ist. Oder weil möglicherweise jemand, der eine Urheberrechtsverletzung begangen hat, sich bei DENIC mit einer Fake-Adresse registriert und wenn ich diese dann überprüfe, feststellen muss, dass sie in Thailand registriert ist und ich dort niemand fassen kann. Ich habe beispielsweise auch selbstverständlich Ansprüche auf Löschung, auf Sperrung personenbezogener Daten. Nur weiß ich bis heute nicht, wie ich einen solchen Anspruch durchsetzen kann, wenn etwa im Rahmen eines Outsourcing-Projektes die Daten in Indien gespeichert sind und ich dort einen Löschungsanspruch geltend machen muss. Dies ist der Ball zurück von der Juristerei, die durchaus findig ist und teilweise mit sehr guten Richtern gute Urteile erwirken kann, an die Praxis: Wie kann ich ein Recht auf Löschen, ein Recht auf Vergessen letztendlich in der Praxis in einem weltweiten Netzwerk technisch umsetzen.

Prof. Eberspächer:
Da es keine weiteren Fragen aus dem Publikum gibt, darf ich die Diskussion abschließen. .

10 Schlusswort

Prof. Dr. Jörg Eberspächer, Technische Universität München

Sehr geehrte Damen und Herren, ich denke, der Umstand, dass die meisten von Ihnen so lange durchgehalten haben und geblieben sind, zeigt, dass es ein spannender Nachmittag war. Ich mache kein langes Schlusswort, sondern zitiere eigentlich nur die Headline unserer Pressemitteilung, die wir heute herausgegeben haben. Die hieß nämlich: „Gemeinsam für ein sicheres Internet“. Das hatten wir uns auch für diese Konferenz vorgenommen, dieses „Gemeinsam“ in mehrfacher Hinsicht umzusetzen. Wir hatten hier sehr unterschiedliche Experten und Teilnehmer dabei von Technikern über Ökonomen zu Juristen, und sie kamen aus verschiedenen Wirtschaftsbereichen. Letztlich ist das ja ein Thema, das wir nur gemeinsam lösen können oder zumindest einer Lösung näher bringen können. Und ich glaube, das hat der heutige Tag gezeigt.

Sämtliche Grafiken und Bilder der Impulsvorträge und der Vorträge von heute Morgen werden im Internet auf der Homepage des Münchner Kreises zu sehen sein. Dazu auch die Zusammenfassungen der Berichterstatter, für die ich ganz herzlich danke. Und schließlich gibt es auch noch über diese abschließende Runde eine stichwortartige Zusammenfassung, die freundlicherweise Herr Hoffmann vom FhG AISEC zusammengestellt hat.

Ich danke vor allem den Referenten von heute Morgen und heute Nachmittag. Wir hatten es wieder einmal eine Veranstaltung mit drei Tracks gewagt. Das ist nicht immer so einfach, weil doch alle oft an allem interessiert sind und auch heute die Querbezüge sichtbar waren. Trotzdem, glaube ich, war es gut, sich zu konzentrieren in den drei Workshops. Ich danke den Hauptorganisatoren, Herrn Thielmann und Frau Eckert, die ja langjährige Erfahrung mit diesem Thema haben.

Noch einmal Dank herzlichen an alle, auch an unsere Geschäftsstelle für die Arbeit im Hintergrund! Ich wünsche Ihnen eine gute Heimfahrt und auf Wiedersehen.

Liste der Referenten und Moderatoren

Prof. Dr.-Ing. Jörg Eberspächer
Technische Universität München
Lehrstuhl für Kommunikationsnetze
Arcisstr. 21
80333 München
joerg.eberspaecher@tum.de

Prof. Dr. Claudia Eckert
Institutsleiterin
Fraunhofer Institut AISEC
Parkring 4
85748 Garching
claudia.eckert@aisec.fraunhofer.de

Jens Fromm
Gruppenleiter Elektron. Identitäten
Fraunhofer Institut FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin
jens.fromm@fokus.fraunhofer.de

Dr. Laura Georg
Head Security, IT Efficiency &
IT Compliance
Detecon AG
Löwenstr. 1
8001 Zürich
SCHWEIZ
Laura.Georg@detecon.com

Alexander Geschonneck
Partner
KPMG AG Wirtschaftsprüfungsgesellschaft
Risk Consulting – Forensic
Klingelhöferstr. 18
10785 Berlin
ageschonneck@kpmg.com

Dr. Kai Grassie
CTO
Giesecke & Devrient GmbH
Prinzregentenstraße 159
81677 München
kai.grassie@gi-de.com

Prof. Dr. Udo Helmbrecht
Executive Director
European Network and Information Security
Agency ENISA
P.O. Box 1309
71001 Heraklion – Kreta
GRIECHENLAND
Udo.Helmbrecht@enisa.europa.eu

Tom Köhler
Head of Public Sector Germany
EMC Deutschland GmbH/RSA
Osterfeldstr. 84
85737 Ismaning
thomas.koehler@rsa.com

Volkmar Lotz
Head, SAP Research Security & Trust
SAP Labs France
805 Avenue du Dr. Maurice Donat, BP1216
06254 Mougins Cedex
FRANKREICH
volkmar.lotz@sap.com

Dipl.-Wirtsch.-Ing. Lutz Neugebauer
BITKOM e.V.
Bereichsleiter Sicherheit
Albrechtstr. 10 A
10117 Berlin
l.neugebauer@bitkom.org

Prof. Dr. Dres. h.c. Arnold Picot
Ludwig-Maximilians-Universität
Institut für Information, Organisation
und Management
Ludwigstr. 28
80539 München
picot@lmu.de

Marco Preuß
Kaspersky Labs GmbH
Head of GReAT Germany
Global Research and Analysis Team
Despag-Str. 3
85055 Ingolstadt
marco.preuss@kaspersky.com

Prof. Dr. Kai Rannenberg
Goethe-Universität Frankfurt
Deutsche Telekom Chair of Mobile
Business & Multilateral Security
RuW 2.256
Grüneburgplatz 1
60323 Frankfurt
Kai.Rannenberg@m-chair.net

MinR Andreas Reisen
Bundesministerium des Innern
Leiter Referat IT 4
Alt-Moabit 101 d
10559 Berlin
Andreas.Reisen@bmi.bund.de

MinDir Martin Schallbruch
Bundesministerium des Innern
IT-Direktor und CIO
Alt-Moabit 101 d
10559 Berlin
Martin.Schallbruch@bmi.bund.de

Rechtsanwältin Barbara Scheben
KPMG AG Wirtschaftsprüfungsgesellschaft
Am Flughafen /THE SQUAIRE
60549 Frankfurt
bscheben@kpmg.com

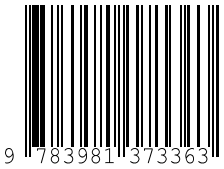
Thorsten Schneider
Global Head of Security Business
Nokia Siemens Networks GmbH
Global Services
St.-Martin Str. 76
81541 München
Thorsten.Schneider@nsn.com

Prof. Dr. Jörg Schwenk
Ruhr-Universität Bochum
Lehrstuhl für Netz- und Datensicherheit
Universitätsstr. 150
44780 Bochum
joerg.schwenk@rub.de

Prof. Dr. Dr. h.c. mult. Ulrich Sieber
Direktor
Max-Planck-Institut f. ausländisches
und intern. Strafrecht
Günterstalstr. 73
79100 Freiburg
u.sieber@mpicc.de

Prof. Dr.-Ing. Heinz Thielmann
Geschäftsführer
Emphasys GmbH
Eichenstr. 11
90562 Heroldsberg
heinz.thielmann@t-online.de

Dipl.-Math. Klaus-Dieter Wolfenstetter
Projektfeldleiter
Deutsche Telekom AG
Products & Innovation
T-Online-Allee 1
64295 Darmstadt
k.wolfenstetter@telekom.de



ISBN 978-3-9813733-6-3