19. Wahlperiode

Deutscher Bundestag
Ausschuss Digitale Agenda

Wortprotokoll
der 45. Sitzung

Ausschuss Digitale Agenda
Berlin, den 11. Dezember 2019, 16:00 Uhr
10117 Berlin, Adele-Schreiber-Krieger-Str. 1
Sitzungssaal: MELH 3.101

Vorsitz: Hansjörg Durz, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt 1 **Seite 03**

Öffentliche Anhörung
zum Thema „IT-Sicherheit von Hard- und Software als Voraussetzung für digitale Souveränität“

a) Liste der Sachverständigen auf Drucksache SB19(23)10

b) Fragenkatalog auf Drucksache SB19(23)11

Mitglieder des Ausschusses

	Ordentliche Mitglieder	Stellvertretende Mitglieder
CDU/CSU	~~Beermann, Maik~~ Durz, Hansjörg ~~Hauer, Matthias~~ Heilmann, Thomas Kemmer, Ronja ~~Sauer, Stefan~~ Schipanski, Tankred	Biadacz, Marc ~~Friedrich (Hof), Dr. Hans Peter~~ ~~Kühne, Dr. Roy~~ ~~Nick, Dr. Andreas~~ ~~Schön, Nadine~~ ~~Steineke, Sebastian~~ ~~Whittaker, Kai~~
SPD	~~Eskon, Saskia~~ Herzog, Gustav Korkmaz-Emre, Elvan Mohrs, Falko Zimmermann, Dr. Jens	~~Bartol, Sören~~ ~~Gerster, Martin~~ ~~Kaiser, Elisabeth~~ ~~Klingbeil, Lars~~ ~~Stadler, Svenja~~ Hartmann, Sebastian
AfD	Cotar, Joana Espendiller, Dr. Michael ~~Schulz, Uwe~~	~~Bühl, Marcus~~ ~~König, Jörn~~ ~~Wiehle, Wolfgang~~
FDP	Höferlin, Manuel	~~Sitta, Frank~~ Brandenburg (Südpfalz), Mario
DIE LINKE.	Domscheit-Berg, Anke Sitte, Dr. Petra	~~Movassat, Niema~~ ~~Pau, Petra~~
BÜNDNIS 90/DIE GRÜNEN	Christmann, Dr. Anna Janecek, Dieter	~~Bayaz, Dr. Danyal~~ Rößner, Tabea
fraktionslos	Kamann, Uwe	

Tagesordnungspunkt 1

Öffentliche Anhörung
zum Thema „IT-Sicherheit von Hard- und Software als Voraussetzung für digitale Souveränität“

Der **Vorsitzende Hansjörg Durz** MdB: Ich darf Sie ganz herzlich zu der 45. Sitzung des Ausschusses Digitale Agenda willkommen heißen, zu der öffentlichen Anhörung zum Thema „IT-Sicherheit von Hard- und Software als Voraussetzung für digitale Souveränität“. Ich begrüße meine Kolleginnen und Kollegen aus dem Deutschen Bundestag, die Mitarbeiterinnen und Mitarbeiter und ganz herzlich heiße ich heute natürlich unsere Sachverständigen willkommen:

- **Arne Schönbohm,** Bundesamt für Sicherheit in der Informationstechnik (BSI)
- **Prof. Dr. Michael Waidner,** Fraunhofer-Institut für Sichere Informationstechnologie SIT
- **Isabel Skierka,** European School of Management and Technology GmbH ESMT
- **Oliver Harzheim,** Vodafone GmbH
- **Klaus Landefeld,** Eco-Verband der Internetwirtschaft e.V.
- **Ninja Marnau,** CISPA Helmholtz Center for Information Security
- **Frank Rieger,** Chaos Computer Club e.V.

Zum Ablauf der Sitzung: Die Sachverständigen halten zu Beginn ein ca. fünfminütiges Eingangsstatement, anschließend erhält jede Fraktion ein Zeitfenster von fünf Minuten, in dem die Frage gestellt wird, aber auch die Antwort erfolgen muss. Das heißt, kürzere Frage bedeutet längere Zeit für die Sachverständigen, um auf die Frage zu antworten. Die Sachverständigen antworten also unmittelbar innerhalb dieser fünf Minuten. Bei jeder weiteren Fragerunde wird dasselbe Verfahren angewandt.

Ich darf des Weiteren darauf hinweisen, dass ein Wortprotokoll angefertigt wird und dass die Anhörung live im Internet auf Kanal 2 des Parlamentsfernsehens *gestreamt* wird und anschließend über die Mediathek des Bundestages abrufbar ist. Mikrofone bitte ich jeweils für den Wortbeitrag einzuschalten und diese nach dem Wortbeitrag wieder auszuschalten, damit der nachfolgende Sprecher oder die Sprecherin gehört werden kann.

Gegenstand der heutigen Sachverständigenanhörung ist die Sicherheit digitaler Infrastrukturen. Wenn Einrichtungen des Gemeinwesens, wie zum Beispiel Krankenhäuser oder Kommunalverwaltungen, zum Ziel von Cyberangriffen werden, ist die staatliche Souveränität in ihrem Kern angetastet. Cyber-Attacken auf sogenannte kritische Infrastrukturen können schwerwiegende Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland haben. Dies wirft nicht nur Fragen nach der digitalen Souveränität des Individuums auf. Vielmehr wird die digitale Souveränität auch zum Garant staatlicher Souveränität.

Vor diesem Hintergrund stellt sich zum einen die Frage nach dem Ist-Zustand: Ist die vorhandene IT-Landschaft den Herausforderungen derartiger Angriffe gewachsen? Oder bestehen womöglich Abhängigkeiten, die die digitale Souveränität gefährden? In einem zweiten Schritt muss danach gefragt werden, wie eine möglichst effektive staatliche Cyberabwehr gestaltet sein müsste, um der skizzierten neuen Qualität von Cyber-Angriffen auf Dauer zu begegnen. Dies sollte auch unter dem Aspekt eines internationalen Vergleichs geschehen.

Diese Überlegungen müssen zudem stets von dem Bestreben begleitet werden, einen Ausgleich zu schaffen, damit digitale Souveränität nicht auf Kosten einer offenen und freien Netzarchitektur erzielt wird. Denn ein freies und offenes Internet bildet den Grundstein für eine offene Gesellschaft und fördert den demokratischen Diskurs.

Bei dieser Sachlage interessieren wir Parlamentarier uns insbesondere für die Chancen regulatorischen Handelns. Wie können mithilfe gesetzgeberischen Handelns offene Standards gesichert und eine Abschottung somit vermieden werden? Welche Chancen bestehen, neben der nationalen Perspektive, auf europäischer Ebene?

Heute hat der Ausschuss Digitale Agenda die Gelegenheit, mit den anwesenden Sachverständigen in den Austausch zu treten und ganz sicher auch gute und kluge Antworten auf unsere Fragen zu erhalten.

Wir beginnen nun mit den fünfminütigen

Eingangsstatements und ich darf als ersten Sachverständigen Präsident Schönbohm um seine Darstellung bitten. Herr Schönbohm, Sie haben das Wort.

SV Präsident **Arne Schönbohm** (BSI): Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren Abgeordnete, herzlichen Dank für die Einladung. Ich freue mich, mit Ihnen heute das Thema „IT-Sicherheit von Hard- und Software als Voraussetzung für digitale Souveränität" diskutieren zu dürfen.

Informations- und Cybersicherheit ist eine unverzichtbare Voraussetzung für eine erfolgreiche Digitalisierung. Ihre Gestaltung ist eine nationale Aufgabe in gemeinsamer Verantwortung von Staat, Wirtschaft und Gesellschaft. Im Bereich Wirtschaft und Gesellschaft gehört hierzu natürlich auch die Wissenschaft.

Die zunehmende Digitalisierung aller Lebensbereiche birgt Chancen, aber auch Risiken. Wachsende globale technologische Abhängigkeiten führen dazu, dass die Sicherheit der eingesetzten Informationstechnik von überragender Bedeutung ist. Ziel muss es sein, Risiken zu minimieren und die Vertraulichkeit, Verfügbarkeit und Integrität der eingesetzten IT-Systeme zu gewährleisten.

Als Gestalter der Informationssicherheit in der Digitalisierung spielt das BSI hierbei eine wichtige Rolle. Mit den globalen Wertschöpfungsketten kann die Herkunft von Endprodukten oftmals nicht mehr eindeutig bestimmt werden. So entwickelt zum Beispiel SAP seine Produkte in mehr als hundert Ländern. Einzelne Automobilhersteller haben noch eine eigene Softwareproduktion von ca. 10 Prozent.

Entscheidend ist daher, bei der Detektion von Fehlern und eventuellen Manipulationen, Soft- und Hardware getrennt zu betrachten. Lässt sich bei Software durch Prüfprozesse das Risiko senken, ist es bei Hardware-Bauteilen wesentlich schwieriger, Fehler und Manipulationen zu detektieren. Daher kann nur ein holistischer Ansatz, der nicht nur Produkte, sondern auch Prozesse betrachtet, das Risiko ausreichend minimieren.

Als die Cybersicherheitsbehörde des Bundes gestaltet das BSI Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Die Gefährdungslage ist nach wie vor hoch. Denken Sie an die über 900 Mio. Schadprogramme! Eine neue Angriffsqualität erfordert flexiblere Gegenmaßnahmen der Verteidiger. Ausgefeiltes *Social Engineering* sowie hochwertige Angriffstechniken führen sowohl zu kurzfristigen Arbeits- und Produktionseinschränkungen als auch teilweise zu existenzbedrohenden Komplettausfällen deutscher Unternehmen.

Daher ist eine zentrale Kompetenzstelle des Bundes für Cybersicherheit wichtiger denn je. Als IT-Sicherheitsdienstleister aller Ressorts zu Themen wie KI (Künstliche Intelligenz), 5G und den digitalen Verbraucherschutz, nimmt das BSI diese Rolle bereits erfolgreich wahr. Technologische Souveränität ist eine Voraussetzung für mehr Cybersicherheit, die gleichzeitig Beurteilungskompetenz erfordert und voraussetzt. Hierfür sind Bildungs- und Weiterbildungsangebote notwendig, um verfügbare Technologien besser zu beherrschen. Vor allem hinsichtlich des Einsatzes von Technologien mit hohem Risikopotenzial für sicherheitskritische Bereiche ist die Schaffung von Prüfverfahren und Techniken für eine kontinuierliche Zertifizierung notwendig; denken wir beispielsweise an 5G.

Mit mehr als 1.000 Zertifizierungen nach *Common Criteria* ist das BSI weltweit führend vor allen anderen Stellen aber auch Ländern in der Welt. Ein stringentes und dynamisches Risikomanagement ist die Grundlage für ein möglichst hohes Maß an IT-Sicherheit. Dieses kann in einer globalisierten Welt nicht allein im nationalen Raum erfolgen. Daher strebt das BSI eine europaweit harmonisierte Zertifizierung von einzelnen Komponenten, kritischen Infrastrukturen sowie auch des Gesamtsystems einschließlich der Lieferkette an.

Der *Cybersecuritiy Act* sowie die gestärkte ENISA (Agentur der Europäischen Union für Cybersicherheit) leisten auf europäischer Ebene einen entscheidenden Beitrag zur verbesserten Koordinierung und Harmonisierung von Prozessen und Entscheidungen. Digitale Souveränität in Deutschland und Europa hängt

auch eng mit der Frage nach Produktionsstandorten zusammen. Eigene Wertschöpfungsketten vor Ort, auch von außereuropäischen Herstellern, tragen zur Risikominimierung und damit zur Stärkung des Vertrauens in die Technik bei.

Meine Damen und Herren, auch bei sämtlichen Zukunftstechnologien, sei es 6G oder *Quantencomputing* muss IT-Sicherheit von Beginn an mitgedacht werden. *Security by Design* und *Security by Default* sind entscheidende Voraussetzungen für eine erfolgreiche Digitalisierung. Nur so kann es gelingen, den Schutz des Einzelnen sowie die gesamtgesellschaftliche Resilienz gegenüber Cybergefahren jeglicher Art zu erhöhen. Ich danke Ihnen für Ihre Aufmerksamkeit und freue mich auf die Diskussion.

SV **Prof. Dr. Michael Waidner** (Fraunhofer-Institut für Sichere Informationstechnologie SIT): Vielen Dank für die Einladung und dafür, dass ich hier vortragen und Fragen beantworten darf. Als Wissenschaftler fange ich mit der Definition an, die Sie aber alle schon kennen: Was ist digitale Souveränität? Die Fähigkeit, die Digitalisierung frei und eigenverantwortlich zu gestalten! Hierfür muss es ausreichend viele vertrauenswürdige Quellen für die notwendigen Dienste, Produkte und Technologien geben und natürlich ausreichend gute und vertrauenswürdige Standards.

Die Notwendigkeit der Sicherheit hat Präsident Schönbohm schon sehr eloquent dargestellt, deswegen kann ich mir das sparen. Aber die Frage ist natürlich, wie sicher sind wir eigentlich. Darauf kann man zwei Antworten geben: Wenn wir uns mit anderen Ländern, anderen Geografien vergleichen, würde ich sagen, steht Deutschland eigentlich ganz gut da. Wir sind gut organisiert, wir stehen in der Forschung – nicht nur in meiner Institution, sondern alle Institute zusammen – auch relativ gut da. Die Wirtschaft ist vergleichsweise auch relativ gut geschützt. Tatsächlich werden wir dafür international sogar darum beneidet. Problematisch ist aus meiner Sicht, dass es in Deutschland auf der Anbieterseite eigentlich keine wirklich großen internationalen *Player* gibt. Wenn Sie die IT-Konzerne in Deutschland versuchen abzuzählen, reicht Ihnen typischerweise eine Hand. In Israel, Singapur oder USA ist das anders.

Das war jetzt die rosige Sicht. Wenn man nicht nur vergleicht, sondern *absolut* fragt, wie sicher ist in Deutschland die IT, dann sind Dinge angreifbar. Wenn man etwas ausmisst und kann es quantifizieren, sind drei Viertel aller Dinge angreifbar, wenn man sich nur viel Mühe gibt. Darum will ich es gar nicht weiter ausführen. Aber das ist das große Problem. Wir sind vergleichsweise gut aufgestellt, aber IT ist angreifbar.

Souveränität wiederum kann man auf zwei Ebenen in diesem Zusammenhang betrachten: einerseits auf staatlicher Ebene, andererseits auf Ebene der Wirtschaft und Gesellschaft. Auf der staatlichen Ebene würde ich sagen, Souveränität fängt mit Organisation an. Auch da muss ich sagen, die Sicherheit in Deutschland – einerseits das BSI, aber auch vor allem die Länder in unserem föderalen System – ist gut organisiert.

Welche Sicherheitsinfrastrukturen gibt es in Deutschland? An dieser Stelle sind wir nicht so gut aufgestellt. Wir haben den neuen Personalausweis, wir haben viele Angebote, um Bürgern und Wirtschaft zu helfen, wir haben das BSI als eine Infrastruktur, um zu unterstützen. Aber so etwas wie eine Verschlüsselungsinfrastruktur oder irgendeine ähnlich geartete Struktur, gibt es noch nicht.

Bei den Innovationen und Kompetenzen sieht es wieder besser aus. Es gibt die Agentur für Sprunginnovation in der Cybersicherheit. Wir müssen schauen, wie sich das entwickelt, aber das ist sicher eine gute Idee. Forschung wird gefördert; wir haben gerade das Zentrum ATHENE (Nationales Forschungszentrum für angewandte Cybersicherheit) in Darmstadt eröffnet mit Förderung durch das BMBF. Das wird sehr positiv gesehen. Bei der Aus- und Weiterbildung ist noch einiges zu tun. Der Mangel an Fachleuten in der Industrie, in der Wirtschaft und im Staat ist eklatant und die Universitäten kommen bei weitem nicht nach, die Leute entsprechend aus- oder weiterzubilden.

Ein anderer Punkt an dieser Stelle, der auch nicht perfekt ist, ist die Vergabe durch die öffentliche Hand. Das ist ein altes Thema. Wir machen sehr viel Innovation in Deutschland, in Europa. Wenn einen dann Vergabekriterien dazu zwingen, Dinge

zu kaufen, die man eigentlich gar nicht kaufen wollte, weil man den entsprechenden Dingen keine Priorität geben darf, dann behindert das aus meiner Sicht die Cybersicherheit.

Auf der Ebene der Wirtschaft und Gesellschaft geht es darum, dass wir Optionen brauchen. Die muss man beurteilen, Vertrauen in sie setzen, die Verfügbarkeit muss gesichert sein – idealerweise mit mehr als einer Quelle. Wie funktioniert das, wie beurteilt man Vertrauen? Da geht es um Kompetenzbildung. Wenn ich Dinge analysieren muss, hilft der Zugriff auf den *Source Code* (Quellcode), Open Source an sich hilft tatsächlich nichts. Das ist ein Mythos, der sich dauerhaft hält, aber Open Source an sich, also dass man darauf schauen kann, heißt nicht, *dass* irgendjemand darauf schaut. Tatsächlich gibt es da keinen großen Unterschied. Aber der Zugriff auf den *Source Code* ist wichtig. Standards für die Auditierung braucht man, für Cloud, für Herstellungsprozesse, für die *Supply Chain* (Lieferkette) usw. Das sind alles wichtige Dinge!

Wie schaffe ich Vertrauen? Es gibt Güterabwägungen, einige Fragen gehen auch in die Richtung, was man mit „Hinter- und Vordertüren" macht. Hier muss ich hinsichtlich der Sicherheitsforschung klar sagen, man darf keine Kompromisse an dieser Stelle eingehen. Man sollte immer darauf achten, dass die Sicherheit so hoch wie möglich ist, dass der Bürger, die Wirtschaft und der Staat wirklich geschützt sind. Man muss auch keine Schwachstellen horten, es gibt genug. Es ist wichtig, dass Schwachstellen tatsächlich gemeldet werden, nachdem man sie gefunden hat.

Eine andere Sache ist die Quelle von IT. Woher bekommt man sie. Das ist eine Frage des Risikomanagements. Wenn ich die Wahl zwischen zwei Quellen habe – egal, ob in Deutschland oder weltweit –, muss man schauen, wie unterscheiden sich diese Quellen hinsichtlich der Verträge, des Rechtssystems, des Landes, in dem es hergestellt wurde. Sind es Partner, die eher ähnliche Rechtssysteme wie Deutschland haben oder andere. Dann muss man einfach abwägen. Es gibt viele Initiativen für nationale Lösungen – GAIA-X und ähnliche Projekte –, die ich sehr positiv sehe. Der Aufwand, alles komplett autark zu machen, ist prohibitiv, das ist keine Frage. Umgekehrt, der Aufwand, Dinge in Einzelfällen zu tun, ist nicht so groß, wie man denkt. Da kann man einiges erreichen. Damit ende ich erst einmal, herzlichen Dank.

SVe **Isabel Skierka** (European School of Management and Technology GmbH ESMT): Sehr geehrte Mitglieder des Ausschusses, vielen Dank für die Einladung und die Gelegenheit, meine Gedanken hier mit Ihnen zu teilen zum Thema digitale Souveränität. Ich arbeite am Digital Society Institut der ESMT Berlin. An diesem Institut arbeiten wir eng mit Unternehmen und anderen gesellschaftlichen Organisationen und von Zeit zu Zeit auch Ministerien zusammen. Wir vertreten dabei immer auch die Perspektive der IT-Anwender. Daher möchte ich hier vor allem aus dieser Perspektive antworten.

Vor drei Tagen hat die chinesische Regierung eine Richtlinie erlassen, mit der alle öffentlichen Institutionen dazu angewiesen werden, ausländische Computerausrüstung und Software innerhalb von drei Jahren mit Technologien aus dem Inland zu ersetzen und auszutauschen. Dieser Schritt ist der Beginn einer breit angelegten Strategie. Auf jeden Fall ist das auch eine Form der digitalen Souveränität oder um auch die eigene IT-Sicherheit, vielleicht zumindest im Sinne der Sicherheit vor Hintertüren, in Technologien von ausländischen Herstellern zu schützen. China investiert massiv in seinen Technologiesektor, so dass das Ziel vielleicht gar nicht so unrealistisch sein mag, wie es zunächst scheint.

In Europa und Deutschland sind wir in vielen Bereichen sehr abhängig von Technologien ausländischer Hersteller. Das haben auch meine Vorredner schon erläutert und das habe ich auch in meiner Stellungnahme noch einmal dargelegt. Seit Monaten debattieren wir daher über digitale Souveränität und Konsequenzen für die Sicherheit unserer Technologien und Gesellschaften. Ist das neueste Beispiel aus China – Abschottung – der richtige Weg? Die Antwort ist nein. Hier kommen wir zum Kern, was nämlich digitale Souveränität bedeutet: Digitale Souveränität ist die Fähigkeit zum selbstbestimmten Handeln und Entscheiden im digitalen Raum.

Dafür müssen Gesellschaften, Organisationen und Staaten die wesentlichen Funktionskriterien, der

von ihnen genutzten Informationstechnik kontrollieren können. Das heißt, IT-Sicherheit ist eine notwendige, wenn auch nicht hinreichende, Bedingung für digitale Souveränität. Wie können wir unsere Handlungsfähigkeit und die Beherrschbarkeit von Technologien langfristig sichern? Abschottung ist hier nicht der richtige Weg. Wir müssen bestimmte Abhängigkeiten eingehen, aber durch ausreichende Beurteilungs- und Handlungsfähigkeit ausgleichen.

Welche Möglichkeiten gibt es dafür? Wir müssen massiv Schlüsseltechnologien und Kompetenzen in Europa stärken. Wir müssen Innovation von offenen Technologien fördern und natürlich müssen wir Maßnahmen für die Sicherheit und Vertrauenswürdigkeit von Technologien ergreifen.

Diesem Punkt möchte ich mich noch kurz widmen: Ein großes Problem ist, dass aufgrund der steigenden Komplexität von Systemen selbst und deren Lieferketten, die Beherrschbarkeit von Technologien eher abnimmt und hundertprozentige Sicherheit nicht möglich ist. Was können wir also tun, welche Maßnahmen können wir ergreifen, um zumindest unsere Beurteilungsfähigkeit hier zu verbessern? Wir brauchen zum einen viel stärkere und einheitliche regulatorische Anforderungen an die IT-Sicherheit von Hard- und Software, deren Einhaltung Hersteller und Anbieter auch nachweisen müssen. Dazu gehört auch die Einrichtung standardisierter Prozesse zur Offenlegung von Schwachstellen und zum Management dieser Schwachstellen.

Für Komponenten, die in kritischen Umgebungen eingesetzt werden, sollten entsprechend höhere Anforderungen und natürlich auch eine Pflicht zur Prüfung und Bewertung – in diesem Fall durch eine unabhängige Stelle – gelten. Die Bewertung der Vertrauenswürdigkeit von Schlüsseltechnologien und Technologien, die *safe* die kritischen Funktionen erfüllen, muss daher auch technische und nichttechnische Risiken umfassen. Das beinhaltet beispielsweise das Rechtssystem im Herstellerland oder die Governance-Struktur des Herstellers selbst. Dazu müssen also nicht nur technische Systeme, sondern auch die Hersteller selbst überprüft werden. Hier empfehle ich noch einmal das EU-weite *Risk Assessment* der Cybersicherheit von 5G-Netzwerken.

Zudem sollten die Betreiber von kritischen Systemen zur Einrichtung effektiver Risikomanagementprozesse verpflichtet werden, die Prinzipien wie Redundanz, Verlässlichkeit und Resilienz priorisieren. Fallen also Teile des Systems aus, muss das System funktionsfähig bleiben und auch Komponenten unterschiedlicher Hersteller genutzt werden.

Außerdem brauchen wir auch viel effektivere Plattformen und Maßnahmen zum Informationsaustausch über Risiken und Evaluation, *Best Practices*, und zwar zwischen Herstellern, Anbietern und Anwendern, aber auch zwischen Staat und Wirtschaft allgemein. Staat und Wirtschaft sollten außerdem die Offenheit und Diversität von Technologien fördern, die eine Voraussetzung ist für digitale Souveränität durch Anreize, gegebenenfalls durch Anpassungen im Vergaberecht und Beschaffungsvorschriften und Beschaffungspolitik. Außerdem sollten wir massiv durch Förderprogramme usw. in Innovation deutscher und europäischer Technologieanbieter investieren.

Bei diesen Gedanken belasse ich es jetzt und freue mich auf die Diskussion.

SV **Oliver Harzheim** (Vodafone GmbH): Sehr geehrte Mitglieder des Ausschusses, danke für die Einladung in diese Runde. Investition in digitale Bildung ist ein Schlüssel für digitale Zukunftsfähigkeit. So sagt es eine Kurzstudie der Vodafone-Stiftung zum Thema „mehr Mut zur digitalen Bildung", die im September dieses Jahres erschienen ist. In dieser Studie wird unter anderem die Frage gestellt, was sind die wichtigsten staatlichen Maßnahmen zur Unterstützung von Bürgern und Unternehmen im Rahmen der Digitalisierung. Dabei wird an erster Stelle die umfangreiche Investition in Digitalisierung und Bildung genannt. Mit kurzem Abstand dahinter die umfangreiche Investition in Digitalisierung und Infrastruktur.

Zu beiden Themen wurden in den letzten Jahren sowie auch in der jüngsten Vergangenheit wichtige Weichen gesetzt. Jedoch bedarf es nun einer konsequenten Weiterentwicklung und Umsetzung, um eine digitale Souveränität über die Gesamtheit der Akteure sicherzustellen.

Digitalisierung und Bildung ist die wichtige Basis, um auf der einen Seite die *Awareness* in der Masse zu steigern, Hemmschwellen bei der Digitalisierung abzubauen, aber auch Deutschland langfristig technologisch wieder konkurrenzfähig zu machen. Dafür benötigen wir sicherlich Fachkräfte und müssen insbesondere auch Fachkräfteabwanderung aufhalten.

Dazu möchte ich auf eine sehr interessante Studie des BIGS (Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH) Potsdam verweisen, in der sehr schön herausgearbeitet wird, dass wir in Deutschland gerade auch in puncto *IT-Security* in der Forschung und auch wenn es darum geht, Patente zu erlassen, sehr weit vorne sind – die Produktion dieser Themen aber letztendlich fast immer in den USA, China oder Indien stattfindet. Die Lebensader der digitalen Gesellschaft ist jedoch die technische Infrastruktur. Ihr kommt eine besondere Rolle zu. Es gibt in Deutschland und Europa deutliche Defizite in der Bereitstellung wettbewerbsfähiger Lösungen in vielen Bereichen, auch bei der *IT-Security*.

Initiativen wie GAIA-X, als europäische Cloud-Lösung, gehen aber in die richtige Richtung. Weitere Initiativen in diesem Umfeld müssen folgen und sind wünschenswert. Die aktuelle Diskussion um den Einsatz chinesischer Lieferanten beim 5G-Netzausbau – irgendwann musste ich auf das Thema kommen – macht dieses Dilemma jedoch besonders deutlich. Ein pauschaler Ausschluss chinesischer Lieferanten hat erhebliche Auswirkungen auf den 5G-Ausbau und somit auf die fortschreitende Digitalisierung in Deutschland. Zudem ist es heute in Zeiten globaler Lieferketten, ohnehin sehr schwierig, bei einem System über ein eindeutiges Herkunftsland zu reden. In einem Huawai-Router finden wir zum Beispiel heute in der Regel eine Netzwerkkarte von Broadcom aus den USA, auf dieser eine Platine aus Südkorea, die wiederum einen Chip von Infineon enthält, der in Deutschland produziert wurde. Auf der anderen Seite war gestern zu lesen, dass die chinesische Regierung den Einsatz US-amerikanischer Hard- und Software in Regierungseinrichtungen verboten hat und dementsprechend den Austausch von Millionen HP und Dell plant. Übrig bleibt Lenovo als chinesischer Lieferant, der aber, wenn man ihn aufschraubt, zu 80 Prozent aus amerikanischen Komponenten besteht.

Das sind in der Regel wirtschaftliche Aspekte. Die Sicherheitsdiskussion scheint mir an dieser Stelle oft zu sehr aufgeladen von diesen wirtschaftlichen Aspekten zu sein. Denn aus Sicherheitssicht sind wir heute schon in der Lage, unser Netz umfangreich zu überwachen und gegen Fremdeinwirkung zu schützen. Das ist auch unsere originäre Aufgabe als Provider. Insbesondere an unkritischen Stellen, wie zum Beispiel im Access-Netz, sehen wir daher weder heute noch zukünftig bei 5G eine Gefahr beim Einsatz chinesischer Komponenten.

Regulatorische Maßnahmen können helfen, das Risiko durch gezielte technische Maßnahmen weiter zu senken bzw. das Sicherheitsniveau zu steigern und sind im Rahmen der laufenden Gesetzgebungsverfahren zu treffen. Das IT-Sicherheitsgesetz 2.0, das sich aktuell in der Ressortabstimmung befindet, wird dem Parlament dazu ausreichende Mitwirkung einräumen.

Dabei muss jedoch sichergestellt werden, dass gute und verlässliche Rahmenbedingungen für deutsche und europäische Hersteller geschaffen werden und neue Technologien, wie zum Beispiel Open-RAN zeitnah in den Einsatz kommen, um auch an der Stelle die Diversität der Hersteller zu steigern. Herzlichen Dank.

SV **Klaus Landefeld** (Eco-Verband der Internetwirtschaft): Vielen Dank für die Einladung. Wir hatten ein paar Punkte, die angesprochen werden sollten: einer davon war Souveränität. Digitale Souveränität ist im hohen Maße eine persönliche Fähigkeit, unabhängig Entscheidungen im digitalen Raum zu treffen und selbstbestimmt handeln zu können. Den Bürgern und Bürgerinnen steht dafür zwar ein breites Portfolio an Angeboten und Diensten zur Verfügung und die bestehende Gesetzgebung unterstützt das auch. Es muss aber betont werden, dass jeder Einzelne für die Ausübung selber verantwortlich ist. Es können nicht nur die Betreiber von Diensten und der Staat in der Verantwortung stehen. Hier muss auch im persönlichen Bereich etwas getan werden. Hier gibt es ein erkennbares Defizit.

Die Herausforderung besteht insbesondere darin,

das Bewusstsein für die Konsequenzen des Einsatzes digitaler Technologien zu stärken und Wissen, Anwendung und den Umgang mit digitalen Technologien als gelebte digitale Souveränität zu fördern. Wünschenswert wäre deshalb eine abstrakte Verpflichtung aller Akteure für eine stringente systematische Erhöhung der IT-Sicherheit und somit auch der digitalen Souveränität von Bürgern, Unternehmen und Staat. Eine derartige Verpflichtung sollte sich nicht allein auf die Betreiber kritischer Infrastrukturen erstrecken, sondern vielmehr analog zum Straßenverkehr *alle* Teilnehmer auf ein Mindestmaß an Regeln und sicheren Systemen verpflichten.

Zweiter Punkt: Verschlüsselung. Zentraler Baustein jeder IT-Sicherheitsarchitektur ist Verschlüsselung, sei es zur Speicherung oder auf dem Transportweg. Es kann nicht hingenommen werden, dass derartige Systeme durch den Staat nicht systematisch gestärkt werden, sondern dass staatliche Stellen durch Softwarelücken und/oder andere systematische Schwachstellen Angriffsmöglichkeiten nach deren Entdeckung bewusst offenhalten, um Ermittlungen oder Überwachungsmaßnahmen gegen Einzelne durchführen zu können.

Dieser Ansatz hat zwangsläufig Gefahren für Gesellschaft, Wirtschaft und den Staat, denn ausländische Geheimdienste oder organisierte Kriminalität können diese Lücken ebenfalls jederzeit nutzen. Der heute florierende Handel mit Sicherheitslücken – das ist derzeit so! – weist beim Verkauf neu entdeckter Sicherheitslücken an staatliche Stellen, an Anbieter von *Dual-Use-Software* oder gar Angeboten auf dem Grau- oder Schwarzmarkt für die Sicherheitsforscher einen deutlich höheren Ertrag auf. Das kann nicht die Lösung sein. Eine umgehende Beseitigung von Sicherheitslücken wird dadurch erschwert. Man muss diesen Handel, auch an Staat oder an *Dual-Use-Software*, im Prinzip unterbinden.

Wir sehen eine Meldepflicht staatlicher Stellen für Sicherheitslücken, die bekannt werden, als sinnvoll und erforderlich an. Denn nur so wird das Vertrauen in den Staat hinsichtlich digitaler Technologien auch befördert.

In Sachen Hard- und Software: Das niedrigste Schutzniveau haben wir derzeit mit Sicherheit bei den privaten Nutzern, in der Peripherie, in Routern, bei *Connected Devices* und ähnlichem. Die sind meist am schwächsten geschützt. Interessanterweise werden aber natürlich die Angriffe deswegen genau dafür entwickelt. Das wird aber nicht erkannt oder behoben. Auch sind, anders als Netzbetreiber und Diensteanbieter, die Hersteller und die, die solche Geräte in den Verkehr bringen, bisher nicht in der Verantwortung für IT-Sicherheit einbezogen. Das müsste dringend überdacht werden. Die müssten eigentlich mit in den Prozess integriert werden. Das kann durch IT-Gütesiegel, Zertifikate oder Konformitätskennzeichen passieren. Das kann aber auch nur bei der Orientierung helfen, denn diese Gütesiegel müssten eine Art zeitlichen Faktor haben, damit nicht das trügerische Gefühl einer dauerhaften Sicherheit vermittelt wird. Vielleicht ähnlich einer TÜV-Plakette, die tatsächlich aber auch ein Ablaufdatum hat.

Es stellt sich die Frage, wie eine Zertifizierung in zunehmend von servicegetriebenen Landschaften – Software ist ein Service, Plattform ist ein Service – überhaupt reinpassen kann und wie man so etwas zertifizieren könnte.

Eine interessante Frage ist auch, inwieweit zum Beispiel zwischenstaatliche Verträge oder Verträge zwischen Staaten und einem Hersteller überhaupt etwas in der praktischen Auswirkung für die Sicherheit von TK-Netzen bringen können. Nur weil der Staat einen Vertrag mit einem Hersteller getroffen hat, dürfte das die Betreiber nicht davon abhalten, weiterhin eigene Sicherheitsprüfungen zu machen.

Interessant finden wir an der ganzen Diskussion hier in diesem Teil, dass die Nutzung öffentlicher Netze auch in der Vergangenheit immer als potenziell kompromittierter Übertragungsweg betrachtet wurde; also auch bei analogen Netzen, ISDN-Netzen der Bundespost – in der Vergangenheit gingen wir immer davon aus, dass der Ende-zu-Ende Übertragungsweg kompromittiert ist. Warum das auf einmal bei 5G anders sein soll, dass man nicht Ende-zu-Ende-Sicherheit herstellen muss, ist uns momentan etwas unklar.

Wir haben auch Projekte wie GAIA-X, die sicher sein sollen. Eine der zentralen Diskussion, die wir dort momentan führen, ist die Frage, wie wird

denn staatlicher Zugriff auf die Daten geregelt und wie sieht der Zugriff anderer Staaten auf die Daten aus, die hier in den Cloud-Diensten gespeichert sind. Dabei wieder unter Umgehung sämtlicher Schutzmaßnahmen, die wir momentan kennen oder die wir in unseren Gesetzen derzeit haben. Das passt natürlich nicht zusammen. Es ist eine paradoxe Situation für die Betreiber, dass sie auf der einen Seite Lücken sofort schließen sollen und auf der anderen Seite immer wieder Zugriffsmöglichkeiten schaffen sollen. Dieser Abfluss an Drittstaaten muss natürlich irgendwie aufgehoben werden.

SVe **Ninja Marnau** (CISPA Helmholtz Center for Information Security): Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren Abgeordnete, ich bedanke mich herzlich für die Einladung. Sie haben mir die Frage gestellt, wie ich den aktuellen Zustand der digitalen Souveränität in Deutschland und Europa bewerten würde. Ich möchte mich der Definition meiner Vorredner anschließen, muss aber sagen, dass ich die Gesamtsituation tatsächlich für besorgniserregend halte. Nicht nur wegen der erwähnten Abhängigkeiten in dem Sinne, dass wir keine Hersteller mehr auf internationalem Niveau in Europa haben von Hardware, von Betriebssystemen, von Browsern und sonstigen zentralen digitalen Infrastrukturen, sondern auch, weil wir flächendeckende IT-Unsicherheit in Deutschland und Europa dulden. Es ist tatsächlich so, dass wir keine flächendeckende, sektorübergreifende Regulierung für IT-Sicherheit haben. Die vielleicht am weitesten reichende Norm ist der Artikel 32 DSGVO (Datenschutz-Grundverordnung) und der ist abhängig von der Verarbeitung personenbezogener Daten.

Ansonsten haben wir viel Regulierung für KRITIS (Kritische Infrastrukturen), Regulierung für Medientechnologie, Regulierung für TK-Anbieter, aber es ist immer noch völlig normal, dass Sie in einen Laden gehen und eine komplett unsichere Webcam beispielsweise kaufen können, ohne dass auch nur die geringste Authentifizierungs- oder Sicherheitstechnologie darin enthalten ist. Aufgrund der zunehmenden Vernetzung sind diese *Consumer*-Entscheidungen tatsächlich Entscheidungen, die weitgehende Auswirkungen haben können.

Wie kann man damit umgehen? Der erste Ansatz wäre natürlich tatsächlich zu sagen, wir möchten wieder digitale Souveränität im Sinne von „europäische Hersteller" für zentrale Infrastrukturen. Das ist eher ein langfristiges Ziel, das auch extreme politische Unterstützung und finanziellen Aufwand bedeuten würde. Was kurz- oder mittelfristig ein pragmatischerer Ansatz wäre ist, wieder Kontrolle herzustellen. Fokussieren auf Kontrollier- und Überprüfbarkeit von Technologie, die Marktdiversität zu erhöhen und bei Fragen wie 5G und der Zulassung von chinesischen Anbietern zum Beispiel, eine risikoabhängige Bewertung zu machen und bei der Vergabe schon beachten, welchem Risiko setzen wir uns aus und welche Anbieter wollen wir aufgrund dieser Risikobewertung tatsächlich zulassen.

Ich möchte verschiedene kurz- und mittelfristige Maßnahmen diskutieren, die aus meiner Sicht zu einer Erhöhung einer digitalen Souveränität beitragen könnten. Das wäre im ersten Schritt eine sektorübergreifende Regulierung von IT- und Digitalprodukten, die ein Grund- und Mindestmaß an IT-Sicherheit verlangt. Diese Regulierung sollte sich – wie auch schon mehrfach angesprochen – zum einen auf die Hersteller, aber auch auf die Betreiber erstrecken und eventuell auch auf die Nutzer. Eine solche Regulierung würde dann ausstrahlen in den gesamten zivilrechtlichen Bereich, nämlich auf Haftung, Gewährleistung, möglicherweise Update-Pflichten und könnte tatsächlich wissenschaftliche Paradigmen, wie *Securitiy by Default*, in die Praxis überführen.

Ich würde mir auch wünschen, dass der Staat mehr mit Standardisierungsorganisationen zusammenarbeitet, dass er konsolidiert, wo es Lücken im Standardisierungsbereich im Hinblick auf den Stand der Technik für IT-Sicherheit gibt und dort gezielt Regulierungsaufträge oder Regulierungszusammenarbeit mit den Standardisierungsgremien schafft und diese Regulierungslücken schließt. Damit kleine und mittlere Unternehmen (KMU), die sich darum bemühen IT-Sicherheit zu schaffen, Dokumente und Hinweise haben, was sie tun müssen, um ihre Produkte und ihren Service sicherer zu machen.

Über Vergabe und die Überprüfung von Vergabeverfahren dahingehend, ob sie offen sind

für Open-Source-Angebote, für Fairness gegenüber kleineren europäischen Anbietern, wurde schon viel gesagt, deshalb möchte ich das nicht wiederholen. Wichtiger wäre mir zusätzlich eine umfassende Bildungsstrategie zwischen Bund und Ländern zu schaffen, die darauf ausgelegt ist, digitale Kompetenz über die gesamte Lebenszeit von Menschen zu vermitteln. Das fängt an mit einer gründlichen Schulbildung im Fach Digitalkompetenz und nicht nur Medienkompetenz. Verstehen, wie Technik funktioniert, wie Vernetzung funktioniert, was Handlungen für Konsequenzen haben und wie algorithmische Entscheidungen getroffen werden. Ich denke, wenn wir informierte Nutzer haben, die informierte Kaufentscheidungen treffen können und sich gleichzeitig auf ein Mindestmaß von IT-Sicherheit auf dem Markt verlassen können, haben wir schon einen großen Schritt im Hinblick auf digitale Souveränität getan. Vielen Dank.

SV **Frank Rieger** (Chaos Computer Club e.V.): Vielen Dank für die Einladung. Viele Punkte haben meine Vorredner schon angesprochen. Ich will mich auf ein paar fokussieren, die mir besonders am Herzen liegen:

Wenn man über technologische Souveränität redet, sollte man sich darüber im Klaren sein, was man eigentlich erreichen will. Technologische Souveränität heißt Handlungsfreiheit, und zwar – das ist der Punkt, der bisher weggelassen wurde – auch unter widrigen Umständen. Auch dann, wenn man andere Akteure weltweit hat, die einem gerade nicht freundlich gesinnt sind. Die Situation ist 2019 in gewisser Art und Weise eskaliert, weil wir mehrere Beispiele gesehen haben, wo Akteure, die uns bisher als verbündet oder freundlich erschienen sind, plötzlich unfreundlich wurden. Jüngstes Beispiel war die drohende Stilllegung der Raffinerie PCK Schwedt, weil ein amerikanisches Unternehmen die Industriesteuerung für die Raffinerie liefert und die PCK Schwedt möglicherweise von den Sanktionen der US-Regierung gegenüber russischen Firmen – denen ein Teil der PCK Schwedt gehört –, betroffen ist.

Was im schlimmsten Fall passieren kann ist, dass ein wesentlicher Teil der Energieinfrastruktur, die den gesamten Nordosten Deutschlands versorgt, plötzlich ausgeht, weil wir eine technologische Abhängigkeit haben, über die bisher niemand geredet hat. Es geht nicht nur um Sicherheit, sondern tatsächlich auch wirklich um Verfügbarkeit, um die Möglichkeit, die Kontrolle über das eigene Schicksal, das eigene Geschehen zu haben – Handlungsfähigkeit!

Deswegen finde ich es wichtig, dass wir, wenn wir über Sicherheit reden, dass wir länderunabhängig darüber reden. Das heißt, alle Prozesse, alle Maßnahmen, alles worüber wir reden und nachdenken, sollte sich nicht in dieser Huawei-Diskussion erschöpfen, sondern wir sollten uns überlegen, wie wir Systeme, Prozesse, Anforderungen und Maßnahmen so gestalten, dass sie unabhängig vom Herkunftsland wirken. Sonst lügen wir uns schlicht und ergreifend in die eigene Tasche.

Wenn man sich anschaut, was eigentlich realistisch ist und welche Ziele wir für Deutschland oder Europa erreichen können, dann stehen wir vor dem Problem, dass wir zu spät damit anfangen. Wir haben einen Großteil unserer technologischen Souveränität deswegen verloren, weil es keine Industriepolitik gab, die gesagt hat, wir müssen dafür sorgen, dass wir deutsche oder europäische *Player* in den relevanten Bereichen erhalten. Wir haben viele unserer Industrieunternehmen, die in den relevanten Technologien wichtig und gut waren, an ausländische Investoren verloren oder an irgendwelche Finanzinvestoren. Das heißt, der Ausblick, nachdem agiert wurde, war der einer heilen Welt, in der der globalisierte Markt einfach weiter vor sich hin funktioniert, niemand Technologie als Waffe benutzt und niemand dem anderen den Zugang zu dieser Technologie verweigert. Diese Welt hat aufgehört zu existieren! Wir müssen uns damit abfinden, dass wir in einer Welt leben, wo andere Staaten und auch nichtstaatliche Organisationen wie große Konzerne, durchaus Technologie als Machtmittel einsetzen. Darauf müssen wir uns jetzt einstellen. Da müssen wir uns nichts vormachen, wir müssen dem relativ klar ins Auge blicken.

Das heißt auch, dass der bisherige Anspruch des Staates zu sagen, „das wird der Markt schon irgendwie regeln und wir müssen uns darum nicht weiter kümmern…“ nicht weiter funktionieren wird. Wenn wir technologische Souveränität wollen, erfordert das stringente

strategische Maßnahmen und Investitionen. Investitionen heißt auch, dass wir uns überlegen müssen, auf welchen Gebieten es denn sinnvoll ist, Geld auszugeben. Dazu gehören zwei Dinge: das eine ist Softwarequalität. Wir haben ein Problem damit, dass wir mehr schlechte Software schneller erzeugen, als wir schlechte Software vom Markt bekommen oder die Lücken schließen können. Wir sind immer noch im „Anschwellen der Lawine". Da müssen wir etwas tun und dazu gibt es mehrere Optionen. Eine der Optionen wäre dafür zu sorgen, dass für öffentlich beschaffte Software immer zwingend Zugang zum *Source Code* vorhanden sein muss und entsprechende aktuelle Sicherheitszertifikate vorliegen müssen. Damit ein Marktdruck entsteht, mindestens in diesem Bereich Sicherheit zu erzeugen.

Außerdem brauchen wir gesetzliche Regelungen, die es einfacher machen, die Sicherheit von Systemen zu überprüfen. Dazu gehört unter anderem die Klarstellung, das *Revers Engineering* – genaues analysieren von Systemen – legal sein muss, wenn es zum Zwecke der Sicherheitsüberprüfung geschieht. Eine dritte Sache, die aus meiner Sicht immer noch immens wichtig ist: Das BSI muss unabhängig werden! Das BSI befindet sich in dem Zielkonflikt zwischen seinem Dienstherren, der für die öffentliche Sicherheit zuständig ist – und dafür manchmal *IT-Security* umgehen muss – und seiner Aufgabe, für IT-Sicherheit zu sorgen. Dieser Konflikt muss aufgelöst werden. Dann gibt das auch eine Vertrauensbasis aus der Industrie, die es möglich macht, eine zentrale Stelle zu schaffen, die für IT-Sicherheit in Deutschland möglich ist.

Was den Bildungsbereich betrifft, gibt es das Bund-Länder-Problem. Unser Vorschlag dazu ist, wenn wir Bildungsmaterialien schaffen wollen – für sicheres Programmieren, sicheres Systemdesign, für die Ausbildung auf allen Ebenen – und die als Bund finanzieren, dann werden die Länder sicher die Letzten sein, die diese Materialien nicht benutzen. Denn die Entwicklung ist teuer und die Leute, die die Bildung gerade machen, suchen händeringend nach so etwas. Da wären wir sehr dafür! Vielen Dank.

Der **Vorsitzende**: Vielen Dank. Dann steigen wir in die erste Fragerunde ein.

Abg. **Tankred Schipanski** (CDU/CSU): Herr Vorsitzender, meine Damen und Herren Sachverständige, vielen Dank. Ich denke, das ist ein Thema, bei dem es fraktionsübergreifend sehr viel Übereinstimmung gibt, selbst von CDU-Seite bei dem Sachverständigen des Chaos Computer Clubs, wenn man das sagen darf. Das hat aber auch deutlich gemacht, dass wir Wissenschaftsfreiheit in Deutschland leben. Ich habe mir aufgeschrieben, Helmholtz sagt „Gesamtsituation besorgniserregend" und Fraunhofer stellt fest „wie sicher sind wir – wir stehen gut da". Man kann das ganz unterschiedlich beurteilen.

Ich will drei Sachverständige befragen, ich würde mit Präsident Schönbohm anfangen. Es wurde aufgezeigt, gegenwärtig werden nur Sicherheitsvorfälle gemeldet, die die kritische Infrastruktur betreffen. Die Sachverständigen fordern jetzt, das deutlich auszuweiten. Ich würde gerne wissen, wie Sie das als BSI-Präsident sehen. Und es ging auch um den Handel von Sicherheitslücken. Vielleicht können Sie kurz skizzieren, inwieweit Sie oder das BSI da schon mit einbezogen sind, was solche Sicherheitslücken gegenwärtig betrifft.

SV Präsident **Arne Schönbohm** (BSI): Ja, ich bin für eine Ausweitung der Meldung. Wir haben 252 Meldungen der kritischen Infrastrukturen bekommen. Ich glaube, da geht noch deutlich mehr. Wir bekommen auch eine Vielzahl von Meldungen aus der Wirtschaft. Verpflichtend wäre deutlich von Vorteil.

Ihre zweite Frage kann ich leider nicht beantworten. Das liegt daran, dass wir an einem möglichen Handel oder sonstigen Aktivitäten mit Sicherheitslücken nicht eingebunden sind. Wenn uns eine Sicherheitslücke bekannt ist, informieren wir die Hersteller, die die Lücke dann zu schließen haben.

Abg. **Tankred Schipanski** (CDU/CSU): Dann knüpfe ich an bei Frau Skierka, die gesagt hat, man möge Maßnahmen zum Austausch über Schwachstellen oder Risiken schaffen. Sie haben Plattformen vorgeschlagen. Vielleicht können Sie das konkretisieren, was Ihnen da vorschwebt.

SVe **Isabel Skierka** (European School of

Management and Technology GmbH ESMT): Auf nationaler Ebene bestehen sehr viele unterschiedliche Initiativen zum Austausch von Informationen zwischen Staat und Wirtschaft. Die sind sehr heterogen und müssen gebündelt werden. Ich habe gesehen, es soll ein Cyberbündnis geben. Die Frage ist, wird das etwas bringen. Aber wir müssen auf jeden Fall diese öffentlich-privaten Partnerschaften konsolidieren und vor allem *Threat Intelligence* (Bedrohungsinformationen) besser austauschen zwischen Staat und Unternehmen. Die Unternehmen müssen auch wichtige Informationen erhalten.

Abg. **Tankred Schipanski** (CDU/CSU): Dann darf ich überleiten zu Herrn Professor Waidner: Sie haben die Vergabe durch die öffentliche Hand angesprochen und dargestellt, dass es dort eigentlich dazu kommt, dass Sie unsichere Produkte erwerben müssen durch Gründe, die Sie uns vielleicht noch einmal aufzeigen. Können Sie das bitte konkretisieren?

SV **Prof. Dr. Michael Waidner** (Fraunhofer-Institut für Sichere Informationstechnologie SIT): Das kann ich gerne machen. Aber nur kurz, weil Sie meinten, Helmholtz und Fraunhofer würden sich widersprechen: Im Vergleich stehen wir nicht schlecht da, aber absolut stehen alle schlecht da. Ein feiner, aber wichtiger Unterschied.

Was ich gemeint habe ist, wir arbeiten viel mit Startups im Bereich Cybersicherheit. Wir päppeln die gerade hoch. Es gibt sehr oft die Situation, dass in Vergabeverfahren aufgrund von europäischen Ausschreibungen und sehr umfangreichen Regelungen eine große Lösung eingekauft werden muss, weil sie die günstigste war und teure, mit Forschungsgeld entwickelte Lösungen nicht zum Zuge kommen. An dieser Stelle sollte man es irgendwie hinbekommen, dass tatsächlich *diese* Lösungen den Vorrang erhalten. Die Lösungen, die mit Forschungsmitteln erstellt wurden und gut sind, haben keinen guten Marktzugang in Europa. Einfach, weil das europäische Vergaberecht große Firmen favorisiert, etablierte Firmen, die mit diesen Prozessen umgehen können. Man muss dann typischerweise oftmals billigste Lösungen nehmen. Die Erfahrung zeigt, dass auf diese Art und Weise kleine Firmen ins Hintertreffen kommen, die die guten Lösungen hätten, die in Europa und Deutschland entwickelt wurden.

Abg. **Tankred Schipanski** (CDU/CSU) noch eine Frage an Herrn Rieger: Sie haben das mit den Sicherheitslücken und dem Handel aufgegriffen. Vielleicht könnten Sie noch einmal skizzieren, wie der Staat gegenwärtig darin involviert ist.

SV **Frank Rieger** (Chaos Computer Club e.V.): Wie der Staat konkret darin involviert ist, ist etwas schwierig herauszubekommen, weil wir mittlerweile eine Vielzahl von Institutionen haben, deren Aufgabe das Brechen von *IT-Security* für die Aufgaben der öffentlichen Sicherheit ist. Was da gerade konkret passiert, entzieht sich meiner Kenntnis, auch inwieweit ein Ankauf von Sicherheitslücken stattfindet und eigene Entwicklungen von Sicherheitslücken priorisiert werden. Das findet alles im geheimen geschützten Bereich statt. Darum ist es schwierig, da hineinzugucken.

Klar ist der Grundsatz, dass der Staat in solche Aktivitäten nicht involviert sein sollte, sondern andere Mittel und Methoden präferieren sollte, um den Aufgaben der Strafverfolgung nachzugehen. Dieser Grundsatz steht nach wie vor, denn in dem Augenblick, wo der Staat anfängt, in diesem Markt zu agieren, treiben wir die Preise hoch und sorgen dafür, dass Sicherheitslücken nicht mehr geschlossen werden. Da ist es in jedem Fall erforderlich, Grundsätze zu schaffen und zu sagen, der Staat sorgt für Sicherheit, und zwar im Sinne von IT-Sicherheit. Was die öffentliche Sicherheit angeht, müssen und können andere Mittel und Wege gefunden werden.

Abg. **Gustav Herzog** (SPD): Vielen Dank, Herr Vorsitzender. Zunächst auch von Seiten der SPD-Fraktion ganz herzlichen Dank an die Sachverständigen, dass Sie uns zur Verfügung stehen. Ich will es Ihnen nicht „androhen", sondern versprechen, wir werden uns mit dem Thema sicherlich in den nächsten Wochen und Monaten noch häufig beschäftigen. Denn für uns steht die IT-Sicherheit und die Souveränität für diese Technik ganz oben auf der Tagesordnung und wir haben auch Zeitdruck im Hinblick darauf, dass zumindest die öffentlichen TK-Netze ausgebaut, aufgerüstet werden sollen im Hinblick auf 5G. Ich glaube, das gibt der ganzen Debatte

noch einmal eine besondere Bedeutung.

Was ich feststelle, wie mein Vorredner von der Union, es gibt hier eine große Übereinstimmung, dass wir insgesamt die Sicherheitsanforderungen erhöhen müssen im Hinblick auf die Technik, das Personal, die Organisation sowohl bei den Herstellern der Komponenten als auch bei den Betreibern der Netze und auch beim Staat. Wenn ich von Sicherheit und Staat rede, geht natürlich meine erste Frage an Präsident Schönbohm: In dem gemeinsamen Papier der drei Ministerien bezüglich der 5G-Sicherheitsbewertung steht, dass wissentliches Vorliegen missbräuchlich nutzbarer Schwachstellen und Hintertüren zum Ausschluss des Produktes oder gar des Herstellers führen kann.

Ich bin über die Worte „missbräuchlich nutzbar" gestolpert, weil Sie für die Sicherheit zuständig sind. Heißt das, „nicht missbräuchlich nutzbare Hintertüren" wären dann für das BSI zu akzeptieren?

SV Präsident **Arne Schönbohm** (BSI): Ich muss zunächst einmal nachschauen, auf welcher Seite das in dem Papier steht, damit ich erst einmal nachlesen kann, was Sie gerade zitiert haben –. Es ist relativ einfach: Wir machen eine Vielzahl von Source-Code-Analysen. In Bonn hat Cisco vor einer Woche ein neues Labor (Technology Verification Service Center) eröffnet. Auch dort werden Source-Code-Analysen durchgeführt. Das, was wir in der Regel entdecken sind schlicht und ergreifend qualitative Mängel, und zwar bei allen – querbeet. Dann ist zu prüfen, wird das bewusst ausgenutzt oder nicht. Das sind Themen, die im öffentlichen Raum zu diskutieren, schwierig ist. Hier bitte ich um Verständnis.

Abg. **Gustav Herzog** (SPD): Vielen Dank, deshalb werde ich auch keine weitere Frage stellen mit Blick auf Australien, wo beschlossen wurde, dass TK-Betreiber und Hersteller entsprechende Hintertüren vorsehen müssen.

Meine zweite Frage geht an Frau Skierka: In der Frage der Vertrauenswürdigkeit für solche Komponenten schreiben Sie in Ihrer schriftlichen Stellungnahme, dass das Herstellerland alleine kein Grund sein kann. Aber Sie schreiben auch, das politische Umfeld ist ein klarer Risikofaktor. Daher meine Frage: Wer stellt Verstöße gegen diese Vertrauenswürdigkeitsanforderungen fest? Wer sanktioniert? Weil, wenn es nicht nur eine Haftungsfrage ist, sondern ein Hersteller aus einem bestimmten Land ausgeschlossen wird, hat das auch eine staatliche Dimension. Wer sollte nach Ihrer Auffassung diesen Verstoß gegen die Vertrauenswürdigkeitskriterien feststellen? Der Betreiber, der in der Haftungsfrage ist oder der Staat?

SVe **Isabel Skierka** (European School of Management and Technology GmbH ESMT): Vielen Dank für die Frage. Ich denke, der Betreiber hat hier nicht die Aufgabe, die politischen Risiken eines Herstellerlandes einzuschätzen, sondern das ist eine politische Entscheidung, eine geopolitische Entscheidung oftmals. Insofern sehe ich hier die Politik in der Verantwortung. Und zwar nicht das BSI, sondern diese Entscheidung sollte zum Beispiel der Bundessicherheitsrat treffen hinsichtlich der Vertrauenswürdigkeit eines Herstellerlandes und des politischen und rechtlichen Umfeldes, in dem ein bestimmter Hersteller operieren muss. Denn dabei geht es auch oft um geheimdienstliche Gesetze. So viel erst einmal dazu. Das könnte man über das IT-Sicherheitsgesetz, § 9 beispielsweise, noch regeln.

Abg. **Gustav Herzog** (SPD): Meine letzte Frage geht an Professor Waidner. Das ist die spannende Diskussion zwischen internationalen Lieferketten und Abschottung. Halten Sie es durch ein risikoorientiertes Management überhaupt für möglich, dass wir die Komponenten bis hin zur Anwendungssoftware prüfen können?

SV **Prof. Dr. Michael Waidner** (Fraunhofer-Institut für Sichere Informationstechnologie SIT): Ich sehe keine Alternative zu dem risikobasierten System, wie es Frau Skierka gerade skizziert hat. Es wird nie hundertprozentige Sicherheit geben. Das ist das Beste, was wir haben. Man muss es konsequent durchsetzen.

Abg. **Dr. Michael Espendiller** (AfD): Dank an die Sachverständigen für die Berichte. Ich hätte einige Fragen an Herrn Harzheim. Er ist hier sozusagen der Mann aus der Praxis und kennt die Marktsituation ganz gut. In meinem ersten Fragenkomplex möchte ich folgende Frage stellen: Wären europäische und südkoreanische Anbieter überhaupt in der Lage, in ausreichender Menge 5G-Komponenten herzustellen, um die

chinesischen Anbieter zu ersetzen, wenn wir – rein hypothetisch – sagen, Huawei hat einen kompletten Ausschluss?

Hätte das Qualitätseinbußen im Netz, wenn man Huawei herausnehmen würde und die alternativen Anbieter nimmt? Gibt es dadurch zeitliche Verzögerungen und wie hoch wären die Mehrkosten beim Aufbau?

SV **Oliver Harzheim** (Vodafone GmbH): Ob europäische Hersteller in der Lage sind Huawei zu ersetzen, dazu gibt es einmal die Meinung der Hersteller und einmal die Meinung der Betreiber. Wenn wir das als europäisches Thema sehen, dann behaupte ich, dass sie das auf die Schnelle nicht sind. Wenn wir in Deutschland oder Europa über einen Ausschluss reden, dann betrifft das eine große Menge von Equipment, das letztendlich umgebaut werden muss. Das kann nur mit sehr großer zeitlicher Verzögerung geschehen. Das 5G-Netz, das derzeit aufgebaut wird, ist ein Hybrid-Netz und kein reines 5G-Netz. Es basiert auf vorhandener 4G-Technologie. Da grundsätzlich die Provider einen sogenannten Single-RAN-Ansatz verfolgen, bedeutet das, dass man immer den gleichen Hersteller auf vorhandene Technologie aufbaut. Einfach um Kompatibilitäts- oder Qualitätsverluste auszuschließen. Das würde für alle Provider bedeuten, dass sie erst einmal die komplette 3G- und 4G-Technolgie mit diesen Lieferanten zurück- bzw. umbauen müssten, bevor Sie dann 5G-Technologie ausbauen würden.

Das ist im Prinzip auch direkt die Antwort zum Thema Qualität und Laufzeiten. Man kann sich natürlich vorstellen, dass wir bei den heutigen Anteilen des Equipments eine unheimliche Vorlaufzeit haben, um erst einmal das vorhandene Equipment umzubauen, bevor wir dann in den 5G-Ausbau einsteigen. Wenn man das in Jahren beziffern möchte, haben wir hochgerechnet, dass das für uns ein Zeitraum von vier bis fünf Jahren bedeutet, den wir als Vodafone benötigen würden, um das vorhandene Equipment umzubauen und 5G *ready* zu machen.

Wenn man das auf alle Provider hochrechnet und auf limitierte Kapazitäten – nicht nur, wenn es um die Komponenten geht, sondern auch um limitierte Kapazitäten bei den *Skills*, die den Umbau letztlich auch vornehmen können –, da kann man sich vorstellen, dass es sich im *Worst Case* unter Umständen noch länger hinauszögern kann.

Dann zu der Frage der Qualitätseinbußen. Sicherlich geht so ein Umbau immer mit Qualitätseinbußen einher. Das ist auch klar. In welchem Rahmen die liegen und wie man sie eindämmen kann, würde dann in letzter Instanz erst die Praxis zeigen. Sicherlich macht jeder Provider regelmäßig Benchmarks, in denen die einzelnen Hersteller, Komponenten und auch die Komponenten je Einsatzzweck miteinander verglichen werden. Wir stellen im Moment immer noch fest, dass wir bei Komponenten von Huawei insbesondere dann, wenn wir sie im *Radio Access Netzwerk* draußen an den Masten einsetzen, immer noch einen deutlichen Qualitätsvorsprung haben.

Es ist absehbar, dass die anderen aufholen. Das sehen wir auch, aber den Qualitätsvorsprung gibt es heute noch und es gibt auch immer Aspekte, die nicht zu vernachlässigen sind. Wir stellen zum Beispiel fest, dass Komponenten im RAN von Huawei wesentlich weniger Strom verbrauchen. Wenn man das auf ein großes Netz umrechnet, kommen atemberaubende Zahlen raus, allein in puncto Stromverbrauch. Das ist der eine Kostenfaktor. Aber sicherlich ist der Umbau insgesamt ein Kostenfaktor. Ich kann jetzt keine Zahlen nennen, was es kostet ein komplettes oder ein halbes Netz umzubauen. Ich denke, die Quoten der Mobilfunkprovider wie Huawei im Vergleich zu Ericsson oder Nokia, die im Netz verbaut sind, sind bekannt. Auch wieviel Masten die Provider in Deutschland einsetzen ist bekannt. Da kann man ungefähr hochrechnen, dass wir hier über sehr große Summen reden, die letztendlich ein solcher Umbau kosten würde.

Abg. **Manuel Höferlin** (FDP): Danke, Herr Vorsitzender, auch von uns vielen Dank an die Sachverständigen für die ausführlichen Stellungnahmen. Zuerst eine Frage an Herrn Landefeld: Es geht um ein konsequentes Schwachstellenmanagement. Wie stellen Sie sich das konkret vor? Sollte der Staat alle Schwachstellen verpflichtend melden, egal welche, wo und wie, egal, ob sie missbräuchlich oder nicht missbräuchlich verwendet werden?

Zweite Frage: Das angesprochene Recht auf

Verschlüsselung, wie wir es auch selbst fordern, erhöht auch die IT-Sicherheit durch den Nutzer selbst, weil er selbst durch das Recht auf Verschlüsselung für sichere vertrauenswürdige Kommunikation sorgen kann. Haben Sie eine Idee, wie das in der Praxis mit den Eingriffsbefugnissen ist, die Sie aus verschiedenen Gesetzen verpflichtet sind, bereit zu halten?

SV **Klaus Landefeld** (Eco-Verband der Internetwirtschaft): Schwachstellenmanagement: Wir sehen das so, dass konsequent jede Schwachstelle, das hieße eine systematische Schwachstelle oder eine Softwarelücke, ein Fehler in der Software, gemeldet werden müsste, und zwar immer. Weil nur so die Sicherheit aller sichergestellt werden kann. Das Problem besteht darin, dass bei Ermittlungsmaßnahmen gegen einzelne, die Sicherheit *aller* gefährdet wird. Jeder kann diese Schwachstelle ausnutzen, egal ob der am anderen Ende der Welt sitzt oder zur organisierten Kriminalität gehört. Typicherweise sind die Firmen, die diese Schwachstellen ankaufen – die können mehrere Leute kaufen – meistens Firmen, die Softwareprodukte für Staaten liefern und die dort auch wieder zur Überwachung eingesetzt werden. Bei denen kann eine große Zahl von Ländern einkaufen, so dass diese Schwachstellen durchaus auch anderen Stellen bekannt sind. Damit holt man sich das quasi durch die Hintertür wieder rein.

Die Definition einer Schwachstelle, das ist vielleicht hier das Problem. Es werden oft Sachen, die für Wartungszugänge oder Port, die offen sind, weil sie von Netzbetreibern benötigt werden, teilweise als Schwachstelle identifiziert. Das kann aber Absicht sein, darum müsste man vielleicht an der Definition arbeiten. Manchmal ist es nicht sinnvoll, dass es offen ist und könnte auch aus der Entfernung ausgenutzt werden, was nicht so gedacht ist. Das ist dann das, was als Schwachstelle rausging. So etwas kommt vor.

Das kann man aber auch systematisch schließen. Als Provider findet man so etwas manchmal und dann wird es im Sicherheitskonzept behoben. Dann wird das Ganze korrigiert. Das ist aber nichts, wo man die Software ändern müsste, sondern da werden tatsächlich Zugangsmöglichkeiten eingeschränkt oder ein paar Komponenten vorgesehen.

Zum Recht auf Verschlüsselung: Verschlüsselung ist im Moment die einzige Sicherheitsmaßnahme, die wir kennen. Das ist bei der Übertragung Standard. Es werden heute so gut wie alle Übertragungen verschlüsselt – wir sehen das bei uns am Netzknoten. Der Verschlüsselungsgrad ist mittlerweile auf zwei Drittel angestiegen und steigt weiterhin steil an. Es ist so gut wie alles, was Individualkommunikation ist, von Ende-zu-Ende verschlüsselt. So dass sichere Verschlüsselungsmaßnahmen elementar sind. Das ist auch die einzige Verteidigung, die wir momentan kennen. Dieses Recht darauf, Verschlüsselungsmaßnahmen anwenden zu können, ist daher auch elementar, um selbst Souveränität herstellen zu können.

Mittlerweile wird selbst von Strafverfolgungsbehörden nicht mehr davon ausgegangen, dass das Brechen von Verschlüsselungen oder unsichere Verschlüsselungsmethoden die Wahl wären. Man findet eher Methoden, die den Zugang auf Quellsysteme herstellen sollen. Man sieht das durch Vorschläge wie *Ghost Protocol* (ein Vorschlag des Government Communications Headquarters – GCHQ): ein Teilnehmer soll zu einer Kommunikation hinzugefügt werden, wo dann Diensteanbieter etwas ausleiten.

Selbst im Ausland ist das nicht mehr der Weg, zu sagen, wir brauchen geschwächte Verschlüsselung, sondern man geht grundsätzlich davon aus, dass man Umgehungsmethoden für die Verschlüsselung braucht. So dass eigentlich *starke* Verschlüsselung im Moment der einzige Weg ist.

Abg. **Manuel Höferlin** (FDP): Aufgrund der Zeit vielleicht nur eine Frage an Herrn Schönbohm. Mich würde interessieren, wie viele Schwachstellen Ihnen von anderen staatlichen Behörden und nicht nur aus der Wirtschaft gemeldet worden sind. Ich nehme jetzt mal exemplarisch eine raus: Wie viele Schwachstellen hat Ihnen ZITiS gemeldet im letzten Jahr?

SV Präsident **Arne Schönbohm** (BSI): Das kann ich in diesem Kreis hier nicht so sagen. Ich kann nur sagen, wir haben…

Abg. **Manuel Höferlin** (FDP): Hat sie denn welche gemeldet, sind es mehr als Null gewesen?

SV Präsident **Arne Schönbohm** (BSI): Tut mir leid!

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ich mache mein Dankeschön an alle mal sehr kurz und gebe Ihnen drei Sekunden, um die Frage „mit mehr als Null" mit Ja oder Nein zu beantworten.

SV Präsident **Arne Schönbohm** (BSI): Ich kenne keine Dinge, die ZITiS uns diesbezüglich gemeldet hat. *Ich* kenne keine.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Dürften Sie es uns sagen, wenn Sie es wüssten?

SV Präsident **Arne Schönbohm** (BSI): Ja, natürlich. Wir schließen alle möglichen Schwachstellen. Von daher weisen wir die Hersteller darauf hin, diese zu schließen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Dann hätte ich eine Frage an Ninja Marnau: Mich würde interessieren, da Sie sich auch mit der IT-Sicherheitsforschung befassen, ob Sie uns etwas zu den aktuellen Rahmenbedingungen im Bereich der IT-Sicherheitsforschung sagen können, insbesondere, was die aktuellen, aber auch geplanten Strafrechtsveränderungen angeht. Wie wirkt sich das auf die Sicherheitsforschung aus? Gibt es Einschränkungen, die man vielleicht nicht unbedingt haben will?

SVe **Ninja Marnau** (CISPA Helmholtz Center for Information Security): Es ist tatsächlich so, dass wir beobachten, dass das aktuelle Strafrecht *Chilling Effects* auf unsere Forschung hat. Dass wir bestimmte Maßnahmen und Instrumente nicht in dem Umfang in Deutschland verwenden, wie das unsere ausländischen Kollegen tun, um Sicherheitsforschung durchzuführen. Auf bestimmte Sachen verzichten wir einfach, zum Beispiel auf großflächige Überwachung des gesamten Internetverkehrs, um DDoS-Attacken frühzeitig zu erkennen. Wir verzichten aus Datenschutzgründen und auch aus strafrechtlichen Gründen, um nicht Teil eines *Botnet* zu werden. Nur als Teil eines *Botnet* kann man vernünftig beobachten, wie ein *Botnet* operiert.

Wir beobachten auch mit Sorge verschiedene Vorschläge zur Erweiterung des aktuellen Computer-Strafrechts, zum Beispiel den digitalen Hausfriedensbruch. All diese Paragrafen, die eine sehr vernünftige Intension haben, um Computerkriminalität abzuwehren, sehen keine Ausnahmen vor für IT-Sicherheitsforschung. Als IT-Sicherheitsforscher müssen wir oftmals agieren wie Kriminelle, um Systeme ausreichend zu verstehen.

Ein weiterer Punkt ist die Berechtigung zum *Revers Engineering*: Aktuell ist die rechtliche Situation, wenn wir uns Systeme in der Tiefe anschauen wollen, um Sicherheitslücken zu erkennen und zu testen, extrem unsicher. Wir haben jetzt das geheime Schutzgesetz, was eine rechtliche Änderung gebracht hat. Aber es ist noch unklar, ob das als strafrechtlicher Rechtfertigungsgrund ausreichend wäre, wenn wir uns Codes anschauen und damit in gewisser Weise Urheberrechte verletzen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Vielen Dank. Ich würde noch eine Frage anschließen, und zwar haben Sie in Ihrer Stellungnahme geschrieben, dass aus dem IT-Grundrecht, das vom Verfassungsgericht 2008 festgeschrieben worden ist, eine staatliche Schutzpflicht abgeleitet werden kann und Gesetzgeber im Rahmen ihrer Gewährleistungspflicht auch regulative Maßnahmen ergreifen sollten. In Ihrem Bericht sind Sie auf einige davon eingegangen. Ich wüsste gerne, welche solcher Maßnahmen wären das aus Ihrer Sicht?

SVe **Ninja Marnau** (CISPA Helmholtz Center for Information Security): Es geht darum, ob aus meiner rechtswissenschaftlichen Sicht, das Untermaßverbot es gebietet, dass der Gesetzgeber tatsächlich regulativ eingreift, um die IT-Sicherheit zu erhöhen und damit das Grundrecht auf Gewährleistung von Integrität und Vertraulichkeit von informationstechnischen Systemen für den gesamten Markt und alle Bürger zu gewährleisten. Genau das würde ich so vertreten. Deshalb habe ich auch so stark darauf hingewiesen, dass es aktuell gar keine sektoral übergreifende und generelle Pflicht zu IT-Sicherheitsmaßnahmen gibt. Es knüpft immer an bestimmte Sektoren oder an die Verarbeitung personenbezogener Daten an, aber nicht an das Herstellen von IT-Systemen oder den Betrieb von IT-Systemen. Das heißt, wir haben ganz große Schutzlücken an dieser Stelle, vor allem haben wir weder die Hersteller noch die Nutzer im Blick, sondern aktuell immer nur die Betreiber.

Weitere Punkte wären tatsächlich eine Konsolidierung des Computer-Strafrechts, eine Konsolidierung des Vergaberechts, worüber wir hier schon viel gesprochen haben, dass es mehr Fairness für Open-Source-Anbieter und nationale KMU-Anbieter gibt und dass diese sich an IT-Vergaben überhaupt sinnvoll beteiligen können.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Vielen Dank. Ich hätte noch eine Frage an Frank Rieger. Welchen Änderungsbedarf gibt es im Bereich des Verteidigungsministeriums und seiner IT-Infrastruktur in Bezug auf eine Verbesserung der IT-Sicherheit?

SV **Frank Rieger** (Chaos Computer Club e.V.): Das Problem beim Verteidigungsministerium ist, dass *Cyber* jetzt als der neue Kampfraum definiert wurde, während mir vor zwei, drei Jahren ein General sagte, „wissen Sie, solange ich über unser IT-System nicht einmal erfolgreich Toilettenpapier bestellen kann, wenn ich welches brauche, brauche ich auch keine Cybereinheiten". Ich denke, dieses Problem, mit großen gewachsenen alten IT-Infrastrukturen – wie beispielsweise beim Verteidigungsministerium – aufzuräumen, ist nach wie vor da, besonders im staatlichen Bereich. Es ist keine einfache Aufgabe und wird sich auch nicht dadurch lösen lassen, dass man verstärkt auf Offensive setzt, also auf Cyberangriffseinheiten, sondern nur dadurch, dass man Defensive systematisch betreibt und die Infrastruktur im Zweifel neu baut, und zwar nach den Kriterien von sicherer Infrastruktur.

Abg. **Tabea Rößner** (BÜNDNIS90 /DIE GRÜNEN): Vielen Dank auch von unserer Seite, dass Sie sich heute die Zeit genommen haben. Ich finde es ist eine sehr interessante Runde. Es ist schon das eine oder andere zu Sicherheitslücken und auch der Diskrepanz bei der Bundesregierung gesagt worden, was das Offenhalten oder den Handel angeht und gleichzeitig die nicht eingelöste Ankündigung, wir wollen Verschlüsselungsland Nummer eins werden.

Meine Frage an Herrn Rieger: Es wurde auch über die Meldepflicht gesprochen. Halten Sie die für zwingend erforderlich und auch in der Form, wie von Herrn Landefeld ausgeführt wurde? Wie kann der Staat dafür sorgen, dass Technologie besser auf Lücken und Hintertüren überprüfbar wird? *Open Source* wurde auch angesprochen. Warum hat sich das in der Verwaltung, auch auf Bundesebene, noch nicht wirklich durchgesetzt und was muss aus Ihrer Sicht zwingend Eingang in die Reform des IT-Sicherheitsgesetzes finden?

SV **Frank Rieger** (Chaos Computer Club e.V.): Was die Frage angeht, was der Staat dazu beitragen könne, damit Sicherheitslücken schneller geschlossen werden: Aus meiner Sicht ist der Staat der einzige Akteur, der dafür sorgen kann, dass die Rahmenbedingungen sich dahingehend ändern, dass es zum einen Marktdynamiken gibt, die dafür sorgen, dass Sicherheitslücken schneller geschlossen werden bzw. gar nicht erst auf den Markt kommen und zum anderen auch Mindeststandards zu setzen.

Was wir uns immer noch fragen, warum kann ich mir in einem Elektromarkt ein Tablet kaufen, kann aber keinerlei irgendwie geartete Hinweise darauf entdecken, wie sicher dieses Gerät ist. Ich kann weder sehen, wie oft man dafür Software-Updates bekommt, noch ob die Software auf diesem Gerät gut ist, oder dass irgendetwas darauf hinweist, dass es mal geprüft wurde. Nichts davon! Der Kühlschrank direkt daneben hat ein Energieausweislabel, wo drauf steht, wie viel Strom er verbraucht und bei der Waschmaschine, wie viel Wasser sie verbraucht usw.

Wir müssen dahin kommen, dass solche abstrakten Kriterien, wie IT-Sicherheit, definierbar und für alle, die IT-Systeme kaufen – sowohl in der Wirtschaft als auch für die Endverbraucher – nachvollziehbar sind. Damit würden wir einen großen Beitrag dazu leisten. Was dazu notwendig ist, ist die Mindeststandards zu definieren. Diese Mindeststandards müssen aus unserer Sicht dynamisch sein. Es kann nicht sein, dass wir das *Common-Criteria*-Ungetüm fortschreiben, was rund zweieinhalb Jahre, wenn Sie Pech haben, Prüfungszeit nach sich zieht, um so ein Produkt auf dem Markt zu bringen. Wir brauchen eher *turnaround*-Zeiten von zwei Monaten.

Was es dazu braucht ist, dass sich die Branchen analog zu dem, was bereits im KRITIS-Bereich passiert oder angefangen wurde, zusammensetzen und sagen, wir definieren einmal Mindeststandards für IT-Sicherheit in unseren Branchen. Diese Standards können dann zur Grundlage werden, zum einen für *Labeling*

(Kennzeichnung) und zum anderen aber auch für Haftung und Versicherung.

Die Frage der besseren Überprüfbarkeit: Momentan ist das Problem, dass es für Sicherheitsforscher sehr schwer ist, zum Teil auch sehr riskant ist, mit Unternehmen zu kommunizieren, bei denen Sicherheitslücken gefunden wurden, sowohl in Produkten als auch in Services. Da haben Sie in der Regel die Rechtsabteilung am Hals. Wir vom Chaos Computer Club machen es, weil wir als Institution ein dickeres Fell haben und uns nicht abwimmeln lassen. Meistens funktioniert es zu sagen „Guten Tag, Chaos Computer Club, Sie haben ein Problem!". Dann hören die uns zu. Aber als individueller Sicherheitsforscher haben Sie gleich die Rechtsabteilung oder einen Rechtsanwalt am Hals. Passiert immer wieder. Da braucht es eine gesetzliche Regelung, die klarstellt, dass Betreiber und Hersteller von Systemen in der Haftung sind, sich aktiv um ihre *Security* zu kümmern und mit Sicherheitsforschern auch ordentlich zu kommunizieren.

Die Verwaltung ist ein richtig schlimmes Beispiel. Wir haben gerade einen Fall, wo auf unserem Kongress jemand ein schweres Problem in einer Software in der öffentlichen Verwaltung deklariert hat gegenüber dem Hersteller. Er wollte darüber reden. Das wurde ihm von seiner Verwaltung aber verboten. Dort wurde gesagt, „wir reden nicht über Sicherheitsprobleme".

Diese Einstellung haben wir in der öffentlichen Verwaltung immer noch. Es gibt teilweise eine Gemengelage zwischen der Verwaltung und deren Zulieferern, die zum Teil dann dem Land gehören oder halb dem Land gehören oder wie auch immer, wo man über Sicherheitslücken lieber nicht redet und schon gar nicht *fixt*, weil dann noch mehr Geld ausgegeben werden müsste. Das heißt, es gibt keine Sicherheitskultur in der öffentlichen Verwaltung. Das muss sich dringend ändern und wird sich nur über Bildung und *Incentives* ändern lassen, die es dahin treiben, dass Sicherheit normaler Bestandteil von allen Beschaffungs- und Revisionsprozessen sein wird.

Der **Vorsitzende**: Gibt es keine weitere Frage? Dann fahren wir mit der zweiten Fragerunde fort.

Abg. **Thomas Heilmann** (CDU/CSU): Auch von meiner Seite herzlichen Dank. Ich würde gerne einen neuen Aspekt in die Debatte einführen, nämlich ob Interoperabilität sicherheitserhöhend ist im Bereich von Software, ja oder nein. Mit dieser allgemeinen Frage würde ich gerne mit Professor Waidner einsteigen und anschließend weitere Fragen stellen.

SV **Prof. Dr. Michael Waidner** (Fraunhofer-Institut für Sichere Informationstechnologie SIT): Generell ist Interoperabilität für die Sicherheit eine gute Sache. Interoperabilität basiert auf Standards und Standards kann man verifizieren. In Standards muss man aktiv sein. Aber da ist Deutschland nicht mehr ganz so aktiv. Das ist auch ein Defizit, woran man arbeiten sollte. Aber generell ist Interoperabilität eine gute Sache.

Abg. **Thomas Heilmann** (CDU/CSU): Gibt es unter den Sachverständigen jemanden, der anderer Meinung ist? – Scheint nicht der Fall zu sein. Würden Sie andeuten, dass wir in der Europäischen Union und in Deutschland in zu wenig Ressourcen investieren? Brauchen wir mehr staatliche Ressourcen dafür?

SV **Prof. Dr. Michael Waidner** (Fraunhofer-Institut für Sichere Informationstechnologie SIT): Generell muss Deutschland, nicht nur der Staat, sondern auch die Industrie, deutlich aktiver werden im Bereich der Standardisierung. Ein gutes Beispiel ist, dass alle über Quantencomputer und über Post-Quanten-Kryptografie reden. Das war, glaube ich, auch eine Ihrer Fragen. Es gibt gerade einen weltweit wichtigen Standardisierungsprozess, der von der amerikanischen Standardisierungsbehörde NIST (National Institute of Standards and Technology) betrieben wird. Ich wüsste nicht, dass es etwas im gleichen Stil in Europa oder Deutschland gibt, obwohl schon sehr viele Forschungsaktivitäten stattfinden.

Abg. **Thomas Heilmann** (CDU/CSU): Inwieweit beteiligt sich das Fraunhofer Institut an diesem Standardisierungsgremium und wie finanzieren Sie das?

SV **Prof. Dr. Michael Waidner** (Fraunhofer-Institut für Sichere Informationstechnologie SIT): Wir beteiligen uns an Standardisierungen, tatsächlich auch an der NIST-Standardisierung beispielsweise. Wir machen das im Rahmen unserer üblichen Forschungsprojekte und dank

ATHENE haben wir jetzt relativ viele Freiheiten, das zu tun. Aber noch einmal, Standardisierung ist nichts, was aus meiner Sicht von der Forschung alleine getrieben werden muss, sondern der Staat muss sich daran beteiligen und noch viel mehr die Industrie. Denn die Industrie muss das im Endeffekt ausbaden, was standardisiert wird. Es ist wichtig, dass Firmen die Rahmenbedingungen für Standards setzen und erklären, was gute Standards sind. Dort muss mehr gemacht werden.

Abg. **Thomas Heilmann** (CDU/CSU): Ist das nicht ein Henne-Ei-Problem? Wir haben nicht so starke Softwarefirmen, wie andere Länder, wenn wir über Softwarestandards reden? Deswegen beteiligen sich natürlich auch weniger Firmen aus Deutschland an diesem Thema.

SV **Prof. Dr. Michael Waidner** (Fraunhofer-Institut für Sichere Informationstechnologie SIT): In der Vergangenheit war es so, dass deutsche Firmen sehr viel intensiver an der Standardisierung beteiligt waren. Also ist es jetzt ein rückläufiger Prozess. Ansonsten denke ich: ja, es ist ein Henne-Ei-Prozess. Aber man kann aus diesem Prozess ausbrechen. Im IT-Bereich aktiv zu werden, globale *Player* aufzubauen, ist aus meiner Sicht nicht so schwierig, wie es immer gedacht wird. Der Aufwand ist vergleichsweise gering.

Abg. **Thomas Heilmann** (CDU/CSU): Ich würde die Frage auch an Frau Marnau stellen. Beteiligt sich die ganze Helmholtz-Gesellschaft an solchen Prozessen?

SVe **Ninja Marnau** (CISPA Helmholtz Center for Information Security): Für die ganze Helmholtz-Gemeinschaft der Forschungszentren kann ich es nicht sagen, aber ich kann es Ihnen für unser konkretes Zentrum, das CISPA, sagen. Wir sind Mitglieder in verschiedenen Standardisierungsorganisationen, die sich vor allem auf europäischer Ebene mit IT-Sicherheit befassen.

Ich selbst war aktiv in der Internet-Standardisierung, der Web-Standardisierung. Wenn uns die Forschungsprojekte die Möglichkeit dazu eröffnen, tun wir das sehr gerne. Aber es ist immer eine nachrangige Priorität nach den primären Forschungszielen. Das heißt, wenn wir Erkenntnisse gewonnen haben, bringen wir die gerne in die Standardisierung ein. Aber das müssen wir uns auch leisten können von der Zeit her. Denn Standardisierung ist ein sehr zeit- und finanzaufwendiger Prozess.

Abg. **Thomas Heilmann** (CDU/CSU): Noch einmal zurück zu Professor Waidner. Würden Sie sagen, dass die Tokenisierung oder die *Ledger*-Technologie ein solcher Standard zwischen Systemen werden und man sich somit eine bessere Interoperabilität vorstellen kann?

SV **Prof. Dr. Michael Waidner** (Fraunhofer-Institut für Sichere Informationstechnologie SIT): Die Blockchain-Diskussion ist jetzt keine, auf die ich gucken würde, um beliebige Standardisierungsprobleme zu lösen. Es ist eher ein Beispiel, dass man da Standards braucht. Aber generell wird diese Technologie, glaube ich, etwas überschätzt, was diesen Punkt betrifft.

Abg. **Thomas Heilmann** (CDU/CSU): Jetzt habe ich noch 32 Sekunden zu dem ganzen Thema KI. Ist es nicht auch ein Sicherheitsproblem, wenn die Erkenntnisse schneller im Ausland als im Inland kommen und ist Datenmangel auch ein Sicherheitsproblem?

SV **Prof. Dr. Michael Waidner** (Fraunhofer-Institut für Sichere Informationstechnologie SIT): Es ist kein Sicherheitsproblem, sondern ganz im Gegenteil, es ist toll, dass Deutschland im Bereich KI sehr aktiv und erfolgreich ist. Bei allen neuen Technologien, d.h. Blockchain oder KI, muss man das Gleiche machen. Man muss Sicherheit von Anfang an mit einbringen, mitdenken. *Security by Design* ist auch schon gesagt worden. Das muss man einfach mitberücksichtigen.

Abg. **Falko Mohrs** (SPD): Vielen Dank. Ich beginne mit Herrn Harzheim. Sie hatten beschrieben, welche Herausforderungen sich beim Single-RAN-Ansatz für Sie beim Netzausbau ergeben würden. Angenommen, Sie würden einen Open-RAN-Ansatz verfolgen, was würde sich ändern?

SV **Oliver Harzheim** (Vodafone GmbH): Ich kann jetzt schon sagen, dass wir auf jeden Fall in der Zukunft einen Open-RAN-Ansatz verfolgen werden. Die Technologie ist im Moment noch nicht marktreif, auch wenn sie in einzelnen Ländern jetzt schon in guten Piloten eingesetzt

wird. Auch Vodafone hat schon einige Pilotmärkte. Aber ich denke, bis zur Marktreife in einem Land wie Deutschland wird es sicherlich noch zwei, drei Jahre dauern. Dann werden wir Open-RAN-Technologie einsetzen. Wir werden dann auch die Vorteile der Open-RAN-Technologie dahingehend nutzen, dass einfach die Diversität der Hersteller wieder sehr stark steigen wird.

Wir werden neben den drei üblichen Herstellern oder vielleicht manchmal auch vier üblichen Herstellern, aus denen wir derzeit nur auswählen können, ein Hersteller-Portfolio haben, das weit darüber hinausgeht. Das wird natürlich auch den ganzen Markt beleben. Durch Standards, die auch da gesetzt werden, gehen wir davon aus, dass wenn wir Open-RAN nutzen, auch solche Umbauthemen, wie ich sie eben angesprochen habe, einfacher realisierbar sein werden, denn es ist wesentlich einfacher, einzelne Komponenten gegeneinander auszutauschen.

Abg. **Falko Mohrs** (SPD): Eine Frage an Herrn Rieger: Herr Harzheim hatte davon gesprochen, dass er das VAN-Netz (Value Added Network) als weniger kritisch und schützenswert eingestuft hat. Jetzt im Hinblick auf 5G und Ihrer technischen Expertise; teilen Sie diese Einschätzung?

SV **Frank Rieger** (Chaos Computer Club e.V.): Es ist natürlich so, dass ein solch komplexes System wie 5G mehr dem von Web-Technologien ähnelt. Die Architektur unterscheidet sich fundamental von denen der bisherigen Telekommunikationsnetze. Sie haben lauter Cloud-Entitäten, in denen die einzelnen Netzwerkfunktionen stattfinden und die Grenze zwischen dem *Radio Access Network Layer*, also den Mobilfunkzellen und dem CoA (*Care-of-Address*) ein bisschen fließend ist und man dort als Betreiber genau hinschauen muss. Aber prinzipiell ist es so, dass die Funktionen, die man im CoA hat, sprich, wo die Nutzerdaten liegen und der Zugang zu den Authentifizierungsfunktionen liegt, viel schützenswerter sind. Insofern ist die Strategie, die die *Operator* momentan betreiben und versuchen den *Radio Access Network Layer* etwas zu isolieren, um möglichst wenig kritische Funktionen darin zu haben und im Kern Komponenten von Herstellern, die aus welchem Grund auch immer, für vertrauenswürdiger gehalten werden, zu installieren, durchaus valide.

Es ist eine Strategie, die nicht dumm ist, sondern eine gute Abwägung zwischen den Sicherheitsanforderungen, die ganz klar da sind und von den Betreibern auch erkannt werden und den ökonomischen Erfordernissen: die Chinesen sind schlichtweg billiger. Ich sehe die Strategie nicht grundsätzlich als schlecht an. Allerdings muss man, was die Abschottung des *Radio Layers* versus CoA angeht, auch tatsächlich etwas tun. Man muss das in der Architektur berücksichtigen, man muss entsprechende Monitoring-Funktionen einbauen usw.

Abg. **Falko Mohrs** (SPD): Halten Sie das für dauerhaft beständig, wenn man davon ausgeht, dass wir ein *5G-Only-Network* haben, bei dem immer mehr Intelligenz in die Peripherie wandert?

SV **Frank Rieger** (Chaos Computer Club e.V.): Letzten Endes müssen alle Komponenten, die in einem solchen Netzwerk sind, auditiert werden, so auch alle *Radio-Access-Layer*-Komponenten. Wir brauchen uns nichts vormachen, die Komponenten von Cisco, Huawei, Ericsson oder Nokia unterscheiden sich in der Softwarequalität kaum. Was wir aus den Audits wissen, die die Briten und befreundete Unternehmen gemacht haben ist, dass die Softwarequalität bei allen ungefähr gleich schlecht ist. Es geht dabei nicht um Hintertüren, sondern um massenweise vorhandene *Bugs*, die auch ausnutzbar sind. Die müssen weg!

Dazu brauchen Sie eine Struktur, die herstellerunabhängig, länderunabhängig, einfach alle Komponenten auditiert und verpflichtende Mindeststandards festlegt dafür, dass solche Komponenten – egal ob im CoA oder Außennetzwerk – eingesetzt werden können. Das ist ein erreichbares Ziel, und nichts wo man sagen kann, das ginge gar nicht. Huawei und Cisco haben sich bewegt und ich rechne damit, dass die anderen Provider sich da auch bewegen werden. Das heißt, die Erreichbarkeit eines auditierbaren Netzes ist auf jeden Fall gegeben. Der richtige Weg ist zu sagen, dass wir Einblick in die Technologie sowie die Verifizierbarkeit der Komponenten herstellen müssen. Da gibt es ganz viele technische Detailthemen – da könnten wir

noch eine halbe Stunde drüber reden. Am Ende ist die Nachricht: es geht! Darauf sollte man sich konzentrieren und nicht darauf, ob dieser einzelne Hersteller vertrauenswürdiger ist als der andere.

Abg. **Joanna Cotar** (AfD): Vielen Dank. Meine erste Frage geht an Herrn Schönbohm: Sie nennen vier konkrete Möglichkeiten, die Auswirkungen von bestehenden Abhängigkeiten zu reduzieren: vertragliche Schnittstellenkompatibilität, Diversifikation, Nutzungsmöglichkeiten des Quelltextes und Nutzung offener Standards. Welche dieser vier Maßnahmen können im Rahmen der IT-Konsolidierung überhaupt noch berücksichtigt werden bzw. wurden berücksichtigt?

SV Präsident **Arne Schönbohm** (BSI): Die IT-Konsolidierung des Bundes ist ein langwieriger Prozess und schreitet rasant voran. Gerade im Bereich der IT-Konsolidierung hat der Haushaltsausschuss auch festgestellt, dass das Thema der Informationssicherheit eine herausgehobene Bedeutung bekommen soll. Es gab gerade vor kurzem einen Beschluss, wo das BSI dementsprechend auch noch einmal gestärkt wird. Ich glaube, das ist die Grundvoraussetzung dafür, dass diese vier Maßnahmen dann auch entsprechend umgesetzt werden können.

Abg. **Joanna Cotar** (AfD): Meine nächsten Fragen gehen an Frau Marnau: Es gibt offenbar unterschiedliche Auffassungen zum Umfang von Prüfungen bei Hardwarekomponenten und Software komplexer Systeme. Sie sagen, eine Konformitätsprüfung für komplexe Systeme, selbst mit Hilfe von *Testing*- und Analyse-Tools, kann nur stichprobenartig erfolgen.

Herr Schönbohm hat mehrfach erklärt, das BSI könne sämtliche Komponenten und Software-Updates beim 5G-Netz prüfen bzw. prüfen lassen. Was gilt denn nun?

SVe **Ninja Marnau** (CISPA Helmholtz Center for Information Security): Ich möchte Herrn Schönbohm nicht widersprechen, wenn er das gesagt hat, aber ich muss es tun. Ich denke, schon allein die schiere Masse an Systemen würde es nie erlauben, dass wir alle Hardwarekomponenten zum Beispiel redundant parallel schalten und schauen, ob sie sich alle bei den gleichen Eingaben gleich verhalten. Das ist schlicht nicht realistisch. Insofern ist es notwendig, dass wir uns auf Stichproben beschränken und dann eine Plausibilitätsprüfung machen und auch eine gewisse Vertrauenserwartung an den Hersteller haben.

Das Ganze muss ein fortlaufender Prozess sein. Nicht, dass es nur einmal am Anfang gemacht werden soll und dann sind alle glücklich mit dem Ergebnis dieser Prüfung. Sondern das muss ein fortlaufender, regelmäßiger Prozess der Überprüfung, der Kontrolle und auch der Überwachung dieser Systeme sein. Insofern können aus meiner Sicht Stichproben schon sehr aussagekräftige Ergebnisse liefern.

Abg. **Joana Cotar** (AfD) Dann noch zwei Fragen zum Thema „informierte Bürger": Welche Maßnahmen außerhalb der schulischen und hochschulischen Bereiche könnte der Staat zur Stärkung der digitalen Souveränität oder zumindest der *Awareness* der Bürger fördern und welche staatlichen Förderprogramme sind Ihnen bekannt? Wie wird deren Erfolg bewertet und wie kann man Defizite gegebenenfalls abstellen?

SVe **Ninja Marnau** (CISPA Helmholtz Center for Information Security): Was wir ganz konkret an unserem Standort in Saarbrücken machen und ich Ihnen beispielhaft nennen kann ist, wir haben neue Professuren für die Didaktik der Informatik eingeführt. Da geht es darum, wie wir Informatik vermitteln. Wir haben Forschungsprojekte, bei denen es darum geht, tatsächlich Lehrmaterialien für die Schulen bereit zu stellen. Wir haben Initiativen, bei denen sich IT-Sicherheitsforscher mit Lehrern zusammensetzen und aktuelle Probleme diskutieren, damit die Lehrer das aufnehmen und für ihren Unterricht verarbeiten können. Es gibt einen großen Strauß an möglichen Maßnahmen. Was fehlt, ist von Bund und Ländern eine übergreifende Strategie, was eigentlich die Ziele dieser Maßnahmen sein sollen und woran man den Erfolg solcher Maßnahmen bemessen könnte.

Außerhalb der Schule bieten wir von uns als Forschungszentrum Lehrgänge für Erwachsene an, die wir einmal im Jahr veranstalten. Wir sagen, wir bringen euch von der Pike auf alles bei: wie man einen Router bedient, wie man ein Handy sicher konfiguriert. So etwas würde ich mir mehr konsolidiert wünschen und dass es nicht unser

eigener Antrieb als Forscher ist, sondern dass es bundesweite Materialien dafür gibt. Vielleicht auch, dass es Onlinekurse gibt, bei denen sich interessierte Bürger einschalten könnten und dass es vor allem Forschungsförderung für solche Projekte geben würde, damit es in allen Bundesländern so ist und nicht nur im Saarland.

Abg. **Joana Cotar** (AfD): Die letzte Frage geht an Herrn Harzheim: Hat Ihr Unternehmen in Deutschland oder weltweit bereits chinesische Komponenten in ihren Mobilfunknetzen mit europäischen oder südkoreanischen Komponenten ersetzt und wie sind die Erfahrungen dabei?

SV **Oliver Harzheim** (Vodafone GmbH): Ja, aber aus dem Grund, weil diese Komponenten immer wieder durchgetauscht werden. Es gibt natürlich auch immer wirtschaftliche Aspekte. Es gibt die Konsolidierung von Wartungsverträgen, es gibt ganz vielfältige Gründe, warum man immer mal wieder zwischen Lieferanten hin- und herspringt. Natürlich gibt es auch eine Multi-Vendor-Strategie. Wir tun gut daran, dass wir immer mit mehreren *Vendors* arbeiten. Aus dem Grund lautet die Antwort ja, wir haben immer mal wieder *Vendors* gegen andere ausgetauscht.

Abg. **Manuel Höferlin** (FDP): Ich habe noch eine Frage an Herrn Harzheim. Wir haben jetzt mehrfach gehört, wie wichtig es sei, beim Thema Sicherheit zu überprüfen, Quellcodes anzuschauen, fortlaufend zu kontrollieren. Die Erwartungshaltung, so wie es immer mitklingt ist, dass das staatlicherseits gemacht wird. Da springt einem das BSI ins Auge, als dasjenige, das das durchführt. Sind Sie der Meinung, dass das BSI das in der derzeitigen Struktur kann? Ich frage nicht Herrn Schönbohm, denn sonst kommt er gleich mit den Sachen, die er sich für den nächsten Haushalt wünscht.

Sie haben jahrelange Erfahrung nicht nur als Provider, sondern auch als derjenige, der am größten Knoten sitzt und weiß, was alles an IT-Sicherheitssachen passiert. Was kann man verändern und besser koordinieren? Sehen Sie beim BSI, bei der Abwägung von Sicherheitslücken – auch wenn Herr Schönbohm immer wieder versichert, er habe nichts von ZITiS bekommen und er gibt alle Lücken weiter – einen gewissen Interessenskonflikt? Wird das in der jetzigen Struktur ordentlich zusammengeführt mit vielen anderen Aspekten, nicht nur aus der IT-Sicherheit, sondern auch aus der inneren Sicherheit? In Klammer dahinter: Diese übergreifende Koordination könnte man auch im Digitalministerium machen. Es gibt ja immer mehr, die sich meiner Meinung [hinsichtlich eines Digitalministeriums] anschließen. Vielleicht können Sie dazu auch noch etwas sagen.

SV **Oliver Harzheim** (Vodafone GmbH): Das ist eine sehr gute Frage. Das schiere Volumen von zu auditierenden Codes dürfte wahrscheinlich ausschließen, dass das exklusiv beim BSI läuft. Die Diskussion, die wir im Bereich 109 TKG (Erhöhung der Sicherheitsarchitektur) hatten, ging darum, dass Auditoren zur Verfügung stehen, um das zu machen. Aber selbst da kamen schon Fragen auf, wie es mit selbstgeschriebener Software in einem Unternehmen ist. Wie kann die überhaupt unsicher sein?

Außerdem ist es ein absoluter Standard, dass *Open-Source-Software* in den Unternehmen eingesetzt wird, eigentlich immer die gleiche. Das haben wir sehr oft im Bereich Mail-Server, Sicherheitssysteme in den Unternehmen usw. Vieles davon ist *Open-Source-Software*. Soll die jeder neu zertifizieren lassen? Das macht eigentlich überhaupt keinen Sinn. Das ganze Vorgehen im Moment zu sagen, das BSI soll alles machen, kann so eigentlich nicht bleiben. Das würde insbesondere, wenn es um kritische Funktionen geht, also auch um Updates, teilweise Stunden dauern. Wenn Sicherheitslücken bekannt werden, müssen wir *sofort Fixes* in die Netze einspielen. Da kann man nicht warten, ob diese Software erst noch zertifiziert oder auditiert wird. Es müssten Ausnahmeregelungen her, die aber momentan nicht vorgesehen sind.

Von daher ist dieses ganze Konzept „wie kriege ich sicherheitskritische Zertifizierung hin, wie soll das in der Praxis ablaufen" im Moment noch nicht richtig durchdacht und muss im Rahmen der Erweiterung des Sicherheitskonzepts wirklich noch einmal aufgenommen werden.

Abg. **Manuel Höferlin** (FDP): Vielen Dank, auch wenn Sie das Digitalministerium umschifft haben. Die Frage, wenn wir Sicherheit nicht mehr durch das Knacken von Verschlüsselung gefährden und davon absehen, Hintertüren in Software

einzubauen, kommt jetzt immer die schöne Formulierung „dann wir nehmen nicht die Hinter-, sondern die Vordertür". Ich frage mich, was das bedeutet.

Ich verstehe darunter, dass man das so konstruiert, dass der Anbieter des Dienstes eine kontrollierte Schnittstelle bereitstellt – ich versuche es freundlich zu formulieren. Welchen Vorteil hat das hinsichtlich der IT-Sicherheit? Wird nicht innerhalb solcher Unternehmen der Angriffsvektor auf den menschlichen Faktor verlagert und auf die Organisationsstruktur der Unternehmen? Wie sieht es dabei mit der Vertrauensstellung aus? Letztlich ist das Vertrauen dann komplett bei diesen Unternehmen angesiedelt, die wir auch im internationalen Umfeld in Deutschland mit Diensten haben.

SV **Oliver Harzheim** (Vodafone GmbH): Das hat Vor- und Nachteile. Man könnte sichere Verschlüsselung verwenden und man könnte sichere Software bauen. Selbst wenn man bei sicheren Betriebssystemen die Anbieter verpflichtet, weitere Korrespondenten oder ähnliches mit aufzunehmen, wäre die Ausleitung per se sicher realisierbar. Das wirft allerdings wieder das Problem auf, wer ist ein Empfänger, wer kann das anordnen, wie funktioniert das eigentlich.

Unsere eigene föderale Struktur, betrachtet mit ihren Landespolizeibehörden, Bundesbehörden, Zoll und Dutzenden von Organisationen, bei denen immer noch mehrere Leute eine Zugriffsmöglichkeit darauf haben müssten, ist nicht mehr kontrollierbar. Sie können keine *Security* herstellen, wenn Dutzende von Leuten einen Schlüssel haben, der noch an Vertreter usw. weitergegeben wird. Methoden wie *Ghost Protocol*, wie Großbritannien das vorsieht, sind nicht geeignet, um wirklich sicherzustellen, dass nur berechtigte Empfänger eingebunden sind.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ich versuche, drei Fragen an drei Sachverständige unterzubringen und bitte daher die ersten beiden um Kooperation: Zuerst frage ich Herrn Landefeld. Sie haben in Ihrer Stellungnahme geschrieben, dass der Ausschluss einzelner Hersteller dann kartellrechtlich ein Problem ist, wenn Sicherheitsrisiken nicht konkret nachgewiesen worden sind, und dass Unterstellungen nicht ausreichen würden. Heißt das konkret, solange man die nicht hat und von Parteizellen-Einflussnahmen in China und irgendwo redet, wäre es illegal, Huawei auszuschließen?

SV **Klaus Landefeld** (Eco-Verband der Internetwirtschaft): Wir denken, das ist sehr schwierig und was soll im Zweifelsfall die Grundlage für die Klage sein? Man muss es irgendwo verteidigen können, wenn das Unternehmen klagt. Nur ein abstraktes *Hearsay*, da könnte ich im Prinzip jeden ausschließen. Das ist eine sehr schwierige Sache.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Man könnte diejenigen ausschließen, wo man das schon genau weiß. Aber da ist in den letzten Jahren nichts passiert.

SV **Klaus Landefeld** (Eco-Verband der Internetwirtschaft): Da müssten wir viele amerikanische Hersteller auch ausschließen…

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Das war mein *Hint*, mein Wink mit dem Zaunpfahl.

Ich habe noch eine Frage an Ninja Marnau: Gehen wir davon aus, wir würden chinesische und amerikanische Unternehmen – bei 5G reden wir hauptsächlich von diesen beiden Ländern – bei Hardware-Komponenten ausschließen. Wie müsste man realistisch, aber auch sicher, beim Ausbau vorgehen?

SVe **Ninja Marnau** (CISPA Helmholtz Center for Information Security): Ich bin mir nicht ganz sicher, ob ich die Frage fachlich beantworten kann. Ich würde mich tatsächlich der Ansicht anschließen, dass die Sicherheitsmaßnahmen, die Sicherheitsüberprüfungsmaßnahmen und die Kontrollfunktionen unabhängig von der Herkunft der Anbieter ohnehin im System vorgesehen und bei der Vergabe bereits mit berücksichtigt werden müssen. Das heißt, wenn wir Hersteller aufgrund geopolitischer Erwägungen ausschließen, sind es exakt nur geopolitische Erwägungen und weniger konkrete IT-Sicherheitserwägungen. Alle Sicherheitsmaßnahmen, die wir vorsehen, müssen tatsächlich unabhängig von konkreten, beteiligten Herstellern vorhanden sein.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ich habe noch eine Frage an Frau Skierka: Sie schreiben, im Bereich der IT-Sicherheitstechnologien haben

Wissenschaftler und Unternehmer in Deutschland konkurrenzfähige IT-Sicherheitslösungen entwickelt, konnten sich aber nicht erfolgreich auf dem internationalen Markt durchsetzen. Woran liegt das und in welchen Bereichen haben wir diese Konkurrenzfähigkeit?

SVe **Isabel Skierka** (European School of Management and Technology GmbH ESMT): Vielen Dank für die Frage. Diese Aussage beruht auf einer Studie, die im Auftrag des BMWi durchgeführt wurde. Demnach sind wir sehr konkurrenzfähig, aber die meisten IT-Sicherheitstechnologien werden auf dem inländischen Markt verkauft. Woran das jetzt genau liegt und warum wir international nicht so erfolgreich sind, kann ich nicht beantworten. Das könnte am Marketing oder auch an anderen Aspekten liegen. Aber wo wir international wirklich führend sind, sind sichere *Embedded Systems* im Bereich Hardware, und das könnten wir sicherlich ausbauen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Aufgrund der verbleibenden Zeit kann ich noch eine Frage an Frank Rieger stellen: Wie kann die im Moment stattfindende und vermutlich noch länger andauernde IT-Konsolidierung der Netze des Bundes dazu beitragen, die vorhandene Abhängigkeit von Unternehmen zu beenden, die bestimmte kommerzielle proprietäre Software vertreiben, und wie würde das die IT-Sicherheit steigern?

SV **Frank Rieger** (Chaos Computer Club e.V.): Ich denke, dass die momentan laufende IT-Konsolidierung eine gute Chance bietet zu sagen, wir nehmen Geld in die Hand und machen nicht nur Beschaffung, sondern auch Entwicklung, bauen eigene Kompetenzen auf für IT-Systeme, die wir als kritisch für den Betrieb des Staates und der Länder ansehen, und gehen auf Open-Source-Komponenten, die eine Hoheit bedeuten im Sinne von „man ist nicht abhängig von Microsoft oder Google, sondern hat die eigene Hoheit darüber".

Es gibt eine große Hemmschwelle, weil die bisherige Historie von staatlichen Softwareprojekten in Deutschland keine besonders rosige ist. Das hat aber benennbare Gründe, die lösbar sind. Daran lässt sich wirklich etwas ändern. Wir wissen mittlerweile sehr viel besser, wie man IT-Großprojekte managt. Es gibt an den Akademien in Deutschland gute Forschungen dazu. Wir haben mittlerweile auch *Best Practices* in großen Unternehmen die zeigen, wie man solche Projekte richtig angehen kann. Das Hauptproblem dabei ist nur, man darf sich kein „Wünsch-dir-was-Requirement-Management" machen, sondern man muss klar wissen, was man will. Damit ließe sich tatsächlich die Abhängigkeit von großen, insbesondere ausländischen Unternehmen, stark reduzieren.

Schon allein, wenn es eine echte Alternative gibt, würde das dazu führen, dass diese Unternehmen sehr viel flexibler werden, auch Zugang zu *Source Codes* zu gewährleisten und man könnte die Hoheit über das, was man auf den eigenen Systemen betreibt, erlangen.

Abg. **Dieter Janecek** (BÜNDNIS 90/DIE GRÜNEN): Meine Frage geht auch an Frank Rieger: digitale Souveränität – das große Schlagwort GAIA-X –, der Versuch, etwas in diesem Bereich zu tun und Standardisierung voranzutreiben. Auf der anderen Seite haben sie zu Recht gesagt, große Softwareprojekte in Deutschland waren jetzt nicht glorreich unterwegs. Aber müssen wir nicht doch zum Teil groß denken? Die Abhängigkeiten haben wir in vielen Bereichen: Suchmaschinen, Infrastrukturen, soziale Netzwerke, etc.

Wir als politisch Handelnde können groß denken, aber wir müssen am Ende etwas umsetzen, das nicht ins Scheitern führt. Das ist der Widerspruch dieser Diskussion. Vielleicht sind wir auch ein wenig geschädigt durch die Diskussion und das Scheitern in der Vergangenheit, etwas aufzusetzen, was vielversprechend sein kann im Rahmen eines europäisch-wertebasierten Konsensus. So würde ich es sehen.

Aber vielleicht können Sie beschreiben, was die wichtigsten Punkte einer digitalen Souveränitätsstrategie Deutschlands/Europas wären?

SV **Frank Rieger** (Chaos Computer Club e.V.): Aus meiner Sicht sollten wir uns davon verabschieden, Großprojekte zu priorisieren. Man sollte sich eher anschauen, was erfolgreich funktioniert und auch aus Erfahrungen anderer Länder lernen. Was erfolgreich funktioniert, ist, viele kleine Projekte mit relativ schneller Schlagzahl anzustoßen, zu fördern und zwar mit einer strategischen Ausrichtung, so dass die wie

Puzzleteile zusammenpassen und durchaus auch Redundanz zu fördern. Dann sollten in diesem Bereich drei, vier Projekte gefördert werden und das erfolgreichste bekommt eine Anschlussförderung, zum Beispiel Geld aus dem staatlichen Startup-Fonds, um daraus eine Firma zu gründen, oder bekommt Geld, um die Softwareentwicklung weiter voran zu treiben. Das bringt mehr, als den üblichen Großforschungsinstituten mal wieder die 50 Mio. Euro zu geben, damit sie irgendetwas bauen, von dem Professor Waidner dann richtigerweise sagt, das findet sowieso keinen Anschluss am Markt. Lieber viele kleine Dinge fördern und versuchen, diese möglichst schnell marktgängig zu machen.

Wenn man sich ansieht, was im internationalen Venture-Capital-Markt passiert, ist die Zeit der *Unicorns* vorbei. Die weisen VCs (*Venture Capitalists*) wissen, wie der Hase läuft und fördern lauter Projekte, die verteilt sind, und sie setzen darauf, dass keine riesige Infrastruktur gebaut wird, sondern eine Technologie, die in der Lage ist, verteilt ausgerollt zu werden.

Beispiel soziale Netzwerke: Es gibt Technologien wie Mastodon, um sogenannte föderierte soziale Netzwerke zu betreiben. Da haben Sie nicht „ein Facebook", sondern tausende kleine Server, die nach einem standardisierten Protokoll miteinander „reden" – so wie das Internet ursprünglich auch mal vorgesehen war – und genau dieselben Funktionen realisieren, nur dass sie keine Machtkonzentration haben, weil die technologischen Funktionen nicht in einer Hand konzentriert sind.

Ich empfehle, darauf aufzusetzen und spezifisch verteilte Technologien zu fördern; Technologien, die darauf ausgelegt sind, dass nicht alles in einer Hand endet und es *einen* großen Fehlschlag gibt, sondern vielleicht 60 oder 70 kleine Fehlschläge und dafür aber auch 30 oder 40 Erfolge, die tatsächlich ausgebaut und größer gemacht werden können. Das ist Mut zum Experiment! Wir sind nicht so gut, dass alles am grünen Tisch designt werden könnte. Dafür ist Technologie viel zu schnell.

Ein Beispiel dafür ist die Hardwareentwicklung: Wir sagen immer, der „Hardwarezug ist abgefahren!" Wir können in Europa keine Prozessoren mehr bauen und es ist alles zu spät. Das stimmt nicht! Wir haben mittlerweile Entwicklungen, wie zum Beispiel den sogenannten RISC-V-Prozessor: Das ist ein offenes Hardwaredesign, das alles – von einem kleinen Prozessor, der eine Waschmaschine steuern kann bis hin zu einem Tablet – abdecken kann und mittlerweile größer wird.

Es ist ein offenes Design, das heißt, die gesamten Unterlagen zum Bau eines solchen Prozessors liegen offen vor. Es gibt schon verschiedene Länder, die sagen, wir setzen mal darauf. Indien zum Beispiel hat gesagt, das ist ein Design, mit dem wir etwas anfangen können und baut darauf mehrere Prozessoren als Teil einer nationalen technologischen Souveränitätsstrategie. Das ist ein Weg, den die EU oder sogar Deutschland auch beschreiten können. Dafür haben wir die Kapazitäten und dafür reichen auch die Fertigungssysteme in Deutschland noch aus.

Der allergrößte Teil der Prozessoren sind nicht die dicken Intel- oder AMD-Prozessoren, sondern der größte Teil der Prozessoren wird in kleinen Geräten verbaut. Und da steht und fällt die *IT-Security:* in den kleinen Geräten, in IoT-Systemen, in den gerade für Deutschland so wichtigen Industriesteuerungssystemen. Wir sind nun einmal ein Land von Maschinenbauern und wir sollten dafür sorgen, dass diese Industrie weiter eine Basis hat und sagen kann, was wir als deutsche Ingenieurstugenden kennen, dehnen wir auch auf den Bereich *IT-Security* aus: Unsere Produkte enthalten auch Prozessoren, bei denen man hineingucken kann, von denen man alle Designunterlagen hat. Das ist ein realistisches erreichbares Ziel und nicht einmal besonders teuer.

Dasselbe kann man auch im Bereich der Software machen. Man baut kleine sichere Komponenten, die Bestandteil einer solchen Puzzle-Strategie sind, die in sicheren Programmiersprachen gemacht werden, die auditiert werden und bei denen dafür gesorgt wird, dass, wenn sie erfolgreich sind und eine Marktakzeptanz finden, eine Anschlussfinanzierung stattfindet. Das ist eine sinnvolle wichtige Strategie und ist für relativ wenig Geld, verglichen mit dem Verteidigungshaushalt, realisierbar und hätte einen sehr großen *Impact.*

Der **Vorsitzende:** Vielen Dank. Jetzt sind wir mit

zwei Fragerunden durch, wir schaffen keine dritte mehr. Wir haben nur noch wenige Minuten. Ich darf mich ganz herzlich bedanken. Ich fand besonders bemerkenswert, dass wir im Vergleich zu anderen gut dastehen, aber absolut eigentlich alle schlecht dastehen. Was in der Konsequenz dazu führt, dass wir auch – das ist mehrfach angeklungen – politisch tätig werden müssen und handeln müssen. Das wiederum führt dazu, was auch Kollege Herzog erwähnt hat, dass wir mit Sicherheit in den nächsten Wochen und Monaten noch intensiv im Austausch sein werden. Danke, dass Sie uns Rede und Antwort gestanden haben und uns diesen Input gegeben haben. Ich bedanke mich auch bei allen Interessierten unserer öffentlichen Anhörung sowie bei der Technik, die es möglich gemacht hat, dass viele Interessierte Zugang zu der öffentlichen Anhörung heute hatten und auch in Zukunft haben werden. Ich weise darauf hin, dass unsere nächste Ausschusssitzung am 18. Dezember, voraussichtlich aber zeitlich schon etwas früher, stattfinden wird. Bitte merken Sie sich das entsprechend vor. Ich wünsche Ihnen noch einen angenehmen Abend. Vielen Dank, die Sitzung ist geschlossen.

Schluss der Sitzung: 17:52 Uhr

Hansjörg Durz, MdB
Amtierender Vorsitzender