Deutscher Bundestag
17. Wahlperiode

Protokoll Nr. 17/25

Unterausschuss Neue Medien (22)
Wortprotokoll*
25. Sitzung

Berlin, den 15.10.2012, 13:00 Uhr
Sitzungsort: Paul-Löbe-Haus
Konrad-Adenauer-Straße 1
10557 Berlin
Sitzungssaal: E 800

Vorsitz: Sebastian Blumenthal, MdB

TAGESORDNUNG:

Öffentliches Gespräch mit Sachverständigen zum Thema "IT-Sicherheit in der Wirtschaft"

Experten:

Klemens Gutmann, Deutscher Industrie- und Handelskammertag e. V. (DIHK)
Marco Junk, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM)
Andreas Könen, Bundesamt für Sicherheit in der Informationstechnik (BSI)
Andy Müller-Maguhn, Chaos Computer Club (CCC)

*Redaktionell überarbeitete Abschrift der Tonaufzeichnung

Anwesenheitsliste*

Mitglieder des Ausschusses

Ordentliche Mitglieder des Ausschusses	Stellvertretende Mitglieder des Ausschusses
CDU/CSU	
Brandl, Dr. Reinhard	
Jarzombek, Thomas	
Wanderwitz, Marco	
SPD	
Dörmann, Martin	
Klingbeil, Lars	
FDP	
Blumenthal, Sebastian	Daub, Helga
DIE LINKE.	
Behrens, Herbert	
Sitte, Petra, Dr.	
BÜNDNIS 90/DIE GRÜNEN	
Rößner, Tabea	.

*) Der Urschrift des Protokolls ist die Liste der Unterschriften beigefügt.

Bundesregierung	
Husch	BMWi
Kujawa	BMWi
Schuldt	BMWi
Mantz	BMMI

Fraktionen und Gruppen	
Morschhäuser	B90/GRÜNE
Kollbeck	SPD
Leberl	CDU/CSU
Göllnitz	FDP
Dunker	CDU/CSU

Der Vorsitzende: Ich bitte die Kolleginnen und Kollegen sowie die Sachverständigen die Plätze einzunehmen, damit wir mit der Sitzung beginnen können. Ich bitte die Vertreter der Ministerien, hier vorn Platz zu nehmen. Damit eröffne ich die Sitzung des Unterausschusses Neue Medien. Wir diskutieren heute ein Schwerpunktthema im Rahmen eines öffentlichen Expertengesprächs: Die IT-Sicherheit in der Wirtschaft. Dazu haben wir vier Sachverständige eingeladen, ferner sind die beiden Ministerien auf Ebene der Bundesregierrung eingeladen worden, die fachlich mit dem Thema befasst sind.

Zunächst möchte ich den Ablauf der heutigen Sitzung im Unterausschuss kurz erläutern. Wir haben uns ein Zeitfenster von insgesamt zwei Stunden vorgenommen, beginnen mit den Eingangsstatements der Sachverständigen und bieten dann der Vertreterin und dem Vertreter der beiden Ministerien die Möglichkeit, aus Sicht der Bundesregierung zu ergänzen. Daran anschließend ist vorgesehen, in Fragerunden einzutreten. Die heutige Sitzung findet, wie fast alle Expertengespräche hier im Unterausschuss, wieder öffentlich statt. Es gibt einen Livestream, der auf www.bundestag.de abrufbar ist. Nach der Sitzung wird es ein redaktionell überarbeitetes Wortprotokoll geben, das Ihnen als Sachverständige im Entwurf zugeleitet wird, so dass Sie Gelegenheit haben, es freizugeben, damit es danach als Dokumentation der heutigen Sitzung ebenfalls auf der Bundestagshomepage öffentlich gemacht werden kann. Soweit zur Vorrede.

Eingeladen haben wir zum heutigen Thema Herrn Klemens Gutmann vom Deutschen Industrie- und Handelskammertag, DIHK, Herrn Lutz Neugebauer an Stelle des ursprünglich angekündigten Herrn Marco Junk vom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Bitkom. Wir haben vom Bundesamt für die Sicherheit in der Informationstechnik, BSI, Herrn Andreas Könen hier bei uns und vom Chaos Computer Club, CCC, Herrn Andy Müller-Maguhn. Sie alle heiße ich zunächst ganz herzlich willkommen. Sie sind heute unsere Sachverständigen und wir freuen uns auf das Gespräch mit Ihnen.

Wir haben von Seiten der Bundesregierung zum einen bei uns Frau Gertrud Husch, Leiterin des Referats für IT-Sicherheit im Bundesministerium für Wirtschaft und Technologie, und zum anderen vom Bundesministerium des Innern Herrn Dr. Mantz, ebenfalls Leiter eines Referats für IT-Sicherheit. Herzlich willkommen.

Da Ihre jeweilige Institution bzw. der Verband diesem Kreis hinreichend bekannt sein dürften, schlage ich vor, auf die Darstellung der Institutionen und Verbände zu verzichten und das Thema unmittelbar anzugehen. Noch einmal zum Hintergrund: Warum haben wir das Thema IT-Sicherheit heute auf die Tagesordnung gesetzt? Angriffe aus dem Cyberraum waren in den letzten Jahren zwar oft Gegenstand der sicherheitspolitischen Diskussion, aber eher unter dem Stichwort Cyberattacken mit dem Fokus auf Verteidigung und Sicherheitspolitik. Wir wissen aber, dass die Zunahme von Cyberattacken im Bereich der Privatwirtschaft ebenfalls ein Thema ist, welches inzwischen die verschiedensten Akteure beschäftigt. Letztes und jüngstes Beispiel waren Aktivitäten der sogenannten Elderwood Gruppe. Es war festzustellen, dass die Anzahl der Angriffe auf kritische Infrastrukturen auch im Bereich der Wirtschaft

signifikant zugenommen hat. Lücken in IT-Systemen und der Software sind verstärkt das Ziel kritischer Angriffe, die oftmals stattfinden, bevor Anbieter und Programmierer von Sicherheitssoftware die Sicherheitslücken überhaupt schließen können. Gute Gründe also, sich auch im parlamentarischen Raum darüber auszutauschen, was im Bereich unterhalb gesetzlicher Maßnahmen bereits gut funktioniert, also beispielsweise die Kooperation der Handelskammer mit der Wirtschaft bzw. die Unterstützung durch das BSI. Gibt es vielleicht weiteren Handlungsbedarf für die Politik? Das sind die Rahmenthemen, mit denen wir uns heute beschäftigen wollen, und das war auch der Anlass, weshalb der Unterausschuss Neue Medien mit Ihnen ins Gespräch kommen wollte.

Wir fangen nun mit den Statements an und gehen dabei in alphabetischer Reihenfolge vor, so dass Herr Gutmann als Erster an der Reihe ist . Herr Gutmann, bitte, Sie haben das Wort.

Klemens Gutmann (Deutscher Industrie- und Handelskammertag e. V.): Herzlichen Dank für die Einladung. Ich bin im Hauptberuf Unternehmer, SAP-Dienstleister, gehöre also zur tätigen Truppe und zu den Betroffenen. Im Nebenberuf bin ich noch Arbeitgeberpräsident in Sachsen-Anhalt und möchte insofern ein Stück weit die wirtschaftlich-industrielle Provinz hier zu Wort kommen lassen. Mein Weltbild ist vermutlich, wenn ich die Fragen richtig verstanden habe, ein bisschen anders als das Ihre.

Ich möchte dieses Weltbild kurz skizzieren, damit Sie danach einhaken können. Ich habe ein 90–9–1 Weltbild, das ergibt zusammen 100 Prozent. 90 Prozent aller Unternehmen, 90 Prozent aller Akteure, die wir mit dieser kommunikativen Bewusstseinsarbeit ansprechen wollen, arbeiten in ganz normalen Unternehmen, und da läuft auf der IT-Schiene das, was vor 20 Jahren der Warenbegleitschein, die Leistungsbeschreibung oder die Rechnung waren. Das heißt, bei diesen 90 Prozent hat der Einsatz von IT im Kern Dinge automatisiert, beschleunigt und vieles erleichtert. Das ist zwar alles wunderbar, aber im Kern läuft nichts anderes, vor allem nicht im Bewusstsein der Unternehmer, so dass ein jeder Tag immer voller Risiko ist. Morgens schicke ich zum Beispiel einen Lkw raus, und ob der jetzt aufgrund eines fehlerhaften Dispatchings auf der IT-Schiene falsch läuft oder weil der Fahrer Fehler macht, wie vor 20 Jahren schon bzw. heute noch, das ist völlig einerlei. Ein Unternehmer in diesen 90 Prozent lebt mit einem alltäglichen Sammelsurium an Risiken, und das IT-Risiko ist eines davon. Es werden ihm allerdings auch sehr viele Lösungen in allen möglichen Bereichen angeboten, und er reagiert dort typischerweise sehr dickhäutig. Das ist einfach die gefühlte Realität der 90 Prozent. Dann gibt es neun Prozent, also eine deutlich kleinere Zahl, ein Zehntel der Akteure, aber immer noch ein relevanter Teil, auch in der Provinz, wo das Geschäftsmodell in nennenswertem Maße auf dem Einsatz von IT-basiert. Überall, wo kritische Information verdichtet wird, um die Produktion und die Dienstleistung überhaupt möglich zu machen, spielt IT eine nicht mehr wegzudenkende Rolle. Ein Beispiel hierfür sind Web-Shops. Ich bin im Grunde genommen als SAP-Dienstleister mit relativ wenig Web-Verkehr ein Vertreter dieser zweiten Gruppe.

Das eine noch fehlende Prozent sind Unternehmen, die auch in Ihrem Fragenkatalog durchklingen, bei denen die IT der eigentliche Unternehmenswert ist. Jedes dieser Unternehmen ist zu nahezu 100

Prozent Rechenzentrumdienstleister. Das sind Technologieunternehmen, wo der zentrale Wert in der IT vorgehalten wird, mithin Technologiekonzerne. Das ist ein Prozent – jetzt nicht der Wirtschaft, des wirtschaftlichen Gewichtes, sondern ein Prozent der Akteure, die wir adressieren, wenn wir Überzeugungsarbeit betreiben wollen, oder das BMI, wenn es denn jemals ein Gesetz machen will. Diese Realität bitte ich zu berücksichtigen und vor allem, keine volkswirtschaftliche Metrik zu betreiben, keine Wissenschaft. Ich glaube nicht, dass die Unternehmensgröße oder andere wissenschaftlich messbaren Kriterien greifen. In den 1990er Jahren habe ich am Frauenhofer ISI gearbeitet und mich an solchen Kriterien abgearbeitet. Heute bin ich auf der Seite der Unternehmer gelandet und habe zirka 2.000 Mitarbeiterinnen und Mitarbeiter. Sehen Sie das Thema als Ganzes bitte als Projekt der Bewusstseinsarbeit, der Produkte und der Lösungen an, die es zu begreifen gilt, und nicht als ein gesetzgeberisches.

Der Vorsitzende: Vielen Dank, Herr Gutmann. Wir fahren fort mit Herrn Könen.

Ltd. RD Andreas Könen (Bundesamt für die Sicherheit in der Informationstechnik): Einen schönen guten Tag, meine Damen und Herren. Ich möchte Ihnen ganz kurz ein Statement des BSI nahebringen, das eine gewisse Brücke über all die Fragen schlägt, die Sie gestellt haben. Aus Sicht des BSI gibt es im Wesentlichen drei große Felder der Zusammenarbeit mit der Wirtschaft und insbesondere den kritischen Infrastrukturen . Das Erste ist zunächst, gemeinsam ein Lagebild der Gefährdungen zu zeichnen, die uns allen im Moment in der IT und speziell in Netzen drohen. Die Erkenntnis der vergangenen fünf Jahre geht da hin, dass Angriffe in ihrer Zahl zunehmen und stärker in die IT-Infrastruktur von Unternehmen, Behörden und in den privaten Bereich eindringen. Die Angriffe werden zudem auch immer spezifischer. Wir stellen Angriffe fest, die auf breiter Front vorgetragen werden und die Nutzung von IT verhindern, stellen aber auch Angriffe fest, die als Spionageangriffe sehr detailliert auf geheim zu haltende, schützenswerte Güter von Unternehmen und Behörden zielen. Und nicht zuletzt gibt es mit Blick auf die kritischen Infrastrukturen auch Schadprogramme und Angriffe, die vermehrt die Sorge aufkommen lassen, dass auch die Funktionsfähigkeit dieser kritischen Infrastrukturen in den nächsten Jahren mehr und mehr in Frage stehen wird.

Aus diesem Grunde ist es unerlässlich, dass wir uns zunächst einmal gemeinsam ein Bild von der Lage machen. Daher plädieren wir dafür, alle Schadvorfälle, die in der Wirtschaft und den Behörden bekannt werden, zentral an uns weiterzuleiten. Wir haben hier gemeinsam mit den Verbänden der Wirtschaft und insbesondere dem Bitkom in der Allianz für Cybersicherheit ein Angebot formuliert, das wir in wenigen Tagen noch einmal auf einer IT-Fachmesse in Nürnberg vorstellen und bewerben werden. Wir plädieren dafür, die Informationen an einer Stelle zusammenzuführen, die diese dann zunächst zentral nutzen soll, um sie dann wiederum allen Akteuren zur Verfügung zu stellen und durch die Kommunikation der Schwachstellen und der Möglichkeiten, gegen diese vorzugehen, allen Akteuren einen Dienst zu erweisen.

Die zweite Kategorie, das zu tun, sind die verschiedenen Kommunikationsangebote des BSI. Da ist auf der einen Seite das Computer Emergency Response Team, Cert, als zentraler Annahmepunkt zu nennen, dann das Cyberabwehrzentrum als Informationsdrehscheibe für die Behörden, und die zuvor erwähnte Allianz für Cybersicherheit gemeinsam mit der Wirtschaft, insbesondere den Vertretern der kleinen und mittleren Unternehmen.

Die nächste Ebene, auf der wir zusammenarbeiten müssen, das ist die eigentliche Ebene der Cybersicherheit, des Schutzes von Informationen von hochwichtigen Gütern, etwa des Wissens in unserer hochspezialisierten und versierten Wirtschaft. Hier ist es ganz entscheidend, dass für 80 Prozent der Unternehmen schon ein Grundschutz völlig ausreicht. Damit ist die sichere Konfiguration der IT gemeint, die von den Unternehmen unmittelbar eingekauft wird. Wenn die an allen Stellen so optimal gemacht würde, wie es allein schon aus dem Angebot der verschiedenen Hardware- und Softwareprodukte heraus möglich wäre, dann wäre damit schon ein gewaltiger Schritt nach vorne getan.

Der nächste Schritt wäre, die Angebote des BSI, die schon immer auf die gesamte Informationssicherheit gerichtet waren, in geeigneter Form für kleine und mittlere Unternehmen und für die ohnehin versierten kritischen Infrastrukturen bereitzustellen. Das, was wir über Jahrzehnte für Behörden bereits geleistet haben, ist hier auch noch einmal in einem Multiplikatorenrahmen – der Cyberallianz – nutzbar zu machen. Die Angebote kennen Sie, das sind insbesondere auch Angebote, die von der deutschen Informationsicherheitsindustrie bereitgestellt werden: Dienstleistungen im Bereich der Informationssicherheit, Software- bzw. Hardwareprodukte.

Der Vorsitzende: Vielen Dank, Herr Könen. Wir fahren fort mit Herrn Müller-Maguhn.

Andy Müller-Maguhn (Chaos Computer Club): Das Thema Sicherheit hat zunächst einmal von der Wahrnehmung her Defizite, weil das Unternehmensinteresse in der Regel darauf abzielt, den Anschein der Sicherheit zu wahren. Andersherum formuliert: Die Bereitschaft von Unternehmen, offen über Sicherheitsprobleme zu reden, das muss man einfach konstatieren, ist für gewöhnlich nicht vorhanden. Der Anschein der Sicherheit und die Reputation eines Unternehmens – auch und gerade in Bezug auf die vorgehaltenen IT-Strukturen – sind oftmals – auch finanziell – mehr wert, als die Offenlegung von Schwachstellen und der Umgang mit ihnen. Das heißt, die Rahmenbedingungen brechen sich natürlich auch herunter auf den einzelnen Mitarbeiter im Unternehmen, der mit der Angelegenheit zu tun hat. Es ist weder modern noch der Karriere zuträglich, über Unzulänglichkeiten bei der Beherrschung der IT allzu offen und vor allen Dingen gegenüber Vorgesetzten zu reden.

Das ist, vorangestellt aus meiner Sicht, eines der Kernprobleme, das erschwerend hinzukommt, wenn man ein realistisches Bild von IT-Sicherheit erhalten möchte, sei es durch Meldepflichten, durch Umfragen oder welche Maßnahmen auch immer. Sicherheit ist, wenn überhaupt, ein Prozess, der kompetente Beteiligte voraussetzt, die Erfahrung haben, die auch zumindest in einem gewissen Rahmen offen miteinander über Ereignisse reden, sich austauschen und vielleicht auch auf externes Fachwissen

zurückgreifen. Die Darstellung, wie sie jetzt in den bisherigen Statements zur Beleuchtung der Lage zum Vorschein kam, Zero Days, Cyberangriffe und auch einzelne Beispiele, sind oftmals lediglich Momentaufnahmen, die nicht geeignet sind, den tatsächlichen Status des Prozesses, wir sagen, die Reife der Unternehmen, sich bestimmten Situationen zu stellen, zu beleuchten.

Für uns gibt es IT-Sicherheit eigentlich nicht, sondern sie ist eine Illusion. Die heute eingesetzten Technologien weisen in der Regel eine sehr hohe Komplexität auf, die nun zunehmend die Infrastruktur in allen möglichen Bereichen prägt. Die Immunität dieser Infrastrukturen gegenüber Problemen, was nicht nur technische Maßnahmen einschließt, sondern auch prozessuale Maßnahmen in den Geschäftsmodellen, in den Haftungsregelungen usw., nimmt eine wichtige Stellung ein. Es stellt sich die Frage, ob die Unternehmen so realistisch sind, die getroffenen Prozesse kritisch zu hinterfragen im Hinblick darauf, dass die eingesetzte Technik, auch Sicherheitstechnik, möglicherweise versagen kann. Es ginge dann um die Beweislast der Kunden, die Begrenzung des Prozesses im Hinblick auf einen ggf. eintretenden Schaden und Ähnliches. Natürlich soll man das Risiko möglichst eingrenzen, aber Schadenseingrenzung für den Fall, dass das Risiko eintritt, ist ebenfalls angebracht. Man kann hier getrost Vergleiche zu anderen Branchen ziehen. Natürlich ist es richtig, dass es IT-nahen Branchen leichter fällt, ihre Technik und ihre möglichen Probleme einzuschätzen und andere Branchen sich möglicherweise blenden lassen von Momentaufnahmen, Hersteller- und auch Dienstleisterversprechen. Der Begriff Restrisiko hat beispielsweise im Zusammenhang mit dem Betrieb von Kernkraftwerken eine völlig andere Bedeutung als andernorts. In der IT meint man, wenn man von Restrisiko spricht, die Wahrscheinlichkeit, eine evtl. Störung eingrenzen zu können.

Wir bleiben also skeptisch, ob eine Meldepflicht oder vergleichbare Maßnahmen tatsächlich hilfreich sind, um hier zu einem realistischen Bild zu kommen. Der Anspruch, sich erst einmal ein Lagebild, sinnvollerweise ein aktuelles, zu machen, scheint mir ein hehres Ziel zu sein. Die Frage ist, wie man die Unternehmen ermutigen und dazu bringen kann, hierzu etwas beizutragen. Das wird nur gehen, wenn man im Gegenzug auch Hilfestellungen anbieten kann. Ein rein nationales Lagebild ist im Kontext des Internets auch in Bezug auf die Klassifizierung von Angriffen kein sinnvoller Ansatz, insofern als Angriffe in der Regel vernetzt und grenzübergreifend stattfinden. Das heißt, wir glauben, dass vor der Erörterung von Maßnahmen erst einmal eine Diskussion hinsichtlich der Unterscheidung von Angriffen stattfinden muss in Bezug auf ihre Intention, in Bezug auf Verantwortlichkeiten, in Bezug auf Haftungsfragen und in Bezug auf die Auswirkung auf Geschäftsprozesse.

Ein weiteres Thema ist die Kriegführung im Hinblick auf Informationen, auch Instrumentalisierung genannt. Dabei geht es um Angriffe aus anderen Ländern, auf die man zwar entsprechend reagiert und ggf. antwortet, wohlwissend, dass die Identifizierung eines Angreifers im Internet keine valide Sache ist. Angriffe unter falscher Flagge, d. h. unter Legendierung der Identität sind eigentlich Standard und nicht die Ausnahme. Hier müsste erst einmal eine versachlichte Diskussion über die sehr unterschiedlichen Angriffe stattfinden, um Maßnahmen abzustimmen und zu einem Lagebild zu gelangen. Das erst einmal zur Einführung.

Der Vorsitzende: Für den Impuls vielen Dank, Herr Müller-Maguhn. Wir fahren fort mit Herrn Neugebauer für den BITKOM.

Lutz Neugebauer (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.): Vielen Dank, Herr Vorsitzender. Guten Tag, meine Damen und Herren. Ich denke, das Thema Informationssicherheit muss in einer versachlichten Diskussion, da würde ich meinem Vorredner zustimmen, auch im politischen Umfeld ankommen. Deshalb freue ich mich sehr, dass wir heute die Gelegenheit haben, in einer hoffentlich sachlichen Diskussion darüber zu sprechen. Für uns ist das Thema Informationssicherheit ein äußerst wichtiges Thema. Unsere Kunden sind von Cyberbedrohungen betroffen, und wir selbst als Netzbetreiber stehen auch im Fokus der Angreifer. Deshalb ist es für uns essenziell, Schutzmaßnahmen zu kreieren, aber auch entsprechend an Schutzmaßnahmen gegen Cyberbedrohung aktiv mitzuwirken, diese zu gestalten und unsere Produkt- und Dienstleistung auch in puncto Sicherheit permanent weiterzuentwickeln. Dazu sehen wir insbesondere auch die Forschungs- und Entwicklungsvorhaben im Bereich der IT-Sicherheit als ganz wesentlich an. Das heißt, die IT-Sicherheitsforschung, die gerade in Deutschland recht stark ist, wollen wir voranbringen.

Neben dem technischen Schutz – einer Studie zufolge, die wir gemacht haben, sind 95 Prozent der KMUs durchaus mit Virenscannern und einer Firewall ausgestattet – fehlt es häufig an organisatorischen Maßnahmen, der Achtsamkeit der Mitarbeiter und entsprechenden Sensibilisierung. Wenn Unternehmen auf einen Basisschutz setzen, heißt das noch lange nicht, dass sie damit sicher sind. Insofern sollten Unternehmen aufpassen, sich nicht in eine Scheinsicherheit hinein zu manövrieren. Ein rein technischer Schutz wird dann unwirksam, wenn die Sicherheitssysteme nicht auf dem neuesten Stand sind, wenn sie schlecht konfiguriert sind oder Angreifer die Mitarbeiter direkt ansprechen und über diesen Umweg letztlich den Weg in die Unternehmen finden.

Die Mehrheit der Unternehmen ist sich durchaus bewusst, dass Bedrohungen im Cyberraum existieren. Wir haben eine Studie durchgeführt und in Erfahrung bringen können, dass 57 Prozent der Unternehmen davon wissen und knapp 40 Prozent schon einmal Erfahrung mit Cyberangriffen gemacht haben, viele Unternehmen sogar mehrfach. Die Konsequenz, die daraus erwächst, ernüchtert einen dann aber doch leider wieder sehr stark. Nicht einmal die Hälfte der befragten Unternehmen verfügt über einen Notfallplan, wenn etwas passieren sollte, um beispielsweise Daten wieder einzuspielen, um zu sehen, wer zu welchem Zweck zu informieren ist, damit Strafverfolgungsbehörden aktiv werden können. Ich habe den Eindruck, da müssen wir noch eine ganze Menge tun.

Mein Verband engagiert sich seit Jahren in Initiativen zur Sensibilisierung und Unterstützung von Unternehmen. Wir sind Mitglied der Taskforce „IT-Sicherheit in der Wirtschaft“, die insbesondere auf kleine und mittlere Unternehmen ausgerichtet ist, und wir sind Gründungsmitglied des Vereins “Deutschland sicher im Netz e.V.“, in dem Privatpersonen und Unternehmen, insbesondere KMUs, letztlich Hilfe finden.

Herr Könen hat es angedeutet, wir haben Anfang des Jahres die Allianz für Cybersicherheit mit dem BSI initiiert, und haben dabei drei besonders wichtige Punkte im Blick. Den Punkt Lagebild stelle ich hinten an, den hat Herr Könen schon ausführlich dargestellt, auch Herr Müller-Maguhn ist darauf eingegangen. Zwei Punkte möchte ich allerdings noch ergänzen. Erstens müssen wir meines Erachtens darauf schauen, dass wir in den Unternehmen die Sicherheitsexpertise steigern, sie darin bestärken und auch inhaltlich unterstützen, IT-Sicherheitsbeauftragte zu benennen, die qualifiziert werden und mit entsprechenden Kompetenzen ausgestattet sind. Denn nur dann sind die Unternehmen auch in der Lage, eine effektive Sicherheitsstrategie zu entwickeln und ein Notfallkonzept. All das ist wichtig und zudem ein individueller Prozess. Man kann bezogen auf einzelne Branchen entsprechende Vorarbeiten leisten, aber jedes Unternehmen muss sich im Grunde genommen selbst damit auseinandersetzen, welche Punkte es für wichtig erachtet, um daraus seine Sicherheitsleitlinie abzuleiten. Die Verantwortung für die Umsetzung kann dem einzelnen Unternehmen niemand abnehmen, aber sollte das hierfür notwendige Personal fehlen, können sich Unternehmen zweifelsohne Unterstützung holen.

Zweitens brauchen wir zwischen den Unternehmen, aber auch zwischen dem Staat und der Wirtschaft, einen verstärkten Informations- und Erfahrungsaustausch. In der täglichen Praxis vernehme ich immer wieder, dass gerade Großunternehmen bereit sind, ihre Erfahrung auch mit kleinen und mittleren Unternehmen zu teilen. Diese Bereitschaft zum Dialog sollte unterstützt werden. Wie kann man das tun? Man sollte jedenfalls meines Erachtens nicht versuchen, kleine und mittlere Unternehmen über eine übergreifende nationale Plattform allein anzusprechen. Vielmehr sollte man, wenn man in einen Dialog treten will, das auch auf regionaler Ebene entsprechend ergänzen. Wir haben heute schon die Industrie- und Handelskammern erwähnt. Diese sind sicherlich eine sehr gute Möglichkeit, um Stammtische auszurichten, um kleinere Veranstaltungen zu machen, wo es dann auch zu einem Dialog im kleinen Kreis kommen kann. Der ist deshalb wichtig, weil das Vertrauen, das man braucht, um Erfahrungen auszutauschen, nicht in großen Konferenzen mit 200 Teilnehmern erreicht werden kann. Dieser Ansatz muss als kontinuierlicher Prozess gestaltet werden, indem man sich regelmäßig zusammensetzt und über das Thema austauscht. Ein Beauftragter für IT-Sicherheit in einem Unternehmen wird sicherlich auch bereit sein, an diesen Veranstaltungen teilzunehmen. Natürlich muss die Unternehmensleitung dem zustimmen und entsprechende zeitlichen Freiräume schaffen.

Das Lagebild ist schließlich noch ein wesentlicher Punkt. Um das bereits Gesagte zusammenzufassen, ist es aus unserer Sicht erforderlich, darauf hinzuarbeiten, den Wirtschaftsstandort Deutschland widerstandsfähig gegen Cyberbedrohungen zu machen. Wir können keine Mauer bauen und uns gegen sämtliche Angriffe komplett schützen, weil immer wieder neue Angriffsmethoden auf den Markt kommen. Wichtig ist deshalb, eine Widerstandsfähigkeit aufzubauen. Das gelingt nur, wenn Unternehmen bereit sind, bei sich selbst Sicherheit umzusetzen, denn nur so kommen wir zu einem sicheren vernetzten Ganzen. Vielen Dank.

Der Vorsitzende: Vielen Dank, Herr Neugebauer, damit haben wir die erste Runde mit den Impulsreferaten der Sachverständigen abgeschlossen. Wir kommen jetzt zur Bundesregierung. Beide

Referatsleiter – aus dem Wirtschaftsministerium und aus dem Innenministerium – hatten darum gebeten, die Aktivitäten, die derzeit jeweils auf administrativer Ebene laufen, darstellen zu dürfen. Frau Husch, ich schlage vor, dass Sie beginnen und wir dann mit Herrn Dr. Mantz fortfahren.

MR´n Gertrud Husch (Bundesministerium für Wirtschaft und Technologie): Ich würde gern die Gelegenheit nutzen, darzustellen, dass IT-Sicherheit auch aus unserer Sicht, aus Sicht des Bundesministeriums für Wirtschaft und Technologie, ein sehr wichtiges Thema ist. Aus diesem Grund hat seinerzeit noch Minister Brüderle die Task Force "IT-Sicherheit in der Wirtschaft" eingerichtet. Dies geschah vor dem Hintergrund, dass wir aus seinerzeit aktuellen Studien entnommen haben, dass es einen Nachholbedarf gibt, insbesondere bei den kleinen und mittleren Unternehmen. Wir haben uns nicht fokussiert auf die Großen, von denen wir glauben, dass sie gut abgedeckt sind, zum einen durch das Eigeninteresse, das sie haben, und durch viele gesetzliche Verpflichtungen, die gerade für Betreiber kritischer Infrastrukturen gelten. Deswegen haben wir uns, wie gesagt, fokussiert auf die KMUs. Dass wir damit ganz richtig liegen, zeigt auch eine aktuelle Studie, die wir gerade vor drei Wochen ins Haus bekommen haben. In einer Befragung von ca. 1.000 kleinen und mittleren Unternehmen hat sich gezeigt, dass wie zu vermuten war natürlich nahezu alle IT-basiert arbeiten, aber auf der anderen Seite auch 93 Prozent mit IT-SicherheitsproblemenErfahrung haben . Gut die Hälfte war Angriffen mit Viren und Trojanern ausgesetzt. Das sind Zahlen, die man nicht ignorieren kann, sondern bei denen wir denken, dass etwas getan werden muss.

Es gibt deshalb die Task Force „IT-Sicherheit“ in unserem Haus, die eng zusammenarbeitet mit Verbänden, mit Wissenschaftlern, mit der Verwaltung und auch mit all den Einrichtungen, deren Vertreter da drüben am Tisch sitzen. In den letzten 1 ½ Jahren habe wir einige Angebote ins Leben gerufen und etliche Initiativen gestartet. Es fängt damit an, dass wir einen kostenlosen IT-Sicherheitsnavigator für die KMUs erstellt haben, bei dem man kostenlos nachschauen kann, wo man Hilfe für bestimmte Probleme erhält. Zusammen mit dem Eco-Verband habe wir einen kostenlosen Webseiten-Check erstellt. Damit kann man seine Homepage auf Schadstellen und Einfallstore hin durchsuchen und die Probleme gegebenenfalls auch beseitigen.

.

Wir fördern demnächst das Angebot an Online-Schulungen und E-Learning und haben neue Wege beschritten, indem wir uns neue Multiplikatoren für das Thema gesucht haben, weil wir uns bewusst geworden sind, dass man Mittelständler vor Ort abholen muss. Deswegen sind wir auf neue Berufsgruppen zugegangen wie Steuerberater, Rechtsanwälte, Notare, Bankfachleute – also solche, die ohnehin schon engen Kontakt zu Mittelständlern haben und die wir für geeignet halten, diesen das Thema nahezubringen.

Was wir jetzt aktuell planen, sind konkrete Angebote für Branchen, also beispielsweise für Handwerker, weil die Studie auch gezeigt hat, dass es da doch noch deutlichen Nachholbedarf gibt. Die Branchen sind zwar alle sehr aktiv im Nutzen innovativer Technologien, aber ihnen sind die Risiken nicht so sehr bewusst. Die Studie hat außerdem gezeigt, dass etwas für die Gesundheitsbranche, die noch

Nachholbedarf hat, ein branchenspezifisches Angebot erforderlich ist, das gemeinsam mit der Wirtschaft zu erarbeiten ist. Wir denken, dass es ein richtiger Weg ist, auf Hilfsangebote zu setzen, die wir zur Verfügung stellen, ohne irgendwelche Meldepflichten einzuführen oder bürokratische Hürden für Mittelständler aufzubauen. Wir wollen hier einen anderen Weg gehen. Vielen Dank.

Der Vorsitzende: Soweit zum Bundesministerium für Wirtschaft und Technologie. Nun für das Bundesministerium des Innern, Herr Dr. Mantz, bitte.

MR Dr. Rainer Mantz (Bundesministerium des Innern): Vielen Dank. Meine Damen und Herren, nur ganz kurz zu den Tätigkeiten des Innenministeriums, insbesondere des IT-Stabs in der zuständigen Abteilung, zum Thema Cyberangriffe, Cyberbedrohung oder IT-Sicherheit ganz allgemein. Die Bundesrepublik Deutschland ist in diesem Bereich, soweit das möglich ist, und ich bitte, diese kleine Einschränkung auch gleich mitzuhören, relativ gut aufgestellt. Wir haben Anfang des Jahres 2011 eine Cybersicherheitsstrategie verabschiedet und sind nun dabei, diese Stück für Stück umzusetzen. Insbesondere haben wir auf Ebene der Staatssekretäre unter Leitung der Bundesbeauftragten für Informationstechnik, Frau Staatssekretärin Rogall-Grothe, einen Cybersicherheitsrat eingerichtet, der sich dieses vielschichtigen Themas annimmt. Und wir haben, das ist schon erwähnt worden, ein Cyberabwehrzentrum eingerichtet, nicht um eine neue Behörde zu gründen und damit den bürokratischen Überbau noch zu vergrößern, sondern um sicherzustellen, dass die existierenden Behörden ihre jeweilige Fachkompetenz in einer Plattform zusammenbringen und wechselseitig befruchtend einsetzen können.

Darüber hinaus hat Bundesminister Dr. Friedrich im Laufe des Sommers mit den Branchen, die für die kritischen Infrastrukturen in der Bundesrepublik Deutschland zuständig sind, Gespräche geführt. Es ging dabei um eine mögliche Cyberbedrohung und die jeweilige Situation. Wir sind gerade dabei, diese Gespräche auszuwerten. Das letzte hat, wenn mich mein Gedächtnis nicht trügt, am 18. September, jedenfalls im September 2012, stattgefunden. Wir werden die Auswertung voraussichtlich Ende dieses Monats abgeschlossen haben. In der Konsequenz geht es darum zu entscheiden, ob in naher Zukunft aus Sicht des Bundesministeriums des Innern gesetzliche Regelungen sinnvoll und erforderlich sind. Es sind hierzu bereits durchaus ernstzunehmende und nachvollziehbare kritische Äußerungen gefallen. Mit einer Meldepflicht ist jedenfalls, und ich glaube, das ist konsensfähig, nicht alles getan.

Und man muss sich in der Tat auch überlegen, ob man da nicht eher eine Scheinsicherheit erzeugt. Aber wie gesagt, das ist noch nicht ganz spruchreif. Unsere Aktivitäten werden international durchaus wahrgenommen. Die Bundesrepublik Deutschland hat – sicherlich nicht allein, es gibt auch andere Nationen, die viel Energie investiert haben – durchaus Gewicht. Wir stehen, denke ich, in einer Reihe mit den USA, Großbritannien und anderen Nationen und stimmen uns international ab. Vielen Dank.

Der Vorsitzende: Vielen Dank, Herr Dr. Mantz. Wir kommen nun zur Fragerunde der Fraktionen und beginnen mit der Fraktion der CDU/CSU. Herr Dr. Brandl hat sich gemeldet, bitte schön.

Abg. Dr. Reinhard Brandl (CDU/CSU): Meine Frage geht an zwei Sachverständige, und zwar an Herrn Gutmann und an Herrn Müller-Maguhn. Wir haben jetzt einiges zur Lagebeschreibung gehört, dass sich insbesondere kleine und mittlere Unternehmen schwer damit tun, entsprechende Sicherheitsvorkehrungen zu ergreifen. Wir haben auch gehört, dass der Vorschlag, der auf dem Tisch liegt, eine Meldeverpflichtung einzuführen, durchaus auch kritisch bzw. nicht als des Rätsels Lösung angesehen wird. Meine Frage an Sie, ganz konkret, lautet, was Sie uns als Gesetzgeber empfehlen. Was können wir tun, um das Thema IT-Sicherheit in der Wirtschaft in Deutschland voranzubringen?

Der Vorsitzende: Soweit die erste Frage. Wir fahren dann fort mit der SPD-Fraktion. Auch hier ist meine Bitte, gezielt darauf hinzuweisen, an wen die Fragen gerichtet sind und diese, wie eben schon vorbildlich gemacht, möglichst konkret zu fassen. Bitte schön, Lars Klingbeil.

Abg. Lars Klingbeil (SPD): Vielen Dank. Der Kollege Brandl hat, glaube ich, sozusagen den Knackpunkt angesprochen. Ich will insofern die Frage nicht wiederholen, aber ich glaube, danach ergeben sich doch noch ein paar andere Nachfragen. Ich will vielleicht einen aktuellen Punkt ansprechen und hätte dazu gern von Herrn Gutmann und Herrn Müller-Maguhn eine Einschätzung. Wir hatten in der letzten Woche eine Berichterstattung über chinesische Technologiekonzerne, über ZTE und Huawei, in der angemerkt wurde, man könne beiden Unternehmen in Bezug auf den Netzausbau nicht wirklich trauen. Der US-amerikanische Geheimdienst und das entsprechende parlamentarische Gremium meldeten sich da auch zu Wort. Vielleicht können Sie dazu einmal eine Einschätzung geben. Welche Rollen spielen diese Konzerne hier in Deutschland und was bedeutet das eigentlich auch für die IT-Sicherheit und für einen evtl. politischen Handlungsbedarf?

Der Vorsitzende: Für die FPD-Fraktion, Helga Daub, bitte.

Abg. Helga Daub (FDP): Noch einmal herzlichen Dank an die Herren und an die Dame für Ihre Ausführungen. Das Thema ist ja in der Tat sehr vielfältig und nicht einfach so vom Tisch zu wischen. Zweifelsohne gibt es natürlich unterschiedliche Unternehmensformen, die mal mehr mal weniger davon betroffen sind. Meine Frage geht an Herrn Müller-Maguhn. Ich meine, aus Ihren Ausführungen herausgehört zu haben, dass Sie vor allen Dingen darauf setzen, die Mitarbeiterinnen und Mitarbeiter in den Unternehmen verstärkt auszubilden. Oftmals sagt man ja etwas salopp: Also, das größte Sicherheitsrisiko sitzt vor dem Bildschirm. Sicher geht es auch darum, entsprechende Geräte zu entwickeln und dann zur Verfügung zu stellen. Gibt es da irgendetwas, damit man das Problem frühzeitig erkennen kann? Iich meine herausgehört zu haben, dass Sie die Meldepflicht in puncto Sicherheit – absolute Sicherheit gibt es nicht, sagten Sie glaube ich – in diesem Fall eher nicht für unbedingt notwendig erachten.

Der Vorsitzende: Für die Fraktion DIE LINKE., Herbert Behrens, bitte.

Abg. Herbert Behrens (DIE LINKE.): Ich möchte an den Sachverständigen Müller-Maguhn zwei Fragen richten. Eine bezieht sie sich auf den sogenannten Hacker-Paragraphen, dass der Besitz und die Verbreitung von Werkzeugen, die zur Aufdeckung von Sicherheitslücken führen können, strafbar gestellt sind. Das wurde seinerzeit vom Chaos Computer Club sehr scharf kritisiert. Nunmehr, nach Ablauf einiger Jahre, könnte Bilanz gezogen werden. Haben sich Ihre Befürchtungen bestätigt, sind entsprechende Dinge eingetreten, die Sie erwartet haben, oder wie müssen wir die aktuelle Situation sehen? Die zweite Frage betrifft die Bemühungen einer Zusammenarbeit zwischen verschiedenen Institutionen, darunter auch staatliche Stellen – das Cyber-Abwehrzentrum wurde eben als Institution bereits erwähnt . Dazu gibt es ja auch die Forderung der Wirtschaft, so etwas zur Verfügung zu stellen bzw. eine Andockstelle einzurichten. Spontan würde ich da erst einmal eine totale Überwachung vermuten und befürchten. Wie sehen Sie die Entwicklung und halten Sie dieses Instrument überhaupt für eine sinnvolle Möglichkeit?

Der Vorsitzende: Für die Fraktion BÜNDNIS 90/DIE GRÜNEN, Tabea Rößner, bitte.

Abg. Tabea Rößner (BÜNDNIS 90/DIE GRÜNEN): Von meiner Seite auch noch einmal ganz herzlichen Dank dafür, dass Sie heute hier sind und uns Rede und Antwort stehen. Ich habe zunächst eine Frage an den Vertreter des Bitkom. Einmal geht es um den Notfallplan, wobei Sie angaben, die meisten Unternehmen hätten keinen. Was schlagen Sie vor, um das zu ändern? Wie kann zügig in die Unternehmen eingespeist werden, dass es wichtig ist, dass es solche Notfallpläne gibt? Sie sagten auch, die Unternehmen müssten das selbst stemmen. Das hieße aber, sie bräuchten Beratung und Know-how, aber auch aktuelle Informationen vor allen Dingen, um reagieren zu können. Also, wie glauben Sie, ist das umsetzbar und welche Aufgabe hat dabei der Staat, wenn überhaupt ? Das, glaube ich, wäre noch einmal wichtig, aufzuklären.

Die andere Frage geht an Herrn Könen vom BSI. Sie erwähnen in Ihrer Stellungnahme auch das Cloud-Computing. Gerade wenn man im Hinblick auf das Angriffsszenario Spionage noch einmal darauf zurückkommt, wie sieht dann hier Ihre konkrete Empfehlung aus? Die Cloud eröffnet ja doch einige Sicherheitslücken, insbesondere wenn man an Szenarien denkt, dass in den USA über den sogenannten FISA Act ein unmittelbarer Zugriff auf Daten von Ausländern und Unternehmen erfolgen soll, die insofern dann keinen Schutz genießen. Wie lautet an dieser Stelle Ihre Empfehlung?

Der Vorsitzende: Soweit zur Fragerunde. Wir machen das in der bewährten Form, Herr Gutmann, dass wir mit Ihnen beginnen. An alle Sachverständigen sind Fragen gerichtet worden, so dass Sie die an Sie gerichteten Fragen einfach in der Beantwortung aufgreifen. Herr Gutmann, Sie haben folglich als Erster das Wort.

Klemens Gutmann (Deutscher Industrie- und Handelskammertag e. V.): Ich beginne mit der wohl am einfachsten zu beantwortenden Frage zu Huawei. Kann man einem chinesischen Routerhersteller trauen? Gestatten Sie mir eine Gegenfrage. Wir wissen, es ist wirklich so gewesen, dass der

amerikanische Geheimdienst versucht hat, auf Microsoft und Cisco Einfluss zu nehmen. Inwieweit ihm das gelungen ist, weiß ich nicht. Mein Wissen in Bezug auf Router endet so um 1996, 1997. Wir können davon ausgehen, dass die Chinesen das ähnlich praktizieren wie ihre US-amerikanischen Kollegen und auch in der einen oder anderen Form an ihre Routerhersteller herantreten, vielleicht sogar noch ein bisschen nachdrücklicher als die US-amerikanischen. Davon muss ich jedenfalls ausgehen, insofern macht es da für mich keinen Unterschied. Ich unterstelle in beiden Fällen die Möglichkeit, dass es Hintertüren gibt.

Als Mittelständler muss ich damit leben, strategisch sensible Daten vorzuhalten. Ich habe keine Patentlösung, und Kollegen in meinem IT-Verband in Sachen-Anhalt haben leider auch keine. Wir müssen folglich mit dem Risiko leben und können es nicht immer verifizieren. Bei großen Netzen unternimmt man stärkere Anstrengungen, indem man gemischte Systeme mit Produkten von verschiedenen Herstellern einsetzt. Aber für uns ist es eine offene Frage, die wir nicht beantworten können. Wir gehen deshalb im Zweifelsfall immer von einer Schwachstelle aus.

Die zweite Frage ging dahin, was wir an Stelle einer einheitlichen Meldepflicht besser machen können. Ich will an dieser Stelle unterstreichen, Herr Müller-Maguhn hat das sehr treffend beschrieben, dass Sicherheit ein Prozess ist und ein Gesetz allein kein geeignetes Mittel darstellt. Ein Gesetz kann unter Umständen begleiten, aber im Kern ist eine gesetzliche Regelung erst einmal kein gutes Instrument, einen gesellschaftlichen Prozess, und es ist ein solcher, in Gang zu setzen. Vielleicht ist es als Begleitmaßnahme geeignet. Sie merken, ich bin da eher skeptisch und würde erst einmal die konventionellen Methoden ausschöpfen wollen. Das ist zum einen, diesen Prozess durch Bewusstseinsarbeit anzugehen.

Sie haben den DIHK angesprochen. Wir sind dazu bereit, denn der DIHK agiert vergleichsweise graswurzelnah und in Ergänzung zu den Fachverbänden kann man da schon eine ganze Menge hinbekommen. Zweitens würde ich vor das Gesetz schalten, dass wir uns gemeinsam überlegen, inwieweit Sicherheitstechniken standardisierbar sind. Frau Husch hat eine Umfrage erwähnt, dass viele, 93 Prozent glaube, ich sagten Sie, Hackerangriffe von sich aus melden. In diesem Zusammenhang würde mich einmal interessieren, und eine solche Frage haben wir in meinem IT-Verband in Sachsen-Anhalt gestellt, wann wir eigentlich den letzten messbaren Schaden durch Angriffe hatten. Es musste erst einmal intensiv überlegt werden, bis dann gesagt wurde, der jüngste sei 2005 gewesen und alles andere vorher, so in den 1990er Jahren, als der Betrieb einen Tag lang still stand. Nimmt man Unternehmen, die wirklich schon 15 Jahre in der jetzigen Größe am Markt präsent sind, so werden Sie, und das ist eigentlich beruhigend, feststellen, dass die wirklich messbaren, signifikanten Schäden dann doch erfreulich lange zurückliegen.

Ich rede jetzt von den IT-affinen Unternehmen. Auch bei denen müssen wir, vermute ich, diese mühsame Zielgruppenbildung, die ich zuvor skizziert habe mit 90–9–1, wahrscheinlich vornehmen. Es kann sein, dass wir bemerken, dass es in anderen Teilen dieser Zielgruppe sehr wohl Schäden gibt. Aber da bitte

ich dann um Differenzierung und würde mir wünschen, dass wir Sicherheitstechnologien für diese Zielgruppen stärker paketieren. Zum Beispiel die mittlere Zielgruppe, die das Thema Intrusionserkennungssysteme fokussiert, da gibt es so etwas noch nicht als paketierbare Lösung. Firewalls sind vorhanden, Signiersysteme und auch Verschlüsselungssysteme sind zu Preisen von 999 bis 9.999 Euro zu haben. Da kann keiner mehr nein sagen, da das ein Stück weit pauschaliert und vereinheitlicht ist. Aber es gibt noch eine Reihe von wirksamen Schutztechnologien, die man paketieren und in die Breite tragen kann. In die von mir erwähnten 9 Prozent sowieso, aber insbesondere in die 90 Prozent. Ich glaube das waren die Punkte, die an mich gerichtet waren.

Abg. Tabea Rößner (BÜNDNIS 90/DIE GRÜNEN): Und was bedeutet das jetzt konkret für uns?

Klemens Gutmann (Deutscher Industrie- und Handelskammertag e. V.): Zumindest sollten Sie mit einem Meldegesetz warten. Ich kenne das Vorhaben noch nicht im Einzelnen, aber ich habe davon gehört. In einem der beratenden Gremien der Bundesregierung, an dem ich einmal teilnehmen durfte, habe ich, unter anderem von Seiten eines Staatssekretärs aus dem Bundesverteidigungsministerium, das Wort Meldekette gehört. Und dazu gab es sogar bereits ein Papier. Ich komme aus der Provinz hier zu Ihnen nach Berlin und sehe ein solches Papier, das von kritischen Infrastrukturen spricht. Die vier großen Netzbetreiber finden darin Erwähnung und es ist ausgeführt, wie es gehen soll und vom BSI und einer Meldekette ist die Rede. Ich kann mir das noch relativ gut vorstellen: Vier Netzbetreiber, große Leitwarten, IT-Spezialisten, alles in Ordnung. Etwas weiter hinten ist dann von Energie und Telekommunikation die Rede, wozu auch nur eine Hand voll großer Akteure zählen. Dann werden Nahrungsmittel aufgeführt und die Metro wird erwähnt. Weiter wird dann nichts mehr ausgeführt. Deshalb habe ich angeregt, wenn man schon die Metro heranzieht, dass es dann Sinn macht, im Geiste einmal die Regale durchzugehen und die Aspekte Lebensmittelsicherheit, Lieferkette, Haltbarkeit usw. anzusehen. Es ist dann relativ schnell nicht mehr von Metro die Rede, wo es vermutlich eine große IT-Abteilung mit einem IT-Stab und Security gibt, sondern man hat es mit einzelnen Produkten wie Spreewaldgurken, Halberstädter Würstchen und Ähnlichem zu tun. Ich weiß nicht, ob Sie schon einmal in solchen Betrieben waren, den einen oder anderen kenne ich in der Größenordnung. Es ist dort in der Regel kein eigenständiger IT-Security-Stab zugange, sondern es sind der Geschäftsführer oder „rechte Hände“, die sich redlich um die IT-Sicherheit kümmern und mitunter auch durchaus ordentlich ausgestattet sind, so dass weder Ausfalltage noch verdorbene Lebensmittel aufgrund dessen zu beklagen sind. Aber in einer solchen Meldekette wären diese Firmen einfach nicht gut aufgehoben.

So bitte ich, meinen Hinweis in Bezug auf die Meldekette zu verstehen. Was hinsichtlich des Gesetzentwurfs jetzt in der Planung ist, weiß ich nicht im Detail. Ich würde mir aber wünschen, dass man es ggf. so gestaltet, dass es eben keine verpflichtende Meldekette wird, die Akteure einbindet, die dafür nicht geeignet sind.

Der Vorsitzende: Also noch einmal, damit keine Sachen durcheinander kommen. Das Meldegesetz, das Gegenstand einer Kontroverse hier im Bundestag und auch im Bundesrat war, sollten wir heute außer Acht lassen, es scheint mir nicht der richtige Rahmen dafür zu sein. Wenn überhaupt, dann ginge es um ein IT-Sicherheitsgesetz. So war der Arbeitstitel auf Seiten des BMI, dazu kann Herr Dr. Mantz gleich noch etwas sagen. Wir machen aber erst einmal mit der Beantwortung weiter, danach haben Sie die Möglichkeit, noch darauf einzugehen.

MR Dr. Rainer Mantz (Bundesministerium des Innern): Vielleicht können wir das dennoch ganz kurz erledigen.

Der Vorsitzende: Gut, wenn Sie es ganz kurz auf den Punkt bringen, damit jeder weiß, worüber wir heute hier reden und was im Raum ist.

MR Dr. Rainer Mantz (Bundesministerium des Innern): Dafür bedanke ich mich außerordentlich, weil ich glaube, hier könnte uns eine Begriffsverwirrung auf eine falsche Fährte locken, was wir vermeiden sollten. Es ist hier von einer gesetzlichen Regelung gesprochen worden. Wir denken ja gerade noch darüber nach, ob wir eine solche überhaupt brauchen und die Verpflichtung, schwerwiegende IT-Vorfälle, Cyber-Angriffe und dergleichen zu melden, beispielsweise dem BSI. Das sollten wir auf keinen Fall verwechseln mit dem Meldegesetz. Mehr will ich im Moment dazu gar nicht sagen. Vielen Dank.

Der Vorsitzende: Gut, dann fahren wir fort mit der Beantwortung der Fragen. Das Wort hat dann Herr Könen vom BSI, bitte sehr.

Ltd. RD Andreas Könen (Bundesamt für die Sicherheit in der Informationstechnik): Danke sehr. Ich möchte zunächst auf die an mich gerichtete Frage eingehen und dann noch einen Abstecher machen. Zunächst einmal möchte ich feststellen, dass wir grundsätzlich als BSI davon ausgehen, dass Cloud-Infrastrukturen als Angebot, insbesondere für kleine und mittlere Unternehmen, Sicherheitsvorteile bieten können. Voraussetzung dafür ist allerdings, dass entsprechende Sicherheitsmaßnahmen in den Cloud-Infrastrukturen auf allen Ebenen eingeführt werden. Da ist zunächst einmal die Plattformsicherheit zu nennen. An und für sich würde die Plattformsicherheit aufgrund entsprechender Maßnahmen, wie etwa Verschlüsselung und sichere Datenhaltung, garantieren, dass Daten in der Cloud geschützt sind und verfügbar bleiben. Damit habe ich eigentlich schon den nächsten Punkt angesprochen: Verfügbarkeit ist das wesentliche Kriterium in der Cloud, denn es ist ein besonderer Schutzbedarf gegeben, weil die Daten nicht mehr unmittelbar bei Ihnen in der hauseigenen IT gelagert sind, sondern bei einem Dienstleister vor Ort. Das heißt, es müssen auch entsprechende Maßnahmen ergriffen werden, dass etwa die Internet- oder andere Netzverbindungen, die zum Cloud-Anbieter bestehen, verfügbar bleiben und vertrauenswürdig betrieben werden. Das setzt die bekannten Maßnahmen voraus, die wir beispielsweise in unseren Eckpunkten ausführlich schildern. Darüber hinaus gibt es Anforderungen, die nicht unmittelbar in der Informationssicherheit, sondern im Datenschutz begründet sind. Da sagen wir natürlich ganz klar: Sie müssen einen Anbieter auswählen

können, der vertrauenswürdig ist, der den deutschen Datenschutzrichtlinien bzw. den europäischen Datenschutzrichtlinien unterworfen ist und diese auch in der Art, wie er seine Cloud-Infrastruktur betreibt, beachten kann. Das heißt also für besonders sensitive Daten sind Sie darauf angewiesen, dass diese Daten auch im Rechtsraum der EU oder im deutschen Rechtsraum verbleiben. Das ist ein erklärtermaßen schwieriger Prozess, in einem Cloud-Angebot, das ja gerade bei Kostenbetrachtung darauf angewiesen ist, elastisch zu sein und ggf. Überkapazitäten an anderen Standorten des Cloud-Anbieters zu nutzen. Vom BSI haben wir über die Eckpunkte zur Informationssicherheit hinaus, die wir ja veröffentlicht haben, ein Projekt initiiert, zunächst einmal als Pilotprojekt gemeinsam mit dem Verband der Versicherungsunternehmen, Cloud-Infrastrukturen mit einem Gütesiegel, nämlich einem Zertifikat des BSI, zu versehen. Das Pilotprojekt dient dazu, basierend auf den Kriterien des IT-Grundschutzes und auf den Common-Criteria Zertifizierungsschemata zu entwickeln, die auf die Cloud Anwendung finden können.

Gestatten Sie mir noch eine Bemerkung zum Thema Meldungen an sich, nicht unbedingt Meldepflicht. In der Debatte sollte man vielleicht etwas differenzieren, weshalb es hilfreich sein könnte, danach zu fragen, worauf es dem BSI ankommt, warum es Meldungen benötigt. Ganz entscheidend kommt es darauf an, die grundsätzlichen Gefährdungen, die sich im nationalen, aber auch im internationalen Raum in der IT- und in der Informationssicherheit ergeben, zu kennen, zu beurteilen und darauf zu reagieren und in weiter Sicht Maßnahmen zu unternehmen. Insofern verstehe ich unter Maßnahmen etwas anderes als Herr Müller-Maguhn, nämlich nicht nur die Reaktion, sondern vor allem präventive Maßnahmen, die abgeleitet aus den Gefährdungen und Gefährdungsmustern, die wir sehen, präventiv wieder Sicherheit in den IT-Infrastrukturen implementieren. Dazu benötigen wir nicht die Kenntnis jedes einzelnen Vorfalls en detail, sondern müssen grundsätzlich erkennen können, welche Angriffsmethoden im Raum stehen. Es gibt einen Konflikt, der auch in der Zusammenarbeit mit der Polizei offenbar wird, wo es um Strafverfolgung geht, Bürger und Unternehmen zu schützen, Straftäter zu entdecken und dingfest zu machen und letztlich eine Kriminalprävention eintreten soll. Für uns ist an der Stelle nicht der Kriminalfall als solcher relevant, sondern die Methodik, mithin zu wissen, ob bestimmte Angriffsmuster laufen, wie man sich gegen diese schützt und sie in anderen kritischen Infrastrukturen abwehrt. Und für uns ist daher die zentrale Aussage, dass wir im Hinblick auf kritische Infrastrukturen mit denjenigen intensiv zusammenarbeiten müssen, die uns entsprechende Informationen geben können.

Die Unternehmen können das in einem gewissen Maß über eine Meldekette selbst strukturieren, aber es ist entscheidend, möglichst frühzeitig über kritische Angriffe, über drängende Angriffe, Bescheid zu wissen. Das heißt, wir brauchen Aggregationsstrukturen und Andockmechanismen. Wie die im Einzelnen zu gestalten sind, ist genau das, worauf sich Herr Dr. Mantz vom BMI eben bezogen hat, das ist eine Frage der Organisation und der vertrauensvollen Zusammenarbeit.

Der Vorsitzende: Vielen Dank Herr Könen. Wir fahren fort mit Herrn Müller-Maguhn.

Andy Müller-Maguhn (Chaos Computer Club): Am besten gehe ich auf die Fragen in der Reihenfolge, in der sie gestellt wurden, kurz ein. Herr Dr. Brandl fragte noch einmal nach der Meldepflicht, oder wie wir es auch immer benennen, und welche Alternativen es gebe. Ich möchte zunächst einmal vorwegstellen, dass ich mir durchaus Bereiche vorstellen kann, insbesondere, wenn Interessen Dritter betroffen sind, wo IT-Schadensereignisse gegenüber den Behörden offenlegungspflichtig sein sollten. Zum einen , wenn es um personenbezogene Daten geht, wenn also Daten von Kunden, Bürgern oder wie auch immer, abhanden gekommen sind und nunmehr anderen zur Verfügung stehen. Und zum anderen, wenn Infrastrukturen, beispielsweise durch Botnetze, missbraucht worden sind, um Angriffe auf Dritte durchzuführen. Hier ist auch die Klärung von Haftungsfragen sicherlich im Interesse der Unternehmen, um nicht fälschlicherweise als Urheber von Angriffen identifiziert zu werden. Trotzdem muss man sich natürlich, wenn man jetzt von so einer Melde- oder Offenlegungspflicht redet, die Frage stellen, gegenüber wem und mit welcher Intention etwas gemeldet werden soll. Bevor wir also von irgendwelchen Verpflichtungen auch gesetzlicher Natur reden, wäre es interessant, wenn die staatlichen Stellen, für deren technische IT-Sicherheit ja auch das BSI zuständig ist, in einer Art Modellverfahren ihre Störfälle zunächst einmal offenlegen und zur Verfügung stellen, um zu evaluieren, wohin es führt, wenn man mehr darüber weiß, wie Meldebehörden und sonstige Stellen agieren, die Daten von Bürgern verarbeiten und ja auch alle nur mit Wasser kochen und denen insofern auch hier und da mal etwas passiert.

Das BSI hat in diesem Zusammenhang zwei Probleme. Ein sehr grundsätzliches, nämlich dass es dem Bundesministerium des Innern unterstellt ist und dass hier Interessenskonflikte vorhanden sind, wie in der Vergangenheit auch. Als Stichwort möchte ich hier nur „Exploits“ nennen, noch nicht bekannte Sicherheitslücken, die sich sowohl zur Behebung von Schwachstellen als auch zum Ausnutzen von Schwachstellen, beispielsweise im Kontext von nachrichtendienstlichen Zugriffen, nutzen lassen. Und es wäre sicherlich hilfreich, wenn für die Förderung der öffentlichen Diskussion eine Stelle geschaffen würde, die eher dem Wirtschafts- oder dem Forschungsministerium untersteht und wo die Betroffenen auch nicht in Verdacht stehen, Interessenskonflikten zu unterliegen, wenn es um die Offenlegung und die transparente Darstellung von Sachverhalten geht.

Das andere Problem, das ich beim BSI sehe, hat damit zu tun, dass Maßnahmen, wie die Zertifizierung, in Richtung Einbahnstraße gehen. Dass das BSI gern Empfehlungen ausspricht und ein Grundschutzhandbuch vorsieht, das will ich gar nicht angreifen, das ist wunderbar, aber die Zertifizierung von Produkten und auch von Cloud-Anbietern, das kann schnell zu einer Art Gütesiegel-Business ausarten. Als Ausgleich dazu würde ich mir gerne wünschen, dass Sie in genau derselben Offenheit mal bitte ohne Veranlassung der Betroffenen auch Produkte benennen, die absolut nicht hilfreich sind zur Förderung der IT-Sicherheit. Nur so ließe sich meines Erachtens Ihre Glaubwürdigkeit wieder herstellen, ansonsten verkommen Sie ein bisschen zum Dienstleister der Industrie, was das Verteilen von Gütesiegeln für nicht gerade zielführende Maßnahmen angeht. Und es wäre auch Ihrer Reputation langfristig zuträglich, wenn sich dieser Eindruck nicht zementierte.

Bei der Fragestellung von Herrn Klingbeil in Bezug auf die Diskussion in den USA, was chinesische Anbieter usw. angeht, muss man natürlich erst einmal den Rahmen sehen, in dem sich das alles abspielt. Die US-amerikanische National Security Agency, NSA, die ja sozusagen das amerikanische Pendant zum BSI ist, hat auch beide Funktionen, nämlich die Zertifizierung von Sicherheitsprodukten und Algorithmen durchzuführen, aber auch den Nachrichtendiensten Informationen zukommen zu lassen. Die NSA hat hier ein Motto, nämlich „Nobus“, „No one but us“, das heißt, man hat in gewisser Weise einen exklusiven Anspruch, dass Hintertürchen, so genannte Backdoors, die in Produkte eingebaut werden, nicht koexistieren sollen neben den chinesischen und anderen unter Umständen von staatlichen Stellen initiierten. Auch in Deutschland gibt es so etwas. Ich kenne mehrere Fälle, wo es interessante Diskussionen zwischen dem Bundeskriminalamt und den in ihrer Entscheidungsfreiheit ja freigestellten Landeskriminalämtern gegeben hat über den Einsatz spezifischer Werkzeuge, die in den Ausschreibungen besonders günstig waren. Die Frage ist immer, wenn etwas besonders günstig ist, wer dann den anderen Teil übernimmt. Eine solche Diskussion haben wir natürlich auch in Bezug auf technische Komponenten, die haben wir bei Firewalls und bei so genannten Virenscannern. Wir nennen sie „Schlangenöl“ oder auch „Snake oil Produkte“, die nach außen hin als IT-Sicherheitsprodukte bezeichnet und als solche verkauft werden, in Wirklichkeit aber Drittinteressen dienen und nur scheinbar die Sicherheit erhöhen.

Das lässt sich gut verbinden mit der Fragestellung von Frau Daub, nämlich wie eigentlich eine sachgemäße Handhabe auch bei den Unternehmen erwirkt werden kann. In der Tat glaube ich, dass man feststellen kann, dass egal, welche Branche man sich heute näher ansieht, die Beherrschung von IT-Strukturen zunehmend vitale Unternehmensinteressen berührt. Es ist für die Unternehmen wichtig, Personal zu haben, um nicht nur IT-Strukturen zu betreiben, sondern in gewissem Umfang auch kritische Sachverhalte einschätzen zu können. Und an dieser Stelle könnte ich das jetzt nochmals mit Kritik am BSI verbinden, weil beispielsweise das Grundschutzhandbuch in den Unternehmen eigentlich auch im Sinne einer Schulungspraxis stärker Beachtung finden müsste und weniger als abstraktes Gebilde, wo man dann sagt, ja, das sind die mit dem Grundschutzhandbuch, wenn die etwas zertifizieren, dann wird das schon gut für uns sein. Ich glaube, eine gelebte und engagierte Prozessbegleitung wäre das eigentlich Hilfreiche für viele kleinere Unternehmen. Frau Husch hat da nach meiner Erfahrung auch oftmals eine ganze Bandbreite an Konzepten zur Hand. Fraglich ist nur, wie die dann ankommen. Grundsätzlich glaube ich aber, dass das Angebot auch an IT-fremde Branchen, mitunter auch an kleinere Unternehmen, ausbaufähig ist und nicht nur darin bestehen sollte, Produkte zu empfehlen oder zertifizierte Anbieter zu bewerben, sondern einen Erfahrungsaustausch, auch dezentral vor Ort zu fördern, um hier eine stärkere Immunität und auch prozessuale Flexibilität zu erzielen.

Damit bin ich bei den Fragen von Herrn Behrens. In der Tat, unsere Befürchtung, dass sich die Kriminalisierung von Angriffswerkzeugen ungünstig auf die Fähigkeit von Unternehmen auswirkt, eigene Strukturen überprüfen zu können und auch auf die Lehre, haben sich so noch nicht erfüllt. Wir haben hier eine Gesetzgebung, die von der Interpretation her gesehen zwar immer noch einen ungünstigen Nachgeschmack hinterlässt, aber zum Glück so nicht umgesetzt wurde, wie wir es befürchtet haben, und

auch nicht in der Rechtsprechung. Trotzdem wäre es wünschenswert, hier vor allem für den Bereich der Bildung, also insbesondere für die Hochschulen, weil man sich dort eigentlich noch penibler an Gesetze halten muss als in anderen Bereichen, eine Klarstellung und proaktive offene Handhabe zu haben. Viele Infrastrukturen gelten nämlich nur deswegen als sicher , weil entweder die Angriffe nicht bemerkt wurden oder die Angriffswerkzeuge noch gar nicht ausprobiert wurden, oder zwar alles schon passiert ist und bereits Tests unternommen wurden, aber das Unternehmen beschlossen hat, nicht öffentlich darüber zu sprechen. Dieses Vakuum an Wissen, wo man den Eindruck hat, da mag etwas sicher sein, weil man jedenfalls noch nicht das Gegenteil vernommen hat, dass es unsicher ist, kann, wenn es dann darum geht, einer solchen Struktur Daten anzuvertrauen oder geschäftskritische Prozesse, natürlich problematisch sein.

Im Hinblick auf die von Ihnen angesprochene Cyber-Abwehrfähigkeit oder wie wir es auch nennen mögen, also die Frage, welche Akteure hier die Abwehrkräfte stellen, möchte ich noch einmal zusammenfassen, dass das BSI diesen Interessenkonflikt klären sollte. Das BSI untersteht dem Bundeministerium des Innern und arbeitet damit auch als Dienstleister für die Ermittlungsbehörden. Das ist kein Vorwurf, verstehen Sie mich da bitte nicht falsch, aber dass in diesen Bereichen auch Interessen in Bezug auf Schwachstellen vorhanden sind, diese zu lösen und nicht nur die technische Sicherheit zu erhöhen, sondern die Sicherheit des Staates, die unter Umständen auf der Unsicherheit der Technik basiert, das liegt doch nahe. Dass es hier Interessenskonflikte gibt, das ist nun einmal so, und es wäre langfristig hilfreich, wenn Sie nicht, wie teilweise Vorgänger in ihrer Behörde oder Behördenleiter, hier in unmittelbare Auseinandersetzungen mit Ihrem Dienstherren geraten. Das heißt, eine Meldepflicht würde ich erst einmal nur für die staatlichen Stellen ausprobieren. Zwei Jahre, mal abwarten, was da zusammenkommt, das möglichst transparent, und dann hat man vielleicht etwas Material, auf dessen Basis man diskutieren kann, was es gebracht hat und ob es ein zielführender Weg ist. Danke.

Der Vorsitzende: Zum Schluss Herr Neugebauer für den Bitkom, bitte.

Lutz Neugebauer (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.): Frau Rößner stellte an mich die Frage bzgl. der Notfallpläne. Ich gehe davon aus, dass dabei auch das Thema Sicherheitskonzepte eine Rolle gespielt hat, wie das eingespeist werden kann und welche Aufgabe der Staat dabei hat. Für die Großunternehmen, insbesondere diejenigen, die zu den kritischen Infrastrukturen gehören, gilt in der Regel ein relativ enger regulatorischer Rahmen. Hier gibt es Aufsichtsbehörden, für die Telekommunikationsbranche beispielsweise die Bundesnetzagentur oder für die Bankenbranche, die Bundesanstalt für Finanzdienstleistungen, die auch im Bereich der IT umfangreiche Sicherheitskonzepte fordern. Das BSI hat diesbezüglich aufgrund des BSI-Errichtungsgesetzes eine beratende Rolle. Andere Unternehmen sollten in jedem Fall die bestehenden Beratungsangebote zur Entwicklung von Sicherheitskonzepten in Betracht ziehen. Hier gibt es viele kommerzielle, aber auch nichtkommerzielle Angebote. Darüber hinaus Notfallpläne bzw. Sicherheitskonzepte für die große Masse an Unternehmen verpflichtend vorzusehen, würde vermutlich einen nicht zu überschauenden bürokratischen Aufwand bedeuten. Das heißt, wenn man eine

gesetzliche Verpflichtung vorsieht, muss diese auch überprüft werden, und das wirft dann Fragen auf: Wer soll das tun, welche Konsequenzen soll es geben, wenn das nicht vollzogen worden ist usw. Ich glaube, dass dies heute gar nicht notwendig ist, denn wir sehen da einen Paradigmenwechsel. Die Unternehmen sehen durchaus, dass Cyberbedrohung für sie ein Thema ist. Das hängt mit der Generation der Digital Natives zusammen, die IT ganz anders nutzt als die weniger IT-affinen Geschäftsführer und die Vorstände, die im Moment Entscheidungen treffen und deshalb erst einmal dafür sensibilisiert werden müssen. Für die jüngere Generation wird ein Risikomanagement zukünftig wahrscheinlich von vornherein IT-Risiken umfassen. Wenn man sich insofern dann Gedanken darüber macht, welche IT-gestützten Geschäftsprozesse es besonders abzusichern gilt, weil sie wesentliche Grundlage des Geschäftes sind, welche Daten besonders vertraulich und deshalb schützenswert sind und was im Falle eines Angriffs als Notfallmaßnahme notwendig ist, dann bilden die Antworten auf diese Fragen, so man sie zu Papier bringt, schon die Basis eines Sicherheitskonzeptes. Wenn man zum Beispiel einen Online-Shop betreibt und eine Denial of Service-Attacke auf einen zurollt oder versucht wird, von außen in die Systeme einzudringen, um ggf. Entwicklungsdaten zu stehlen, dann wäre es gut, konkrete Handlungsvorgaben für die Mitarbeiter zu haben und auch konkrete Meldewege. Hierfür muss man aus unserer Sicht keine gesetzliche Regelung schaffen. Wie gesagt, das würde eher ein Bürokratiemonster werden, bei jedem Unternehmen letztlich die Umsetzung zu überwachen.

Der Vorsitzende: Vielen Dank. Wir sind damit am Ende der ersten Fragerunde angekommen. Es scheint, alle Fragen sind beantwortet worden. Dann darf ich die zweite Fragerunde aufrufen. Da hatte sich für die Fraktion der CDU/CSU schon Thomas Jarzombek gemeldet.

Abg. Thomas Jarzombek (CDU/CSU): Danke Herr Vorsitzender. Es macht immer besondere Freude hier im Deutschen Bundestag über Datensicherheit zu sprechen und dabei vor Augen zu haben, wie die eigenen Mitarbeiter Computer nutzen, an denen teilweise ein Jahr lang keine Patches für die Webbrowser installiert wurden und bereits beim Besuch von lediglich einfach kompromittierten Websites mittlerweile fast jeder Rechner in meinem Büro mit großem Aufwand neu installiert werden muss. Vor diesem Hintergrund wäre es vielleicht auch einmal interessant, über eigene Standards zu reden und bevor man Meldepflichten für Unternehmen aufsetzt, erst einmal eine Meldepflicht für den Deutschen Bundestag zu etablieren, was das BSI betrifft. Nun gut, das sind jetzt zwar keine Fragen, aber ich spreche aus eigener Erfahrung.

Wenn man über Großunternehmen und zugleich über kleine und mittlere Unternehmen spricht, dann sind das komplett zweierlei Paar Schuhe. Ich glaube, das, was Herr Müller-Maguhn in Bezug auf Großunternehmen gesagt hat, ist richtig und kann man unterstreichen, insofern gibt es meines Erachtens in der Tat in der Regel kein Kompetenzproblem. Ich glaube aber, dass es ein solches Kompetenzproblem gibt, wenn man in den Bereich der kleinen Unternehmen blickt und die Frage aufwirft, wer dort eigentlich die Sicherheit implementiert. Das sind dann nämlich kleine IT-Dienstleister, teilweise Freiberufler oder Studenten, mitunter Leute, die das mal eben so nebenher machen. Abgesehen einmal von der Schwierigkeit, einem Manager klarzumachen, für etwas zu investieren, das nicht sichtbar ist, für

irgendwelche Kisten und Software, die im Keller stehen, was meistens weniger Spaß macht, als für Flachbildschirme oder andere repräsentative Dinge IT-Budgets auszugeben, geht es meistens darum, wie kompetent eigentlich der Dienstleister ist. Und wenn das dann tatsächlich ein Student, ein Freiberufler bzw. eine kleine Firma machen, dann ist davon auszugehen, dass die einen vielleicht eine ganz bestimmte möglicherweise passende Technologie kennen und beherrschen und andere eben halt nicht. Insofern, glaube ich, ist hier zwar eine Menge Potenzial vorhanden, das man bergen kann, aber nicht auf gesetzlichem Wege. Deshalb würde ich auch gern an Herrn Neugebauer und an Herrn Müller-Maguhn die Frage richten, ob sie diese These teilen und ob es nicht eine Initiative wert wäre, wie auch immer geartet, ich traue mich fast gar nicht, es auszusprechen, bei all den Gütesiegeln, die hier heute schon angesprochen wurden, gleichwohl aber irgendeine Kennzeichnung und Zertifizierung der IT-Dienstleister für KMUs vorzusehen.

Wenn Sie heutzutage Geschäftsführer einer Firma mit z.B. zehn Mitarbeitern sind und einen IT-Dienstleister suchen, dann kommen dafür in der Regel eher kleine Firmen in Frage. Es geht dann darum, herauszubekommen, ob dort Kompetenz vorhanden ist. Man kann vielleicht sehen, ob die Firma den Eindruck erweckt, zuverlässig zu sein, Ansprechpersonen freundlich sind und die Systeme hinterher einwandfrei funktionieren, aber was da im Verborgenen so passiert, das weiß eben keiner. Und deshalb glaube ich, ist eigentlich die Wirtschaft selbst in der Verantwortung, entweder über den Bereich der Industrie- und Handelskammern, vielleicht aber auch über den Verband Bitkom oder über welche Initiativen auch immer. Ich glaube nicht, dass dies ein Ansatz für irgendwelche Gesetze ist.

Schließlich habe ich noch eine Frage an Herrn Könen, weil ja vorhin schon einmal gefragt wurde, wie das denn mit der NSA in den USA und mit den Chinesen bei Huawei aussieht. In dem Kontext würde ich schon gern einmal wissen wollen, ob das BSI bei der Fritzbox und bei den Nachfolgern des früheren Anbieters Elsa, also Lancom und Devolo, Backdoors zu implementieren gedenkt oder mit diesen auch über Sicherheit gesprochen wird.

Der Vorsitzende: Das war nicht als Ermunterung zu sehen. Ich glaube, das können wir so festhalten. Für die Fraktion der SPD Herr Dörmann, bitte.

Abg. Martin Dörmann (SPD): Danke Herr Vorsitzender. Meine Frage richtet sich in erster Linie an Herrn Könen und Herrn Müller-Maguhn, wobei ich nichts dagegen hätte, wenn die anderen beiden Herren Sachverständigen, so sie sich berufen fühlen, auch darauf eingehen würden. Meine Frage zielt im Kern darauf ab, ob es geboten wäre, eine Differenzierung je nach Infrastruktur und betroffenen Einrichtungen und Unternehmen vorzunehmen. Anfang des Jahres 2012 erschien ein Buch mit dem Titel „Zeitbombe Internet: Warum unsere vernetzte Welt immer störanfälliger und gefährlicher wird “, welches das Problem sehr reißerisch, muss man ehrlicherweise sagen, aufgegriffen hat. Darin wurde gefragt, wieso man nicht hingeht und neuralgische Punkte wie Flughäfen und Verkehrsinfrastrukturen und Atomkraftwerke mehr oder weniger in gesonderten Netzen betreibt – ich verkürze das jetzt ein bisschen – ihnen zumindest erhöhte Sicherheitsstandards auferlegt. Nun gehe ich davon aus, dass solche ohnehin bestehen,

weshalb ich zunächst gerne wüsste, ob Sie die Analyse, die verbreitet wird, teilen, dass es besondere Gefahren gibt, auf die man auch besonders reagieren sollte. Daran anschließend möchte ich die Frage stellen, wie eine differenzierte Lösung im Hinblick auf neuralgische Punkte in Bezug auf Infrastruktur aussehen könnte, unabhängig von gesetzlichen Regelungen. Könnte es sein, dass man bis hin sogar zu eigenständigen Infrastrukturen, die man vorschreibt, noch tiefer gehen muss, als es eine gesetzliche Regelung je könnte.

Der Vorsitzende: Für die FDP-Fraktion Frau Daub, bitte.

Abg. Helga Daub (FDP): Meine Gedanken gehen im Grunde genommen in die Richtung derer von Herrn Dörmann und befassen sich auch mit der Differenzierung. Und da haben wir nicht nur die Branchen und Dinge, die Sie eben erwähnt haben, sondern auch Unternehmen aus dem KMU-Bereich, die im Verteidigungssektor tätig sind. Dazu lautet meine Frage, ob diese Unternehmen nicht von sich aus schon verpflichtet sind, Sicherheitssysteme zu installieren, denn es wäre sicherlich besonders wichtig, da etwas zu machen. Danke.

Der Vorsitzende: Die Frage ging wahrscheinlich an das BSI, vermute ich. Ja, Herr Könen, Sie signalisieren, dazu etwas sagen zu wollen. Dann machen wir jetzt weiter mit Herrn Behrens für die Fraktion DIE LINKE.

Abg. Herbert Behrens (DIE LINKE.): Ich habe eine Frage an Herrn Müller-Maguhn und an Herrn Könen bezüglich der Tendenz und der Entwicklung in der Privatwirtschaft, aber auch hier im Deutschen Bundestag, vermehrt private Geräte einzuführen und Bestandteil des jeweiligen Netzwerks werden zu lassen. Die IT-Betreuer sind zunächst immer sehr kritisch bei solchen Fragen, gleichwohl, gestatten sie es letzten Endes. Wie müssen wir da eigentlich vorgehen? Wäre es grundsätzlich nötig, einen Standard festzulegen, mit dem die Geräte ausgestattet sein müssen, um keine sicherheitsrelevanten Türen, Hintertüren oder Vordertüren aufzumachen? Oder ist das eher eine Frage, die auch dann, wenn ggf. eine solche Tür geöffnet ist, noch über interne Schutzmechanismen innerhalb der jeweiligen Netze aufgefangen werden kann? Ist da möglicherweise auch gesetzgeberischer Handlungsbedarf gegeben?

Der Vorsitzende: Nun noch Frau Rößner für die Fraktion BÜNDNIS 90/DIE GRÜNEN.

Abg. Tabea Rößner (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Ich habe eine Frage an Herrn Könen. Mir scheint, die Skepsis, was eine Meldepflicht betrifft, ist hier sehr groß. Steckt hinter dieser Meldepflicht nicht auch die Idee, dass andere Unternehmen im Hinblick auf ihre Infrastruktur und ihre zu schützenden Daten davon profitierten, wenn möglichst schnell und aktuell reagiert werden könnte? Wie soll das denn gewährleistet werden? Wie aktuell kann das denn sein, wenn eine solche Meldepflicht nicht besteht und keine Meldung erfolgt? Ist der Schutz der anderen Unternehmen dann nicht geringer, wenn man nicht mehr so schnell reagieren kann? Vielleicht können Sie dazu etwas sagen.

Und dann habe ich noch eine Frage an Herrn Müller-Maguhn. Sie betrifft die Position Ihres Kollegen Sandro Gayken, der eine Entnetzung fordert. Wie stehen Sie dazu? Ein bisschen ist hier ja auch schon angeklungen, was es mit getrennten Netzen auf sich hat. Aber das ist, glaube ich, insgesamt wohl etwas schwierig.

Der Vorsitzende: Dann haben wir hiermit die zweite Fragerunde komplett. Wenn ich es richtig sehe, hat Herr Gutmann diesmal keine Frage erhalten und wir können direkt bei Herrn Könen einsteigen. Bitte schön.

Ltd. RD Andreas Könen (Bundesamt für die Sicherheit in der Informationstechnik): Danke sehr. Diesmal hat mich zwar eine geballte Ladung an Fragen erwischt, aber nichtsdestotrotz möchte ich die Gelegenheit nutzen, um auch noch auf die eine oder andere Anmerkung von Herrn Müller-Maguhn einzugehen. Also, beginnen wir mit der Frage in Bezug auf Backdoors, die von Ihrer Seite kam. Ich möchte ausdrücklich sagen, dass wir nirgendwo Backdoors einbauen, da so etwas völlig kontraproduktiv wäre. Die im BSI-Gesetz vorgesehene Unterstützung der Polizei und der Nachrichtendienste ist eine eindeutig fallgebundene Option, die dazu dient, in schwierigen Fällen der Strafverfolgung oder bei entsprechenden nachrichtendienstlichen Erkenntnissen mit den Mitteln des BSI fallbezogen zu helfen. Das kann zum Beispiel die Lesbarmachung von Asservaten sein. Wir lehnen es grundsätzlich ab, irgendwelche Backdoors in Geräte einzubauen oder irgendeinen Gebrauch im Sinne von Dual Use von uns bekannten Zero-Day-Exploits oder irgendwelchen anderen Schwachstellen zu machen oder einen solchen zu propagieren. Sie können sicher sein, dass wir das, was im BSI-Gesetz in Bezug auf eine Meldepflicht mit entsprechender Warnung implementiert ist, voll und ganz im Sinne der Informationssicherheit nutzen. Verstehen Sie das bitte auch als Replik auf verschiedene Einwürfe von Herrn Müller-Maguhn. Diese Trennung ist klar und deutlich gegeben. Selbstverständlich reden wir mit Firmen wie Lancom und AVM, um diesen unsere Vorstellungen in Bezug auf Informationssicherheits- und Qualitätskriterien mitzuteilen. Wir haben diese Firmen verschiedentlich auch im Bund und in anderen öffentlichen Verwaltungen als Vertragspartner. Maßstäbe, die da angelegt werden, basieren auf Kriterien, die wir in Bezug auf die Informationssicherheit insbesondere auch im Bereich der Common Criteria entwickelt haben.

Dann möchte ich die Frage von Herrn Dörmann bezüglich der Differenzierung von kritischen und besonders kritischen Infrastrukturen aufgreifen. Wir haben es bei „kritischer Infrastruktur“ mit einem Begriff zu tun, der sich an der Daseinsvorsorge orientiert. Wir haben aufgrund des Umsetzungsplans „Kritis“ im Laufe der vergangenen fünf Jahre gelernt zu differenzieren, welche Unternehmensgruppen gerade im Bereich der Informationstechnik als besonders kritisch zu gelten haben. Natürlich haben Sie recht, in dem Moment, in dem wir Flughäfen oder andere Infrastrukturen bei Providern betrachten, sind diese in der Tat in besonders hohem Maße Risiken ausgesetzt. Deshalb haben diese sich in aller Regel bereits aus rein wirtschaftlichen Gründen mit Fragen der Notfallvorsorge und der Geschäftsfortführung (Business Continuity Management) befasst und sich Regeln der Informationssicherheit auferlegt, die unter anderem auch die Separierung von Netzen beinhalten. Die Infrastrukturen beispielsweise von

Flughäfen werden nicht nur in Bezug auf die Elektrizitätsversorgung abgesichert, sondern natürlich auch dahin gehend, dass die kritischen Netze, die beispielsweise in der Flugsicherung verwendet werden, abgeschottet und getrennt sind von allen anderen. Das trifft nach unseren Erkenntnissen in hohem Maße auch auf andere sicherheitskritische Branchen zu, erst recht dort, wo natürlich schon grundsätzlich gesetzliche Regelungen im Raum sind, etwa bei den Kraftwerksbetreibern und anderen, bei deren Betrieb Informationssicherheit bereits integriert ist in zahlreichen andere Vorschriften, die zu beachten sind. Wir würden dafür plädieren, entweder über Standards oder technische Richtlinien und notfalls per gesetzlicher Regelung, das für besonders kritische Branchen, die bislang noch nichts implementiert haben, einzuführen. In dieser Eskalationskette befassen wir uns zunächst mit Standards. Das BSI ist in Bezug auf Standardisierung äußerst intensiv mit dem Deutschen Institut für Normung (DIN) und der International Organization for Standardization (ISO) zugange und in deren Aktivitäten integriert. Das ist der Weg, mit dem wir beginnen und lediglich da, wo praktisch trotz besseren Wissens keine Maßnahmen unternommen werden, plädieren wir dafür, entsprechende gesetzliche Regelungen einzuführen.

Die nächste Frage betrifft die Differenzierung bei KMU. Natürlich muss man bei KMU differenzieren, denn es gibt Unternehmen, die besonderes Know-how aufweisen, sehr innovativ sind, mit Patenten und Ähnlichem einen Wissensschatz besitzen, den man besonders schützt. Und auch in der Verteidigungswirtschaft ist es natürlich so, dass Unternehmen dort in einem besonders hohen Maße Angriffen ausgesetzt sind. Im Verteidigungsbereich gibt es mit den Maßnahmen des Geheimschutzes ohnehin besondere Regelungen. Das Bundesministerium für Wirtschaft und Technologie ist auf Seiten der Bundesregierung für den Geheimschutz in der Wirtschaft und die Regelungen, die dort zu treffen sind, zuständig. Diese entsprechen denen des behördlichen Geheimschutzes, für den das BSI – insbesondere auch meine Abteilung – zuständig ist. Derartige Maßnahmen sind überall dort anzutreffen, wo eine Zusammenarbeit mit öffentlichen Stellen stattfindet.

Schließlich ist „Byod“, „bring your own device“, das Stichwort. Das ist ein echtes Problem. Der öffentlichen Verwaltung empfiehlt das BSI definitiv ausschließlich den Einsatz entsprechend zugelassener Geräte. Wenn Mitarbeiter ihre eigenen Geräte mitbringen, hat man nämlich ansonsten mit den verschiedensten Problemen zu kämpfen. Das einfachste davon ist das der IT-Vielfalt. Sie muten den Administratoren eines bis dahin gut gesicherten Hauses zu, sich auf ein Sammelsurium an Geräten einrichten zu müssen, das sehr schwer unter Kontrolle zu bekommen ist. Es gibt für fast jedes dieser Geräte natürlich auch von Herstellerseite gelieferte Sicherheitsmaßnahmen. Die sollte man in jedem Falle einsetzen. Darüber hinaus gibt es aus unserer Sicht aber für nicht wenige Geräte Gefährdungen, die damit nicht aus der Welt zu schaffen sind und die insbesondere dort, wo es eben, wie hier im Deutschen Bundestag, besonders sicherheitskritische Dinge zu kommunizieren und zu speichern gilt, nicht ausreichen. Gut, was den Deutschen Bundestag angeht, sind wir zwar nicht zuständig für dessen Informationssicherheit, aber wir reden intensiv mit der Bundestagsverwaltung und geben, wenn wir darum gebeten und gefragt werden, konsistente Empfehlungen ab unter Berücksichtigung dessen, was wir der gesamten Bundesverwaltung empfehlen. Das ist der Einsatz zugelassenen Geräts für Kommunikation, für Internetsurfen und Datenverarbeitung.

Dann möchte ich auf die letzte Frage, die von Frau Rößner in meine Richtung gegangen war, eingehen. Natürlich können andere Unternehmen davon profitieren, wenn ihnen bekannt ist, was in der eigenen Branche an Gefährdungen anfällt. Insofern führte ich eben ja auch aus, dass wir als BSI Wert darauf legen, die Angriffsmethoden zu kennen, um in der Lage zu sein, diese Information und eine solche über mögliche Präventivmaßnahmen an andere potenziell Betroffene geben zu können. Das ist der entscheidende Punkt. Wenn wir zu einer Meldepflicht kommen, die so etwas natürlich per se garantieren würde, dann ist im Rahmen der Selbstorganisation gefordert, kritische Informationslücken wirklich zentral, im Idealfall natürlich beim BSI, anhängig zu machen. Wir haben dann die Möglichkeit, Warnungen nach der Maßgabe von § 7 BSI-Gesetz abzugeben und das ist dann auch der Weg, um auf eher schwache Dienstleistungen im Hinblick auf die Informationssicherheit hinzuweisen. Solche Warnungen sind aber, um auch noch einmal auf Ihren Einwand einzugehen, lediglich eine Ultima Ratio. Würden wir das jedes Mal und immer wieder machen, könnte man uns zu Recht vorhalten, dass wir uns an der Stelle in den Wettbewerb zwischen Informationssicherheitsunternehmen einmischen. Und das ist ein schwieriges Terrain. Wir haben es beschritten in der letzten Zeit und gelegentlich explizit vor bestimmten Produkten gewarnt. Nicht nur zur Freude der Unternehmen, aber immer in Rückkoppelung mit ihnen. Nach wie vor halte ich es für den besten Weg, hier zu Warnungen und Negativaussagen zu kommen. Flächendeckende Negativaussagen halte ich allerdings nicht für das probate Mittel, sondern Positivaussagen scheinen mir eigentlich durchweg besser zu sein.

Der Vorsitzende: Vielen Dank Herr Könen. Wir fahren dann fort mit Herrn Müller-Maguhn.

Andy Müller-Maguhn (Chaos Computer Club): Dankeschön. Herr Jarzombek, Sie fragten, inwieweit es denkbar wäre, ein Gütesiegel für Dienstleister zu vergeben. Das ist eine schwierige Sache, weil nach meiner Erkenntnis bislang weder beim BSI noch bei anderen Behörden Bewertungen für Prozesse eine Rolle spielen, sondern eher Bewertungen für Produkte geregelt sind. Es gibt natürlich im Zusammenhang mit dieser ganzen Compliance–Diskussion den Versuch, auch Prozesse einzuführen – im Bereich des Datenschutzes beispielsweise ist das schon ein bisschen etablierter als jetzt bei der IT-Sicherheit –, indem man sagt, Unternehmen müssen diese und jene strukturellen Merkmale haben, um entsprechend den gesetzlichen Bestimmungen Daten zu verarbeiten und bei Sachverhalten zu reagieren. Und damit komme ich, glaube ich, zu einem der Kernpunkte, nämlich dem Stichwort Reaktion. Wenn man noch einmal einen Schritt zurück macht und sagt, Sicherheit ist ein Prozess, dann ist eines der entscheidenden Sicherheitskriterien nicht so sehr die Frage, ob ein Produkt heute hier in der Betrachtung sicher ist, sondern wie schnell der Hersteller Probleme löst und ihm zugänglich gemachtes Wissen um Probleme überhaupt bzw. umgehend einbringt. Das heißt, Reaktionszeiten sind zum Beispiel ein Aspekt, wo ich mir denken könnte, ohne das gleich negativ zu bewerten, aber vielleicht als Anregung zu verstehen, dass sich das BSI um die Objektivierbarkeit der Bewertung von Sicherheitsprodukten kümmert und sich das somit alles ein bisschen relativiert, denn es handelt sich dabei lediglich um Momentaufnahmen. In dem Zusammenhang kommt auch die Frage auf, wie man das bei Unternehmen bewerten könnte. Ich würde das für eine reizvolle Aufgabe halten, kann Ihnen jetzt aber nicht gleich aus dem Stehgreif heraus sagen, wie das funktionieren könnte und wie man bewerten wollte, inwieweit Unternehmen bei Ereignissen

vorbildlich agieren in Bezug auf zum Beispiel betroffene Daten von Kunden bzw. in Bezug auf die Eingrenzung von Risiken und welche Konsequenzen es ggf. für Dritte gäbe. Ich nenne nur den Missbrauch von Infrastrukturen für Angriffe und ähnliche Dinge. Ich bin also nicht sicher, ob wir da schon sind.

Die Differenzierung zwischen kritischen und normalen Infrastrukturen, damit komme ich jetzt zur Frage von Herrn Dörmann, ist ein Thema, das wir eigentlich gerade in der Retroperspektive diskutieren. Früher war es so, dass es getrennte Netze gab. Geldautomaten beispielsweise liefen über X25, über ISDN und so etwas. Heute, wo man aus Kostengründen naheliegenderweise internetbasierte Protokolle und ähnliche Infrastrukturen hat, „fressen“ die das alles auf. Und selbst wenn man jetzt mit der Idee käme, wieder eine strikte Trennung zu machen, und zu sagen, das hier ist kritisch im Gesundheitswesen oder andernorts, wo bestimmte Daten verarbeitet werden, so würde man mit Sicherheit doch Standardkomponenten und Standardtechnologien verwenden. Das heißt, es ist aus meiner Sicht nicht realistisch, hier zu einer anderen Infrastruktur zu kommen, weil man am Ende des Tages dieselben Mittel benutzen würde und dieselben Probleme hätte.

Was eine Einschätzung in Bezug auf Backdoors und eine mögliche Exploitability, also das Ausnutzen von Schwachstellen, angeht, scheint mir all das eine Frage der Offenheit zu sein, wie damit umgegangen wird. Es gibt ja auch Open–Source–Ansätze, bei denen man die Vermutung haben kann, indem der Quellcode offenliegt, könnte es einfach sein, Schwachstellen zu bewerten. Das mag zwar grundsätzlich richtig sein, aber wenn kein Personal vorhanden ist, um diese Bewertung durchzuführen, dann ist es damit eben nicht getan. Und es lässt sich hier in der Tat Personalbedarf in der ganzen Angelegenheit feststellen, weil Unternehmen sich oftmals darauf reduzieren, genau das zu tun, was zur Aufrechterhaltung ihrer Geschäftsprozesse notwendig ist. Dabei gelten mitunter ganz einfache Kalkulationen. Wenn man mehr in Marketing investiert, hat man vielleicht mehr Umsatz. Wenn man mehr in Sicherheit investiert, was hat man dann? Dann hat man vielleicht ein paar Leute, die sich im Keller mit Technik beschäftigen, aber Sicherheit ist an dieser Stelle eben kein messbarer Unternehmensgewinn. Und das ist eines der Probleme, denen auch mit einer Meldepflicht nicht beizukommen ist, sondern bestenfalls mit einem intensiveren Erfahrungsaustausch zwischen den Beteiligten.

Herr Behrens, da war noch die Frage nach privaten Endgeräten und Ähnlichem, was einige Ortungswanzen und andere wiederum mobile Endgeräte nennen. Klar ist natürlich, wenn Sie als Betrieb Smartphones einführen oder Ähnliches, dann haben Sie das Problem, dass mit der Voreinstellung der Geräte Google-Account, GPS-Funktion und Facebook-Account gleich mitkommen bzw. standardmäßig schon konfiguriert sind und entsprechend die Daten der Teilnehmer, denen die Geräte dann in die Hand gedrückt werden, Dritten bereits zugänglich sind, bevor sie eigentlich für die betrieblichen Zwecke genutzt werden. Darin liegt das Problem, und das hat auch damit zu tun, dass diese Geräte teilweise von den Datenverwertern subventioniert auf den Markt kommen . Ich denke, dass hier zunächst einfach einmal Aufklärung zielführend ist. Denn ich bin skeptisch, ob es funktionieren würde, aufgrund gesetzlicher Verpflichtungen anbieterneutrale Geräte auf den Weg zu bringen. Da müsste mir erst einmal

jemand aus dem legislativen Bereich eine Gegenfrage beantworten. Sie können sich die ja notieren. Ich glaube, damit habe ich die Aspekte beantwortet.

Der Vorsitzende: Gut, dann fahren wir fort mit Herrn Neugebauer. Ich weiß, Herr Gutmann, dass Sie um 15:00 Uhr eigentlich einen Anschlusstermin haben. Also, wenn das knapp wird, dann nehme ich die Gelegenheit wahr, Ihnen zu danken und Sie zu verabschieden, ansonsten bleiben Sie gern bis zum Ende. Ja? Dann Herr Neugebauer, bitte.

Lutz Neugebauer (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.): Es ist noch die Antwort auf die Frage bezüglich eines Gütesiegels, insbesondere für Personen, glaube ich, offen. Herr Jarzombek, das war Ihre Frage. Wie kann ich dem vertrauen, der als Dienstleister zu mir in die Firma kommt, mich berät oder vielleicht eine Konfiguration von bestimmten Hard- bzw. Softwareteilen vornimmt? Es gibt neben der Produktzertifizierung auch die Personenzertifizierung. Im Bereich der Informationssicherheit kann man sich beim BSI als Grundschutzauditor zertifizieren lassen, was eine durchaus anspruchsvolle, das heißt aber auch aufwändige und nicht ganz günstige Leistung, ist, die man in Anspruch nehmen kann. Man kann sich natürlich auch bei diversen TÜV-Institutionen als ISO 27.001-Auditor zertifizieren lassen. Es gibt darüber hinaus internationale Zertifikate, Akronyme wie CISSP und T.I.S.P. Letzteres ist ein deutsches Akronym von Teletrust, einem Informationssicherheitsprofessional. Es ist für einen Mittelständler nur schwer zu erkennen, welche Qualität konkret hinter einer Dienstleistung steckt. Das ist ein Punkt, mit dem wir uns im Bitkom in diesem Jahr intensiv auseinandersetzen. Dabei sind – das habe ich bereits in meinem Eingangsstatement erwähnt – die Ausbildung und die Weiterqualifizierung ganz wesentliche Punkte. Beispielsweise ist die Funktion eines Sicherheitsbeauftragten in einem Unternehmen ein solch wesentlicher Punkt. Und auch dort muss man darauf schauen, wie man die Personen adäquat qualifiziert. Diesbezüglich gibt es dann verschiedene Möglichkeiten, je nachdem, wie anspruchsvoll man das Thema IT-Sicherheit in einem Unternehmen umsetzen will. Also, an diesem Thema sind wir dran beim Bitkom, versuchen eine entsprechende Einordnung vorzunehmen und mit einem Leitfaden Unternehmen eine Hilfestellung zu geben. Und natürlich sollte man auch erwähnen, dass wir unseren Bitkom-Mitgliedern entsprechende Angebote machen.

Bei Zertifikaten ist allerdings beachtlich, ist, dass diese auf einen Zeitpunkt bezogen sind und man damit die Qualität einer Ausbildung lediglich zu einem bestimmten Zeitpunkt darstellen kann. Einige Zertifikate, die es am Markt gibt, fordern deshalb, dass man sich regelmäßig weiterqualifiziert und an bestimmten Veranstaltungen teilnimmt. Prüfungen, glaube ich, muss man nicht immer wieder ablegen, aber eben diese Weiterbildung entsprechend ernst nehmen und ein bestimmtes Volumen an Stunden absolvieren. Als Mittelständler, sofern man mit diesen Akronymen etwas anfangen kann und sich informiert und schaut, ob ein Dienstleistermitarbeiter diese Zertifikate vorzeigen kann, dann kann man schon relativ sicher sein, dass man qualitativ gut beraten wird. Abraten würde ich tatsächlich von einer studentischen Aushilfe, die sich vielleicht ganz gut über den Heise-Ticker informiert, aber über keine tiefer gehenden Kenntnisse verfügt. Da muss man zudem prüfen, wie man ggf. Regressansprüche geltend machen kann,

weil es letztendlich schwierig nachzuweisen ist, ob ein Student, der prinzipiell vielleicht gut sein mag, dort auch dieses Qualitätsniveau erreicht.

Der Vorsitzende: Wenn der Student den Heise-Ticker kennt, ist das ja schon einmal ein erster Schritt. Von Frau Husch habe ich signalisiert bekommen, dass sie auf die Frage von Herrn Jarzombek hin ein paar Punkte aufgreifen möchte.

MR´n Gertrud Husch (Bundesministerium für Wirtschaft und Technologie): Ich wollte gern zu der Frage der IT-Dienstleister etwas sagen, aber im Prinzip hat Herr Neugebauer es schon umfassend dargestellt. Ich denke, dass es richtig ist, das Thema der Wirtschaft zu überlassen. Die Verbände kümmern sich intensiv darum, es gibt Teletrust und es gibt Bitkom, die entsprechende Zertifikate erteilen. Die IT-Dienstleister sind eine sehr lohnende und wichtige Gruppe, die es gilt weiterzubilden. Dann muss ich an der Stelle auch einmal eine Lanze für die deutsche Sicherheitsindustrie brechen, die manchmal vielleicht zu kurz kommt, weil es überwiegend nur kleine und mittlere Unternehmen sind. Aber, da gibt es sehr viele, die sich etwa eine No-Backdoors-Kampagne auf die Fahne geschrieben haben, und das halte ich für ganz wichtig, da sie damit auch gut fahren und erfolgreich sind im Export solcher Produkte. Ich finde, man sollte sie nicht vergessen, aber das nur am Rande.

Ansonsten möchte ich noch kurz auf die Frage nach gesetzlichen Verpflichtungen eingehen. Es gibt zum einen Verpflichtungen für Betreiber kritischer Infrastrukturen, Sicherheitsvorfälle zu melden und Mindestanforderungen in Bezug auf die IT-Sicherheit zu genügen. Die gibt es für den Telekommunikationsbereich, für den Energiebereich und für den Bankensektor. Die Anforderungen für letzteren sind als sehr weitgehend anzusehen, weil die Branche jeglichen Sicherheitsvorfall der zuständigen Aufsichtsbehörde anzeigen muss. Und das ist, denke ich, auch ganz richtig so. Zum Zweiten gibt es, was den Verlust personenbezogener Daten anbelangt, Verpflichtungen gemäß dem Bundesdatenschutzgesetz. Im Falle eines Falles sind entsprechende Vorfälle dem Bundesbeauftragten für den Datenschutz und die Informationssicherheit zu melden. Darüber hinaus gibt es nach unserer Auffassung keinen Bedarf für eine allgemeine Meldepflicht, zumal diese insbesondere auch kleine und mittlere Unternehmen außerhalb der kritischen Infrastrukturen treffen würde. Das ginge uns zu weit. Neben dem bürokratischen Aufwand wäre auch zu bedenken, dass es letztlich ein Wettbewerbsnachteil wäre, weil wir in Europa da noch ganz alleine dastehen würden. Ein solcher Alleingang würde für die Unternehmen immer einen Wettbewerbsnachteil bedeuten. Deshalb denke ich, sollten wir das erst dann einführen, wenn es von europäischer Seite tatsächlich als Verpflichtung vorgegeben würde.

Der Vorsitzende: Ja, bitte Herr Dr. Mantz, noch einmal zur Ergänzung für das BMI.

MR Dr. Rainer Mantz (Bundesministerium des Innern): Nur zum allerletzten Satz der Frau Kollegin. Da würde ich einfach gern klarstellen wollen, dass ich eingangs bereits gesagt hatte, dass wir uns sehr reiflich überlegen müssen, ob eine Meldepflicht sinnvoll sein könnte. Aber, wenn überhaupt, dann ist die Debatte da ja immer nur im Hinblick auf kritische Infrastrukturen erfolgt. Also, etwas anderes steht ja nun

wirklich nicht im Raum. Und, wie gesagt, nehme ich aus dieser Diskussion gern mit, dass das sicherlich etwas ist, was sehr sorgfältig erwogen sein will. Das machen wir ohnehin und dabei soll man, auch das ist ja bereits mehrfach angesprochen worden, sich genau überlegen, ob das denn so zielführend ist und einen wesentlichen Fortschritt oder Unterschied zur bestehenden Situation bringen würde.

Der Vorsitzende: Vielen Dank auch an die Vertreter der beiden Ministerien. Wir haben mit der heutigen Sitzung die Reihenfolge richtig eingehalten: Wir setzen erst auf den Sachverstand in Person der Experten, beraten das Thema dann später erneut im parlamentarischen Raum, um in einem weiteren Schritt zu der Frage zu gelangen, inwieweit administratives Handeln, in welcher Ausprägung und Detailschärfe auch immer, überhaupt notwendig sein könnte. Mir liegen jetzt keine weiteren Wortmeldungen und auch keine Fragen mehr vor. Dann hätten wir die beiden Fragerunden abgeschlossen und lägen auch gut in der Zeit, so dass ich die Gelegenheit nutzen möchte, mich bei Ihnen, den Sachverständigen, zu bedanken, dass Sie den Weg zu uns gefunden haben. Jetzt habe ich aber offenbar Herrn Gutmann noch einmal aus der Reserve gelockt. Sie haben noch eine Anmerkung? Dann bitte schön.

Klemens Gutmann (Deutscher Industrie- und Handelskammertag e. V.): Ich wollte noch einen Aspekt beitragen, auch weil eine eventuelle Meldepflicht im Raum ist, und dafür plädieren, eine Regel der klugen Stichproben vorzusehen. Ähnlich wie beim Mikrozensus oder bei der Feststellung eines Wahlergebnisses, wo mit relativ wenigen Stichproben ja schon sehr genau erfasst werden kann, was Sache ist. Bereits wenige Minuten nach dem Angriff – das gilt auch für Angriffe im Internet – ließen sich die Art eines jeweiligen Angriffs und die Quelle dokumentieren. Wenn wir einmal die Summe aller täglichen Angriffe und deren Quellen nehmen, dann ist es sicher so, dass, wenn man ein intelligent gewähltes Netzwerk von Partnern und angriffsattraktiven Websites hat – und da sind eben nach unserer Sichtweise der Internetbroker oder das Kreditkartenunternehmen oder eine andere sichtbare Website auch der Bundesregierung deutlich attraktiver, als die einer mittelständischen Bäckerkette in der Provinz – die Art der Angriffe und auch die Quellen durchaus mit einer überschaubaren Anzahl von Stichproben pro Tag erfassbar wären. Ich würde annehmen und unterstellen wollen, dass das der Bundesregierung bzw. Ihnen vom BSI zumindest eine ausreichend gute Übersicht geben würde und es nicht notwendig wäre, den Mittelstand mit mehr als Stichproben zu belasten. Aber Stichproben sollte man schon ruhig auch vornehmen, um der Frage nachzugehen, wie der Mittelstand angegriffen wird und welche Mittel dabei eingesetzt werden. Ich plädiere dafür, vor einer allgemeinen holistischen Regelung erst einmal intelligente Stichproben anzuwenden. Es wurde ja auch angesprochen, dass es wichtig ist, unter den potenziellen Opfern zu differenzieren. Ich hatte Ihnen eingangs bereits eine Klassifizierung genannt und möchte das noch einmal etwas anders formulieren. Es sollte nach der Attraktivität und zwar aus der Außenbetrachtung beurteilt werden, mithin nach dem Wertrisiko in der Innenbetrachtung, was wirklich kaputtgehen kann, ob die Kundendaten sensibel sind, welches Technologie-Know-how vorhanden ist und ob ggf. langkettige Prozesse gestört werden können. Es gibt auch Unternehmen, bei denen nicht viel kaputtgehen kann. Natürlich wäre auch nach der Art der Infrastruktur zu unterscheiden, ob es sich lediglich um einen Stand-alone-Webshop handelt oder ein komplexes System.

Es fiel vorhin auch das Stichwort Entnetzung. Es gibt in der betrieblichen Praxis schon mehr Entnetzung als Sie denken, gerade im Betrieb von Rechenzentren. Das zeitweise Abkoppeln einzelner Segmente, mithin das intelligente Entnetzen, nicht das vollständige, wird schon häufig eingesetzt. Vielen Dank.

Der Vorsitzende: Vielen Dank auch Herr Gutmann und vielen Dank noch einmal an alle Beteiligte, dass Sie den Weg heute zu uns gefunden haben. Das Thema wird uns mit Sicherheit noch weiter begleiten. Sie haben wichtige Impulse gesetzt, mit denen wir uns hier im parlamentarischen Raum und auf Regierungsseite weiter beschäftigen werden. Die Sitzung des Unterausschusses Neue Medien ist hiermit geschlossen. Uns allen noch eine erfolgreiche Woche. Vielen Dank.

Schluss der Sitzung: 14:00 Uhr

Sebastian Blumenthal, MdB
Vorsitzender