18. Wahlperiode

Deutscher Bundestag
Ausschuss Digitale Agenda

# Wortprotokoll
der 7. Sitzung

**Ausschuss Digitale Agenda**
Berlin, den 7. Mai 2014, 14:30 Uhr
Paul-Löbe-Haus
Konrad-Adenauer-Allee 1
10557 Berlin
Sitzungssaal: 4.600

Vorsitz: Jens Koeppen, MdB

## Tagesordnung

**Liste der Sachverständigen**

**Michael Hange**,
Präsident des Bundesamt für Sicherheit in der Informationstechnik (BSI)

**Dr. Sandro Gaycken**,
Institut für Informatik der Freien Universität Berlin

**Prof. Niko Härting**,
Rechtsanwalt

**Pascal Kurschildgen**,
IT-Sicherheitsberater

**Linus Neumann**,
Chaos Computer Club e.V.

**Thorsten Schröder**,
IT-Sicherheitsberater

**Mitglieder des Ausschusses**

| | **Ordentliche Mitglieder** | **Stellvertretende Mitglieder** |
|---|---|---|
| CDU/CSU | Beermann, Maik<br>Durz, Hansjörg<br>Jarzombek, Thomas<br>Koeppen, Jens<br>Nick, Dr. Andreas<br>Schipanski, Tankred<br>Schwarzer, Christina | Hornhues, Bettina<br>Lange, Ulrich<br>Schön (St. Wendel), Nadine<br>Tauber, Dr. Peter<br>Wanderwitz, Marco<br>Wendt, Marian<br>Whittaker, Kai |
| SPD | Esken, Saskia<br>Flisek, Christian<br>Kampmann, Christina<br>Klingbeil, Lars<br>Reichenbach, Gerold | Bartol, Sören<br>Dörmann, Martin<br>Stadler, Svenja<br>Träger, Carsten<br>Zimmermann, Dr. Jens |
| DIE LINKE. | Behrens, Herbert<br>Wawzyniak, Halina | Korte, Jan<br>Pau, Petra |
| BÜNDNIS 90/DIE GRÜNEN | Janecek, Dieter<br>Notz, Dr. Konstantin von | Beck (Köln), Volker<br>Rößner, Tabea |

Tagungsbüro

Deutscher Bundestag

# Sitzung des Ausschusses Nr. 24 (Ausschuss Digitale Agenda)

Mittwoch, 7. Mai 2014, 14:00 Uhr

## Anwesenheitsliste

gemäß § 14 Abs. 1 des Abgeordnetengesetzes

| Ordentliche Mitglieder des Ausschusses | Unterschrift | Stellvertretende Mitglieder des Ausschusses | Unterschrift |
|---|---|---|---|
| **CDU/CSU** | | **CDU/CSU** | |
| Beermann, Maik | ..... | Hornhues, Bettina | ..... |
| Durz, Hansjörg | ..... | Lange, Ulrich | ..... |
| Jarzombek, Thomas | ..... | Schön (St. Wendel), Nadine | ..... |
| Koeppen, Jens | ..... | Tauber Dr., Peter | ..... |
| Nick Dr., Andreas | ..... | Wanderwitz, Marco | ..... |
| Schipanski, Tankred | ..... | Wendt, Marian | ..... |
| Schwarzer, Christina | ..... | Whittaker, Kai | ..... |
| **SPD** | | **SPD** | |
| Esken, Saskia | ..... | Bartol, Sören | ..... |
| Flisek, Christian | ..... | Dörmann, Martin | ..... |
| Kampmann, Christina | ..... | Stadler, Svenja | ..... |
| Klingbeil, Lars | ..... | Träger, Carsten | ..... |
| Reichenbach, Gerold | ..... | Zimmermann Dr., Jens | ..... |
| **DIE LINKE.** | | **DIE LINKE.** | |
| Behrens, Herbert | ..... | Korte, Jan | ..... |
| Wawzyniak, Halina | ..... | Pau, Petra | ..... |
| **BÜ90/GR** | | **BÜ90/GR** | |
| Janecek, Dieter | ..... | Beck (Köln), Volker | ..... |
| Notz Dr., Konstantin von | ..... | Rößner, Tabea | ..... |

**Ausschuss Digitale Agenda**

**Mittwoch, 7. Mai 2014, 14:00 Uhr**

| | **Fraktionsvorsitzende:** | **Vertreter:** |
|---|---|---|
| CDU/ CSU | ..... | ..... |
| SPD | ..... | ..... |
| DIE LINKE. | ..... | ..... |
| BÜNDNIS 90/ DIE GRÜNEN | ..... | ..... |

| **Fraktionsmitarbeiter:** (Name bitte in Druckschrift) | **Fraktion:** | **Unterschrift:** |
|---|---|---|
| Pohl, Jörn | Grüne | |
| SCHEELE | LINKE | |
| KRACHER | SPD | |
| KÜHNAU | CDU/CSU | |
| [illegible] | CDU/CSU | |
| | | |
| | | |
| | | |

**Tagesordnungspunkt 1**

Öffentliches Fachgespräch

**IT-Sicherheit**
Selbstbefassung 18(24)SB1

**Fragenkatalog**
Selbstbefassung 18(24)SB2

Der **Vorsitzende,** Abg. **Jens Koeppen** (CDU/CSU): Meine Damen und Herren, liebe Kolleginnen und Kollegen, werte Gäste. Ich begrüße Sie ganz herzlich zur 7. Sitzung des Ausschusses Digitale Agenda. Wir haben heute unser erstes Fachgespräch zum Thema „IT-Sicherheit“. Das Interesse daran ist noch größer, als wir gedacht haben. Die Besuchertribüne ist gut besetzt. Ich begrüße Sie ganz herzlich. Wir haben so viele Anmeldungen, dass wir uns einen zweiten Saal nehmen mussten und nun einen Livestream dorthin übertragen. Das ist im Saal
E 800. Ich bitte um Ihr Verständnis, aber es stand heute kein größerer Raum im Deutschen Bundestag zur Verfügung. Deswegen müssen wir mit diesen Räumlichkeiten Vorlieb nehmen. Außerdem wird das Fachgespräch heute auf www.bundestag.de live gestreamt. Auch allen, die dort zuschauen, ein herzliches Willkommen. Ein besonderes Willkommen gilt unseren Experten und Sachverständigen. Ich begrüße ganz herzlich Herrn Michael Hange, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Herrn Pascal Kurschildgen, IT-Sicherheitsberater, Herrn Dr. Sandro Gaycken von der Freien Universität Berlin, Fachbereich Mathematik und Informatik, Herrn Thorsten Schröder, modzero GmbH Deutschland, Herrn Linus Neumann, Chaos Computer Club e. V. (CCC) und Herrn Professor Niko Härting, Rechtsanwalt. Herzlich willkommen. Wir freuen uns, dass Sie uns heute hier Rede und Antwort stehen. Von der Verfahrensweise her wollen wir es so machen, dass wir Ihnen die Möglichkeit geben, drei Minuten ein Eingangsstatement zu halten. Wir schauen da nicht genau auf die Uhr, wollen aber, dass wir mehr Zeit haben, um Fragen zu stellen und dass Sie dann auch antworten können. Für die Abgeordneten wollen wir es so halten, dass sie zwei Fragen an einen Sachverständigen oder eine Frage an zwei Sachverständige stellen. Das ist ein übliches Verfahren und hat sich gut bewährt. Das wollen wir hier auch probieren, so dass wir zu einer guten Diskussion kommen. Die IT-Sicherheit ist gerade in den letzten Tagen ein Thema, das an Bedeutung und Aktualität nicht verloren hat. Deswegen ist dieses Fachgespräch nicht nur wichtig für unsere parlamentarische Arbeit, sondern insbesondere auch für die Bürgerinnen und Bürger und all diejenigen, die sich im Netz bewegen, um Information und Aufklärung zu bieten. Wir möchten, gerade in diesem Ausschuss, die Überschriften „Chance Digitalisierung“, „Chance Internet“, „Chance Vernetzung“ immer in den Vordergrund stellen. Dazu gehört natürlich, dass das Netz auch sicher ist, dass die Daten sicher sind, dass die Daten geschützt werden. Das ist unser erstes Thema. Ich bitte die Sachverständigen, die Mikrofone zu benutzen und nach dem Statement auch wieder auszuschalten. Ich begrüße außerdem noch ganz herzlich die Parlamentarische Staatssekretärin Brigitte Zypries. Dann können wir auch schon beginnen. Ich bitte als erstes den Sachverständigen Herrn Michael Hange um sein Statement.

SV **Michael Hange**: Vielen Dank, Herr Vorsitzender. Ich beginne mit der ersten Frage (*des Fragenkatalogs*): Die Gefährdungslage. Dort sind drei Dinge erwähnt: Der Ausspähskandal, der Identitätsdiebstahl und die Sicherheitslücke in Heartbleed oder Heartbeat. Diese Dinge sind von der Ausgangssituation her sehr unterschiedlich und machen in der Ausdifferenzierung deutlich, wie man agieren muss. Also erst einmal die Ausspähaktionen von Nachrichtendiensten. Das sind zum einen Angriffe auf Kommunikationswege. Das sind aber auch individuelle Cyberangriffe auf IT-Systeme und die Manipulation von Standard und Geräten. Zweitens, das Thema Identitätsdiebstahl, welches die hohe Aktivität der Cyberkriminalität zeigt, die arbeitsteilig agiert. Man kann solche Dienstleistungen und Produkte heute sogar kaufen bzw. mieten. Die Cyberkriminalität hat im Grunde eine sehr hohe Fähigkeit erreicht, nicht nur Bürger anzugreifen, sondern auch Unternehmen. Beim ersten Punkt spielt das Thema Kryptografie eine Rolle, aber auch das Thema – und das möchte ich differenziert sehen – Abwehr von Cyberangriffen. Bei Cyberangriffen versucht man, da, wo Kryptografie eingesetzt wird, hinter die Kryptografie zu kommen, um mit der Übernahme von Systemen an die Klardaten selbst bzw. in die Pro-

zesssteuerung zu gelangen. Ziel ist dann, das System zu übernehmen. Bei Identitätsdiebstahl zeigt sich für uns in der Beobachtung sehr deutlich, dass der Online-Handel mit softwaregestützten Passwortverfahren wesentlich anfälliger ist als z. B. Online-Banking, bei dem es mit der EC-Karte doch ein Stück Hardware gibt. Es gibt Schwächen bei den Anbietern. Es ist aber vielfach auch so, dass die Internetnutzer mit einem Virenschutz und einer Firewall nicht mehr hinreichend geschützt sind. Dem muss mit noch mehr Aufklärung begegnet werden. Auf der anderen Seite muss man aber auch die Anbieter mehr in die Pflicht nehmen.
Schließlich das Thema Heartbleed: Das idealtypische Open Source Produkt, aber eben nicht sehr gut programmiert, vor allen Dingen breit eingesetzt und von keinem Betreiber richtig inspiziert. Open Source ist wegen des Transparenzgebots begrüßenswert. Es muss jedoch eine gewisse Trennung zwischen Entwickler und Prüfer da sein. Soviel zunächst zur Ausgangssituation.
Das Thema „Sichere Verschlüsselung“ ist nicht nur eine Frage des Angebotes, sondern auch der Nachfrage bei den Nutzern. In der Verwaltung wird Verschlüsselung teilweise vorgeschrieben, dort setzen wir sie ein. Die Wirtschaft hält sich zum Teil sehr zurück oder hat andere Kostensätze für das, was man eben in Kryptografie, in IT-Sicherheit investieren will. Ich glaube, es ist auch für das Management sehr wichtig, Zahlen zu nennen, was man beim IT-Einsatz, bei IT-Investitionen auch für die IT-Sicherheit einsetzen muss.
Vielleicht abschließend zu meinem Statement: An sich bewegt sich das Ganze in einem Dreieck. Das sind einmal die Internetnutzer auf den verschiedenen Ebenen – also der Bürger, die Unternehmen, aber auch der Staat. Das sind die Anbieter, die Dienstleister, die Hersteller und dann noch die Rolle des Staates, der meiner Meinung nach auch die Interessen der Nutzer vertreten muss. Gerade bei Global Playern müssen die Mindeststandards deutlich gemacht werden, welche Hürden Produkte bzw. Dienstleistungen im Minimum nehmen müssen. Das vielleicht zu meinem Eingangsstatement.

Der **Vorsitzende**: Vielen Dank, Herr Hange. Herr Kurschildgen, Sie haben das Wort für Ihr Eingangsstatement.

SV **Pascal Kurschildgen**: Vielen Dank, Herr Vorsitzender. Ich bedanke mich für die Einladung und fasse mich ein bisschen kürzer. Eigentlich kann man diesem Statement nicht mehr allzu viel hinzufügen. Wir sind ja alle auf einer ähnlichen Linie, aber grundsätzlich finde ich schon, dass die Fragen (*des Fragenkatalogs*) hauptsächlich auf den Bereich der Verschlüsselung abzielen. Die Heartbleed-Schwachstelle hat vielen erst die Augen geöffnet, sich dem Thema überhaupt zu widmen. Ich finde immer noch – oder generell die meisten finden –, dass Verschlüsselung immer nur so stark ist wie das schwächste Glied in der Kette – und das ist heutzutage der Nutzer. Das ist nicht der Gesetzgeber, das ist nicht der Staat, das ist kein Unternehmen. Es sind die Nutzer der Systeme, die abgeholt werden müssen. Wir können technisch so viel umsetzen wie wir wollen, auch gesetzgeberisch so viel umsetzen wie es vielleicht Sinn macht oder geht, aber es bringt alles nichts, wenn wir die Nutzer als schwächstes Glied nicht abholen. Das heißt aus meiner Sicht ganz klar: Es muss einen Bildungsauftrag geben, der in Deutschland umgesetzt werden muss. Das heißt, die Bevölkerung muss informiert und aufgeklärt werden. Nur ein informierter und aufgeklärter Mensch kann aller Voraussicht nach richtig handeln. Man kann ihn dazu nicht zwingen, aber es ist ein Versuch, die Menschen darüber aufzuklären, was heutzutage alles passiert. Was am Markt alles möglich ist, was für Kriminelle an die Daten heran wollen, und da sage ich: Aufklärung ist enorm wichtig. Wir müssen die Menschen einfach bei der Stange und auf dem Stand der Technik halten.

Der **Vorsitzende**: Ich bedanke mich. Herr Dr. Gaycken, Sie sind der Nächste.

SV **Dr. Sandro Gaycken**: Vielen Dank. Vielen Dank auch für die Einladung. Ich will nur ganz kurz einige Dinge aus meiner Perspektive erzählen. Ich bin eher Experte für nachrichtendienstliche, militärische Angreifer und kann und will mich auch nicht so sehr zum Thema „Cybercrime“ äußern. Aus meiner Perspektive muss ich sagen, dass wir inzwischen eine deutlich andere Gefährdungslage haben. Die NSA hat uns natürlich viel gezeigt. Wir müssen aber sehen, dass das, was da getan wurde, auch nur pars pro toto für die Fähigkeiten und Interessen aller Nachrichten-

dienste ist, und für die Fähigkeiten vieler organisierter Krimineller, vieler Industriespione und natürlich auch Militärs. Das ist eine Bedrohungssituation, die nicht nur von den USA ausgeht, auch wenn wir das in den Feuilletons gerne in diese Richtung treiben, sondern die uns insgesamt etwas angeht. Vor allen Dingen müssen wir auch stärker die Sicherheitsaspekte sehen und uns vielleicht ein bisschen weniger intensiv um die Datenschutzaspekte kümmern. Denn die sind wirklich sehr essentiell. Wenn wir uns ansehen, was da technisch auf uns zukommt, dann sehen wir einen ganz klaren Kollaps der klassischen Sicherheitsmaßnahmen, der vor allem im Kollaps der Rahmenbedingungen besteht. Dass man also IT-Systeme isolieren kann, dass es Perimeter gibt, die einfach genug sind, dass man die beobachten und auch Angriffe detektieren kann. Das ist alles sehr schwierig geworden. Im Moment gibt es international drei Ansätze, wie man das lösen kann. Der erste Ansatz ist, dass wir so weitermachen wie bisher. Wir akzeptieren also eine IT, die in der Basis sehr verwundbar ist, mit vielen Tausend bis Hunderttausend Schwachstellen in den Produkten, und machen einfach die Wälle höher und die Detektion besser. Da gibt es aber erhebliche Zweifel, ob das funktionieren wird, weil diese Ansätze prinzipiell schlecht sind. Der zweite Ansatz ist im Moment sehr gefährlich und insbesondere in den USA und bei einigen Großmächten sehr hip. Wir wissen, dass diese Systeme sehr angreifbar sind, dass unsere Sicherheitssysteme nicht funktionieren. Also müssen wir bei möglichen Angreifern eine maximale Abschreckungswirkung generieren – durch Rückschläge, durch Strafverfolgung. Dies präsupponiert dann wieder, dass wir sehr genau über diese möglichen Angreifer Bescheid wissen. Das kann ich natürlich nur, wenn ich international maximale Überwachung installiere, alles sehr genau beobachte und auch in der Lage bin, mich zurückzuhacken. Dass die im Grunde genommen überall sitzen und alles beobachten, heißt elegant: „Upstream Intelligence“. Und da haben wir natürlich hohe Gefährdungen bei Eskalationen. Wir zwingen auch die Angreifer in einen Evolutionsprozess, dass diese ihre Spuren sehr viel besser tarnen und sich sehr viel mehr Mühe geben, diesen stärkeren, offensiveren Ansätzen zu begegnen. Das ist alles sehr gefährlich – und wir wollen wahrscheinlich auch nicht dieses exorbitante Maß an internationaler Überwachung haben. Deswegen schlage ich immer gerne als einen dritten Ansatz vor, dass wir einfach die Basistechnologien neu entwickeln. Das ist natürlich angesichts der Pfadabhängigkeiten, die wir haben, sehr stark disruptiv. Und es ist auch sehr teuer, Computer neu zu entwickeln. Aber dann können wir einen sehr guten Sicherheitsstand einziehen, sind wesentlich besser und haben auch keine Überwachungsprobleme. Danke.

Der **Vorsitzende**: Ich danke Ihnen. Herr Thorsten Schröder ist der nächste Redner.

SV **Thorsten Schröder**: Vielen Dank und vielen Dank auch für die Einladung. Ich kann mich meinen Vorrednern anschließen, die primär darauf Wert legen, dass die Bevölkerung und auch die Unternehmen stärker für Risiken und deren Folgen sensibilisiert werden. Denn nur, wer die Risiken und die Folgen kennt, kann sich auch wirksam dagegen schützen. Wir müssen dafür sorgen, dass man sich auf etwaige Schutzmechanismen, die immer wieder neu aufkommen, nicht blind verlässt. Beispiel Open SSL. Das ist eine Open Source-Library, eine Bibliothek, eine Programmierschnittstelle, die genutzt wird, um Kommunikation durch starke Kryptografie abzusichern. Viele Menschen nehmen an, dadurch, dass das jetzt eine Open Source-Software ist, sei sie sicher, weil jeder da drin nach Fehlern suchen und auch beheben kann. Aber dass diese Bibliothek viel zu komplex ist, als dass da jemand einmal kurz rüber schaut und Fehler erkennt, haben wir jetzt bei Heartbleed gelernt. Somit denke ich, dass nicht nur die Investition in die Bildung der Bevölkerung und der Unternehmen hinsichtlich IT-Security eine sinnvolle Maßnahme ist, sondern auch eine Investition in ein Audit solcher Open Source-Produkte notwendig ist. Diese kann maßgeblich zur Sicherheit im Internet beitragen. Open SSL ist nur ein Beispiel, da gibt es auch noch ganz viele andere Produkte, die auch unter Open Source-Lizenz veröffentlicht wurden. Das BSI hatte, noch bevor die Heartbleed-Attacken bekannt geworden sind, tatsächlich sogar einen Audit ausgeschrieben, eine Source Code Review dieser Bibliothek. Was daraus geworden ist, weiß ich allerdings nicht. Ich denke aber, es gibt auch noch einige weitere Punkte, die man zusätzlich beachten muss. So würde ich empfehlen, nicht nur ein Un-

ternehmen mit dem Audit einer solchen kritischen Bibliothek zu beauftragen, sondern mehrere, die unabhängig voneinander sich im Detail mathematische und kryptografische Funktionen ansehen. Wichtig ist auch, dass die Bevölkerung nicht dem Irrglauben überlassen wird, dass der neue elektronische Personalausweis (*nPA*), die elektronische Gesundheitskarte, irgendein Schengen-Routing oder eben auch De-Mail nun alles sicherer machen. Dass sich die Benutzer dieser Technologien jetzt blind darauf verlassen und sagen: „Ist ja alles verschlüsselt, das ist jetzt alles sicher und ich brauche mich um nichts mehr zu kümmern“. Die Gefahr, dass die einzelnen Benutzer am Ende noch angreifbarer sind als zuvor, ist recht hoch. Außerdem sollte grundsätzlich das Wohl der Bevölkerung über das Wohl der wirtschaftlichen Unternehmen gestellt werden, wenn es darum geht, kritische Sicherheitslücken zu beheben. Als Beispiel möchte ich hier einfach mal ein sehr bekanntes Produkt nennen, ein Produkt, das jeder benutzt – Mobiltelefone. Es gibt sehr viele bekannte Schwachstellen in den Protokollen. Diese Schwachstellen werden nicht behoben, weil es viel zu teuer wäre, all diese Geräte auszutauschen. Es gibt das Problem mit der Rückwärtskompatibilität. Ich finde, dass hier eigentlich ganz klare Vorgaben an die Betreiber kritischer Infrastrukturen, wie die Telekommunikationsanbieter, gemacht werden müssen. Dass sie verpflichtet werden, diese Sicherheitslücken zu beheben, die in den Protokollen schon festgeschrieben sind. Die Kosten dafür müssen dann eben die Unternehmen tragen bzw. könnten sicherlich auch durch den Endnutzer subventioniert werden, wenn es um die Anschaffung neuer Geräte geht. Damit möchte ich mein Statement erst einmal abschließen und gebe das Wort weiter.

Der **Vorsitzende**: Vielen Dank, Herr Schröder. Herr Neumann, Sie haben das Wort.

SV **Linus Neumann**: Auch ich bedanke mich für die Einladung. Ich fand Ihre Fragen sehr interessant und freue mich, dass die Fragen auch in dieser Tiefe diskutiert werden. Inzwischen ist es in der Welt angekommen, dass wir uns im Bereich der IT-Security plötzlich zurück ins Mittelalter geworfen haben, und viele Annahmen, auf die wir jahrelang gebaut haben, vor unseren Augen zusammengebrochen sind. Ich möchte deshalb auch mit einem kleinen Vergleich aus dem Mittelalter anfangen. Und zwar mit Reetdächern. Reetdächer hat die Menschheit irgendwann entdeckt, um sich in ihren Häusern vor Regen zu schützen. Dann fing die Menschheit irgendwann an, Städte zu bauen. Man hat gemerkt, wenn jetzt so ein Reetdach anfängt zu brennen, dann brennt die ganze Stadt ab. Man hat festgestellt, diese Reetdächer brennen leicht und sie können auch immer wieder brennen. Also hat man entschieden, in Städten solche Reetdächer nicht mehr zu verwenden. Man hat aber auch festgestellt, dass auch Häuser ohne Reetdach brennen. Das heißt, wir bauen keine Reetdächer mehr in den Städten, wir halten Feuerlöscher bereit, wir erlegen uns Brandschutzvorschriften auf. Und eine Sache, die ich immer wieder gefragt werde, wenn ich über IT-Security spreche, ist, was denn überhaupt noch sicher ist. Wer kann mir denn garantieren, dass das nicht auch kaputt ist? Niemand kann das. Und genau deshalb müssen wir jetzt dafür sorgen, dass wir nicht immer alles an eine Sicherheitsmaßnahme hängen, damit wir genau diese Probleme vermeiden, die wir jetzt gerade sehen. In der IT-Sicherheit heißt das, dass wir uns riesige zentrale Angriffspunkte bauen: große E-Mail-Provider, die mehrere Millionen Kunden in Deutschland haben. Wir bauen De-Mail, zentrale Infrastrukturen, mit denen wir die gesamten Bundesbürger an drei Server anschließen möchten. Alle diese Systeme tragen die Handschrift einer einzelnen Sicherheitsmaßnahme, die immer in der Hand des Anbieters liegt und keine zweite Möglichkeit bietet, um ein Problem an dieser einen Sicherheitsmaßnahme noch irgendwie zu lindern. Wir müssen uns natürlich überlegen, wie es dazu gekommen ist und was wir in Zukunft anders machen müssen. Wir können natürlich einerseits sagen – und davon bin ich ein großer Befürworter– wir sorgen dafür, dass es weniger Sicherheitslücken gibt. Der angesprochene Audit von Open SSL ist eine großartige Sache. Ich hoffe dass das Projekt so stattfindet. Die zweite wichtige Möglichkeit, in der jetzt unsere Versäumnisse liegen, ist, dass wir die Folgen von Sicherheitslücken in einzelnen Technologien, in einzelnen Systemen einschränken müssen. Das heißt, am Ende plädiere ich für Programme wie Audits und Bug Bounties, die dafür sorgen, dass

die einzelnen Sicherheitsmaßnahmen der Software, die wir nutzen, auf Sicherheitslücken abgeklopft werden, damit diese gefunden werden, bevor Angreifer sie ausnutzen. Dass wir auf dezentralere Infrastrukturen setzen, wo also nicht mehr ein zentraler Angriffspunkt zu einem Massenproblem führt. Dass wir auf Ende-zu-Ende-Verschlüsselungen setzen, die massiv die Attraktivität der zentralen Infrastruktur senken, weil das, was der Angreifer bekommt, wenn er die zentrale Infrastruktur angreift, dann trotzdem immer noch verschlüsselt ist. Und natürlich – es wurde gerade schon gesagt –, dass wir auch die Anbieter dazu bringen müssen, Sicherheitsstandards anzubieten, die dem aktuellen Anspruch genügen. Natürlich ist es gut, wenn der Nutzer weiß, dass GSM-Telefonate abgehört werden können. Das sollte eigentlich jeder spätestens seit 2011 wissen. Angela Merkel hatte trotzdem keine nennenswerte sinnvolle Alternative, sich vor diesen Angriffen zu schützen. Da ist sicherlich auch der Gesetzgeber in der Situation, hier Bedingungen zu schaffen, um daran etwas zu ändern. Ich komme sofort zum Schluss. Ein wichtiger Punkt, den ich noch ansprechen möchte, ist, dass wir im Moment eine sehr sinnvolle Institution für solche Fragen haben. Das ist das Bundesamt für Sicherheit in der Informationstechnik. Dieses untersteht aber gleichzeitig dem Bundesministerium des Innern, das an dieser Stelle einen Interessenkonflikt hat. Deshalb würde ich dafür plädieren, das Bundesamt für Sicherheit in der Informationstechnik als eine unabhängige Behörde aufzustellen. Vielen Dank.

Der **Vorsitzende**: Ich danke Ihnen für Ihre Ausführung und auch für die Bebilderung mit den Reetdächern. Das hilft manchmal weiter. Ich gebe das Wort Herrn Professor Härting. Bitteschön.

SV **Prof. Niko Härting**: Vielen Dank für die Einladung. Als Jurist möchte ich mich darauf beschränken, zu regulatorischen Fragen etwas zu sagen. Erstens. Wenn man über IT-Sicherheit spricht, muss man über die Nachrichtendienste sprechen. Die Methoden der Dienste – ausländische Dienste, aber auch inländische Dienste – stellen eine kardinale Bedrohung für die Sicherheit der digitalen Kommunikation dar. Jetzt taucht hier als Frage auf, was denn von der EU-Datenschutzgrundverordnung in diesem Zusammenhang zu halten ist. Die EU-Datenschutzgrundverordnung in all ihren Entwurfsfassungen klammert den gesamten Bereich der nationalen Sicherheit aus und setzt daher europäischen Nachrichtendiensten keine Grenzen. Für europäische Nachrichtendienste wird die EU-Datenschutzgrundverordnung nicht gelten. Noch weniger ist damit zu rechnen, dass sich ausländische Nachrichtendienste in irgendeiner Form – und ich spreche bewusst auch nicht nur von den amerikanischen – von etwas beeindrucken lassen, was in Brüssel verabschiedet wird. Es ist vielfach darauf hingewiesen worden, dass der Rechtsbruch einfach das Geschäft der Dienste ist. Soweit jetzt mit den Vorschlägen, die in Brüssel liegen, versucht wird, amerikanische Unternehmen an einer Zusammenarbeit mit ausländischen Diensten durch europäische Verbotsnormen zu hindern, geht das zunächst einmal an der Realität vorbei. Außerdem verkennen die Brüsseler Entwürfe die Zwangslage und die Pflichtenkollision, die für diese betroffenen Unternehmen entstehen. Wenn sie einerseits nach amerikanischem Recht und auch noch im Geheimen verpflichtet sind zu kooperieren und ihnen andererseits dann nach europäischen Recht dasselbe verboten ist, dann würde dort etwas Gesetz, was wir im umgekehrten Verhältnis zu Recht kritisieren. Etwa im Discovery-Verfahren, wo wir die umgekehrte Problematik haben, dass amerikanische Dienste von europäischen Unternehmen etwas verlangen, was sie nach europäischem Recht nicht liefern dürfen. Wir müssen aufpassen, was da geschieht. Zu den Messenger-Diensten: Die Messenger-Dienste – das ist ja nicht nur WhatsApp – machen aus meiner Sicht auf ein Problem aufmerksam, bei dem möglicherweise Regulierungsbedarf besteht. Nämlich auf die Abgrenzung dessen, was eigentlich noch Telekommunikation ist. Der DAV (*Deutscher Anwaltsverein*) hat sich dazu auch etwas ausführlicher geäußert. Das Problem haben wir schon bei den E-Mails. Bei E-Mails gibt es Bereiche – ich kann hier nur das Stichwort Privatnutzung am Arbeitsplatz nennen – hoher Rechtsunsicherheit, weil wir nicht wissen, ob das noch unter das Telekommunikationsgeheimnis fällt oder nicht. Wir haben dort keine klaren gesetzlichen Grundlagen, eine unübersichtliche Rechtsprechung und keine höchstrichterlichen Entscheidungen. Bei den Messenger-Diensten haben wir das noch verschärft. Hier zeigt sich, dass wir festlegen müssen, wo denn eigentlich Telekommunikation endet.

Was fällt denn eigentlich noch unter Telekommunikation? Das Telekommunikationsrecht enthält ja ganz andere Regulierungen als das Telemedienrecht. Wir brauchen hier eine Grenze und müssen auch aufpassen, dass wir das Telekommunikationsgeheimnis nicht zu weit fassen. Je weiter wir es fassen – und das lässt sich belegen, etwa in der Providerbeschlagnahmeentscheidung des Bundesverfassungsgerichts –, desto schneller wird man dazu kommen, dass die Schranken für Eingriffe in das Telekommunikationsgeheimnis herabgesetzt werden. Das hat dann Rückwirkungen auf die Bereiche, in denen uns das Telekommunikationsgeheimnis besonders wichtig ist. Mit Blick auf die Zeit darf ich mich zunächst hierauf beschränken.

Der **Vorsitzende**: Ja, meine Herren Sachverständigen, ich bedanke mich ganz herzlich für die ersten Ausführungen und auch dafür, dass Sie sich so diszipliniert an die Zeitvorgabe gehalten haben. Aber es ist natürlich nicht ganz so einfach, diese wichtigen Ausführungen in der Kürze der Zeit zu vermitteln. Deswegen eröffne ich jetzt die Aussprache. Ich bitte die Abgeordneten, jeweils immer zu sagen, an wen die Frage oder die Fragen gehen. Ich eröffne die Aussprache, für die CDU/CSU-Fraktion. Thomas Jarzombek, bitte.

Abg. **Thomas Jarzombek** (CDU/CSU): Herr Vorsitzender, meine Damen und Herren, sehr geehrte Sachverständige. Ich habe sehr vieles gehört, dem man so zustimmen kann. Ich glaube, es ist eine ganz wichtige Botschaft, dass es nicht eine technische Lösung gibt, mit der man alle Probleme lösen kann. Dass diese trügerische Sicherheit bei vielen Dingen, die vorgeschlagen werden und in der Diskussion sind, ein ganz zentrales Problem ist. Hundertprozentige Sicherheit – glaube ich – gibt es nicht. Aber aus Sicht meiner Fraktion ist es wichtig, dass man die Anzahl, die Menge der verschlüsselten Verkehre drastisch nach oben führt. Je mehr verschlüsselte Verkehre wir haben, umso knapper werden die Ressourcen, so etwas am Ende zu knacken. Deshalb ist es unser Ziel zum Verschlüsselungsstandort Nummer eins in der Welt zu werden. Die Frage ist, wie kann man dahin kommen. Während ich gestern Abend eine Veranstaltung hatte, habe ich von der Re:publica häufig auf Twitter den Spruch gelesen „Kondome sind einfacher zu installieren als PGP“ (*Pretty Good Privacy*). Ob das jetzt nun so ist oder nicht, möchte ich hier nicht beschreiben. Ich glaube, dass es bei allen technischen Hilfsmitteln Anwendungsprobleme geben kann. Nichtsdestotrotz glaube ich, dass die Installation von PGP wirklich nur etwas für Hartgesottene ist. Deshalb glaube ich, dass – aus einer ganzen Reihe von Maßnahmen, die sich meine Fraktion vorstellt – es wichtig ist zu sagen, dass wir Verschlüsselung mit einem Klick ermöglichen müssen. Es ist richtig, an der Selbstverantwortung der Menschen zu appellieren. Aber es ist auch einfacher zu machen, nicht so kompliziert wie bisher. Also Verschlüsselung mit einem Klick bei jedem Webmailservice, jedem anderen Dienst, der E-Mails auf unserem Rechtsgebiet innehat. Als Zweites eine Verschlüsselungspflicht der E-Mail Provider – nicht nur die, die bei der De-Mail beteiligt sind, sondern aller. Das ist dann zwar nicht Ende-zu-Ende, aber zumindest die Verkehre werden alle verschlüsselt. Deshalb jetzt meine Frage an Herrn Kurschildgen, ob Verschlüsselung mit einem Klick technisch möglich ist. Ich weiß, dass das eine Herausforderung darstellt. Aber ist so etwas denkbar? Und meine Frage an Professor Härting: Unser erstes Ziel wäre natürlich so etwas im Rahmen von Selbstverpflichtungen herbeizuführen. Aber wäre es möglich, sowohl für das Thema „Verschlüsselung mit einem Klick“ wie für die Verschlüsselung zwischen den E-Mail Providern zur Not auch eine gesetzliche Lösung zu verabreden?

Der **Vorsitzende**: Ich freue mich, dass wir heute so in Bildern sprechen, das ist sehr schön. Ich gebe das Wort jetzt an die Fraktion DIE LINKE. Bitte, Halina Wawzyniak.

Abg. **Halina Wawzyniak** (DIE LINKE.): Ich sage vorweg, dass sich die erste Frage an Herrn Schröder, die zweite Frage an Herrn Neumann richtet. In der Projektgruppe Zugang, Struktur und Sicherheit im Netz hat sich die Internet-Enquete unter dem Rubrum „Spionage“ mit Spionageangriffen befasst. Damals ist man auf Grundlage des Verfassungsschutzberichts davon ausgegangen, dass die Mehrzahl der Spionageangriffe aus dem Ausland, aus Russland und China, kommen. Ich könnte jetzt lange Ausführungen zum Verfassungsschutz und seiner Analysegenauigkeit machen, das ist aber heute kein Thema. Die Drucksache ist nun ungefähr ein Jahr alt. Wir haben die

Enthüllung von Edward Snowden, und wir wissen, dass die Angreifer – ich formuliere es mal vorsichtig – nicht nur in China und Russland sitzen. Die Frage zum Thema wäre jetzt eigentlich, ob das Ausmaß der Überwachung der Internetkommunikation, wie wir es jetzt durch Geheimdienste erlebt haben, die Infrastruktur einschließlich Soft- und Hardware nicht komplett kompromittiert hat. Und – wenn das so ist –, was man dagegen machen kann. Zweite Frage dann an Herrn Neumann. Es ist vorhin das sogenannte Schengen-Routing angesprochen worden. Nun wissen wir, dass der Bundesnachrichtendienst (BND) berechtigt ist, die Kommunikation mit dem Ausland bis zu einer Höhe von 20 Prozent des gesamten Traffics zu überwachen. Wir wissen auch, dass der Überwachung der Kommunikation im Ausland selbst keine Grenzen gesetzt sind. Wir wissen zudem, dass es eine Kooperation von Nachrichtendiensten gibt. Ich könnte das jetzt noch länger ausführen. Die Frage ist nun, ob ein Schengen-Routing überhaupt geeignet ist, um der bekanntgewordenen Massenüberwachung zu begegnen.

Der **Vorsitzende**: Vielen Dank. Herr Reichenbach, Sie haben das Wort für die SPD-Fraktion.

Abg. **Gerold Reichenbach** (SPD): Die erste Frage geht an Herrn Dr. Gaycken. Wenn ich Sie richtig verstehe, schlagen Sie eine ziemliche Umstrukturierung der Architektur, auch der Sicherheitsarchitektur des bestehenden Netzes oder der digitalen Kommunikation, vor. Das erinnert mich ein bisschen an das Beispiel von Schiller, der sagt, wir können ja nicht von vorne anfangen. Also das heißt, wir müssen sozusagen die Uhr umbauen, während sie weiterläuft. Die Räder austauschen, während sie weiterlaufen. Deswegen würde mich interessieren, wo Sie operativ die ersten Schritte sehen. Das heißt, an welcher Stelle ist es denkbar und machbar, das so zu strukturieren, dass wir einen Sicherheitsgewinn bekommen, ohne alles von Anfang an zu machen. Um in dem Bild zu bleiben: Erst einmal alle raus aus der Stadt – und dann bauen wir wieder neu auf. Die zweite Frage geht an Herrn Prof. Härting. Sie haben gesagt, die EU-Datenschutzgrundverordnung hat zunächst einmal nichts mit dem Sicherheitsbereich zu tun. Ihr Beispiel hat aber dann deutlich gemacht, dass es sehr wohl etwas damit zu tun hat. Wir haben Public Private Partnerships. Unternehmen sammeln aus dem Interesse der Verkaufsförderung hier in Europa oder in Deutschland möglichst viele Daten über Individuen, um deren Verhalten zu steuern oder vorhersagen zu können. Dann sitzen in Amerika Dienste, die sagen, dass die Daten für sie genauso interessant sind, weil auch sie ein Interesse daran haben, deren Verhalten vorherzusagen. Es geht dann aber nicht um Kaufverhalten, sondern um die Frage, ob möglicherweise Terroristen darunter sind. Und diese Dienste greifen dann legal auf die Daten zu. Wir haben ja momentan auch umgekehrt die Debatte bei der Frage des NSA-Untersuchungsausschusses. Macht sich ein deutscher Abgeordneter nach amerikanischem Recht strafbar, wenn er seinen demokratischen Pflichten nachgeht? Deswegen sind meine Fragen:
a) Lassen sich der öffentliche und der private Bereich überhaupt noch trennen, so, wie Sie dies in Ihrer Systematik getan haben, weil wir eine immer stärkere Beschränkung haben?
b) Kann es ein Argument sein, dass amerikanische Unternehmen in Konflikte geraten und wir dann sagen, wir unterlassen das? Beim Steuerrecht fallen denen viele Geschäftskonstruktionen ein, wie sie Konflikte vermeiden können. Kann man nicht eher sagen, aus Sicherheitsgründen ist das ein Problem, das die Unternehmen lösen müssen, wenn sie in zwei konfliktäre Rechtsbereiche kommen?

Der **Vorsitzende**: Vielen Dank. Konstantin von Notz für die Fraktion BÜNDNIS 90/DIE GRÜNEN.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender, vielen Dank an die Herren für die Expertise und die Ausführungen. Ich wollte ganz kurz noch anmerken, dass man an dieser Rückmeldung von Interessierten einmal sieht, wie wichtig dieses Thema für die Öffentlichkeit ist, wie wichtig insgesamt die Themen dieses Ausschusses für die Öffentlichkeit sind. Deswegen sollten wir wirklich versuchen, so oft wie möglich transparent und offen zu tagen, damit die Menschen daran teilhaben können, was wir hier besprechen. Ich wollte ganz kurz eine Anmerkung machen, weil das Wort Datenschutzgrundverordnung so oft gefallen ist. Ich teile absolut die Einschätzung von Herrn Prof. Härting, dass man sich damit nicht gegen staatliche, geheimdienstliche Überwachung wehren kann. Das ist ja

einer von zwei Vorschlägen von Frau Merkel gewesen. Einmal dieses bilaterale Abkommen und dann die Datenschutzgrundverordnung. Das ist untauglich. Die Datenschutzgrundverordnung ist unter anderen Gesichtspunkten ein sehr wichtiges Verfahren, aber bei der Abwehr staatlicher Spionage hilft sie nicht. Ich möchte zwei Fragen an Linus Neumann stellen. Bei der Diskussion, die wir hier vor gar nicht allzu langer Zeit zur De-Mail geführt haben – manche Kolleginnen und Kollegen erinnern sich –, ging es viel darum, ob Ende-zu-Ende verschlüsselt werden soll oder nicht. Und da gab es zwei Argumente, die ins Feld geführt wurden, warum man das nicht machen wollte. Das erste war, dass es teuer für die Unternehmen ist und man es deswegen nicht in das Gesetz geschrieben hat. Das zweite war, dass es schlecht für die Sicherheitsbehörden ist, denn dann können die ja nicht mehr reingucken. Da stellt sich dem Laien die Frage, ob es eventuell im Hinblick auf die Verletzlichkeit der Infrastruktur einen Interessenskonflikt mit den Sicherheitsbehörden gibt. Wenn wir überlegen, dass Firmen, die Schadware herstellen, teilweise von staatlichen Institutionen beauftragt werden, diese Schadware herzustellen, die sie dann erst den deutschen Sicherheitsbehörden und danach ins Ausland verkaufen, und diese dann irgendwo anders noch auftaucht, ob da eigentlich ein strukturelles Problem gegeben ist. Zieht der Staat im Hinblick auf Schadprogramme eine klare Grenze? Meine zweite Frage ist, ob nicht der Umstand kurios ist, dass von staatlicher Seite – nicht zwingend deutsche Sicherheitsbehörden – mit Steuergeldern die Sicherheit des Internets aufgebohrt wird, man Trojaner kauft, versendet und ähnliches und vielleicht sogar Einfluss auf Telekommunikationsunternehmen nimmt, und auf der anderen Seite privaten Unternehmen und Privatleuten rät: „Schützt Euch doch, kauft Euch Programme, rüstet Euch hoch gegen unsere Angriffe, dann seit Ihr geschützt“. Ob da nicht ein Widerspruch in der Debatte liegt? Und wie geht man den am besten an? Vielen Dank.

Der **Vorsitzende**: Damit sind wir am Ende unserer ersten Fragerunde, und ich bitte nun, in der Reihenfolge zu antworten. Erst einmal die Fragen von Herrn Jarzombek an Herrn Kurschildgen und Herrn Prof. Härting. Bitteschön, Herr Kurschildgen.

SV **Pascal Kurschildgen**: Vielen Dank für das Wort. Herr Jarzombek, vielen Dank für die Frage. So einfach, wie die Frage nach einer Ein-Klick-Verschlüsselung durch Nutzer gestellt ist, so komplex ist aus meiner Sicht die Umsetzung. Die Nutzer müssten ihr komplettes Verhalten erst einmal grundsätzlich ändern. Das bedeutet, dass schöne Absenden der E-Mails über EDV-Geräte, über ein Smartphone, wäre damit so schnell und so einfach gar nicht möglich. Das heißt, das Aufsetzen einer Ein-Klick-Verschlüsselung auf bestehende Apps, Programme, die es schon gibt, das ist aus meiner Sicht erst einmal gar nicht möglich. Es muss etwas vollkommen Neues geschaffen werden. Es muss erst einmal auf einen gemeinsamen Nenner heruntergebrochen werden. Mit einer Browseranwendung, wie man es von den ganz normalen kostenlosen Maildiensten kennt, kann man im Webbrowser gewisse Funktionen wie Ein-Klick-Verschlüsselungsfunktionen einbinden. Da gibt es mittlerweile sogar technische Lösungen, die bereits patentiert sind. Was es für eine Verschlüsselungslösung für Endanwender im Bereich der Browsernutzung gibt, kann man auch in meiner Stellungnahme lesen, in die ich einen entsprechenden Link mit eingefügt habe.
In der Theorie gibt es das auch schon. So wie es aussieht, wird das auch demnächst auf den Markt kommen. Allerdings ist da die angesprochene Transportverschlüsselung mindestens genauso wichtig. Also nicht nur die End-User-Sicht ist wichtig, denn wir reden ja über eine Ende-zu-Ende-Verschlüsselung. Die Frage ist, brauchen wir eine Ende-zu-Ende-Verschlüsselung und können wir diese überhaupt umsetzen. Eine Ende-zu-Ende-Verschlüsselung ist aus meiner Sicht generell eine Verschlüsselung zwischen Absender und Empfänger. Wenn wir jetzt zum Beispiel das Thema De-Mail nehmen, über die viele sagen, dass es ja eine Ende-zu-Ende-Verschlüsselung ist und wir ja die Ein-Klick-Lösung haben. Die besteht aber faktisch einfach nicht, weil die Verschlüsselung aufgebrochen wird. Das heißt, zwischendurch kann jemand mitlesen. Damit ist aus meiner Sicht die Vertraulichkeit in diesem Bereich nicht mehr gegeben, da die Verschlüsselung aufgebrochen wird. Das heißt, eine richtige Ende-zu-Ende-Verschlüsselung ist ein Schutz vor Einsichtnahme durch Dritte, wer auch immer das ist. Jetzt haben wir gerade eben in der Frage gehört, ob wir eine richtige Ende-zu-Ende-Verschlüsselung

überhaupt einsetzen können. Wir haben natürlich auch Behörden, Nachrichtendienste, Geheimdienste, deren Zweck und deren Aufgabe es ist, solche Informationen abzufangen. Wenn wir jetzt unsere Ende-zu-Ende-Verschlüsselung großartig aufbauen und installieren, wie greifen die dann in Zukunft auf unsere Daten zu? Dann kaufen sie sich eben einen Staatstrojaner oder bauen sich irgendeinen Keylogger und holen dann nachher beim Endkunden im Grunde an der Tastatur die E-Mails und die Nachrichten ab. 100 Prozent Sicherheit bekommen wir nicht. Wir müssen aber in die Nähe davon kommen. Wenn wir eine Ein-Klick-Lösung haben wollen, müssen wir das Nutzerverhalten ändern, d. h. die Nutzer dürfen einfach nicht mehr ihr gewohntes Verhalten an den Tag legen, was die Außenstehenden dann ausnutzen, um an Informationen zu kommen. Alteingefahrene Verfahren, unsichere Smartphones, alte Protokolle – warum gibt es das? Weil wir mit alten Protokollen arbeiten müssen, weil wir als Mensch faul sind, uns nicht weiterbilden wollen, alte Programme nutzen wollen oder vielleicht auch nicht anders können. Dann müssen wir abwärtskompatibel sein. Das ist in diesem Fall dann alles nicht mehr gegeben. Das heißt, wir müssen auch ein kleines Stück in dem Bereich – was Herr Dr. Gaycken gesagt hat – die IT von Grund auf neu gestalten. Das wäre aus meiner Sicht erst einmal ein harscher Eingriff. Aber so eine Ein-Klick-Lösung für Nutzer anzubieten, ist eine Marktlücke,und als Ziel gar nicht so weit weg. Es ist aus meiner Sicht auch technisch machbar. Um es abschließend zu formulieren: Ja, es ist möglich, aber es ist mit Schmerzen für die Nutzer verbunden, die dann ihr Verhalten ändern müssen. Ob die Nutzer das mitmachen, ist natürlich die andere Frage. Es ist nicht mehr schön, es ist nicht mehr komfortabel. Mal eben eine E-Mail abzusetzen, mal eben eine Nachricht an jemanden zu senden, ist dann so nicht möglich. Man muss sich mit einem sehr guten Passwort – welches man sich merken muss – an einem sicheren System einloggen. Ich kann dann nicht im Intercafé an irgendeiner Mittelmeerküste vertrauliche Nachrichten absetzen. Das heißt, mit einer Ein-Klick-Lösung kann hier die Vertraulichkeit nicht sichergestellt werden. Die Vertraulichkeit ist für mich nur gegeben, wenn wir eine richtige Ende-zu-Ende-Verschlüsselung haben, und die können wir meines Wissens nach derzeit ausschließlich durch Browseranwendungen umsetzen. Das ist heute der Stand der Technik. Man möge mich eines Besseren belehren, was nächste Woche auf den Markt kommt, aber heute stehen wir grundsätzlich an dem Punkt, dass so eine Lösung denkbar und anwendbar wäre.

Der **Vorsitzende**: Vielen Dank. Herr Prof. Härting, bitte.

SV **Prof. Niko Härting**: Mit mittlerweile mehr als 15 Jahren Hintergrund zu Fragen des Internetrechts bin ich ein großer Skeptiker, was bei der Verschlüsselung das Regulatorische angeht. Denn wir haben ja bereits einen Erfahrungsschatz. Wir hatten im Jahr 1997 das Signaturgesetz, da war Deutschland Vorreiter. Ich habe es damals mit Mühe kommentiert. Es hat nie eine praktische Anwendung gefunden. Ich will die Reihe nicht fortsetzen, aber alle Versuche, auf regulatorischem Wege die Bürger zur Verschlüsselung anzuhalten, sind bislang misslungen. Das ist ein Erfahrungsschatz, den man sehr genau im Auge behalten sollte, wenn man hier zur Verschlüsselung über Regulierungsmaßnahmen spricht.

(*Zwischenruf*)Abg. **Thomas Jarzombek** (CDU/CSU): Das ist aber keine Antwort auf meine Frage.

SV **Prof. Niko Härting**: Keine Antwort auf die Frage? Dann habe ich Sie nicht richtig verstanden.

Der **Vorsitzende**: (*an Abg. Thomas Jarzombek (CDU/CSU) gerichtet*) Sie möchten die Frage präzisieren? Bitte schön.

Abg. **Thomas Jarzombek** (CDU/CSU): Genau. Die Frage der Akzeptanz ist das Eine, auch beim Signaturgesetz, das Sie anführen. Meine Frage war aber, wäre es – als zweitbeste Lösung – möglich, so etwas gesetzlich oder regulatorisch zu machen? Ich würde es jetzt als „Ja“ verstehen.

SV **Prof. Niko Härting**: Selbstverständlich ist das möglich. Da haben wir den Erfahrungsschatz. Aber wir haben eben auch den Erfahrungsschatz, was das auf dem Papier stehende Gesetz und die

Wirklichkeit und deren Verhältnis zueinander angeht.

Der **Vorsitzende**: Vielen Dank. Ich begrüße auch die Vizepräsidentin des Deutschen Bundestages, Frau Petra Pau, heute in ihrer Funktion als stellvertretendes Mitglied in unserem Ausschuss. Herzlich Willkommen, Frau Pau. Und jetzt können wir gleich die Fragen von Frau Wawzyniak von der Fraktion DIE LINKE. beantworten. Das machen Herr Schröder und Herr Neumann. Bitte, Herr Schröder, Sie haben das Wort.

SV **Thomas Schröder**: Vielen Dank. Die Frage war, was alles kompromittiert ist oder wie es mit dem Ausmaß aussieht. Was können Geheimdienste – und nicht nur die Geheimdienste aus Russland und China – grundsätzlich so anrichten? Ob nun alles kompromittiert ist, lässt sich so natürlich schwer sagen. Wenn man das wissen würde, könnte man die Probleme ja beheben. Aber wir sehen anhand der Veröffentlichungen aus dem Snowden-Fundus, dass die National Security Agency (NSA) sehr eindeutige Forschungen in die Richtung betreibt, langfristig Netzwerkkomponenten und auch Softwareprodukte mit Hintertüren auszustatten und somit zu kompromittieren. Ich versuche einfach mal ein wenig aufzuschlüsseln, was für Möglichkeiten es überhaupt gibt, oder wo man grundsätzlich ansetzen würde, um beispielsweise eine Kommunikation zu belauschen. Das, was ganz am Anfang bekannt wurde, ist, dass die Geheimdienste möglicherweise physikalischen Zugriff auf die Unterseekabel haben – also die Glasfaserleitungen, über die die Daten transferiert werden – und dort, an diesen sehr zentralen Knotenpunkten, in der Lage sind, mitzulesen. Die Technik für so etwas ist vorhanden und mittlerweile auch erschwinglich. Das heißt, nicht nur für Regierungen, sondern auch für private Wirtschaftsunternehmen ist es grundsätzlich möglich, an solchen Glasfaserleitungen mit hohen Geschwindigkeiten die Daten mitzulesen und auch zu speichern. Wobei das mit dem Speichern und Verarbeiten der Daten sicherlich die größte Herausforderung ist. Was für einen Stand der Technik die Geheimdienste und insbesondere die NSA da haben, ist mir natürlich nicht bekannt. Aber bei einem physikalischen Zugriff auf die Leitungen und auf die Netzwerkgeräte ist ja grundsätzlich schon eine ganze Menge möglich, was das Mitlesen oder auch Einleiten von bösartigen Inhalten angeht. Bei Softwaresystemen ist es so, dass immer mehr Kryptografie gefördert und gefordert wird. Hier sehen sich die Dienste in der Situation, dass sie nicht wissen, wie sie diese Kommunikation am Ende noch unbemerkt mitlesen können. Deswegen ist es natürlich plausibel, dass man – wie es auch die deutschen Strafverfolgungsbehörden fordern – an der Quelle ansetzt, also dort, wo die Kommunikation terminiert oder eben initiiert wird, also hier Hintertüren einzubauen oder eben Software zu haben, die Daten auswertet. Man kann über die Bereitschaft von Betriebssystemherstellern – also geschlossener Betriebssysteme, die nicht quelloffen sind – mit irgendwelchen Behörden zu kooperieren, nur spekulieren. Man kann aber grundsätzlich davon ausgehen, dass so etwas durchaus denkbar ist. Aber auch in quelloffenen Betriebssystemen und Bibliotheken können Hintertüren eingebaut werden, möglicherweise ganz gezielt durch Geheimdienste. Es gibt regelrechte Wettbewerbe, wie man am besten ein Stück Code so programmiert, dass es nicht wie eine Hintertür, sondern wie ein Programmierfehler aussieht. Diese sogenannten „Underhanded C Contests“ finden jährlich statt. Danach kann man im Internet suchen. Das erklärte Ziel dieser Wettbewerbe ist es, eine Hintertür einzubauen oder einen Seitenkanal zu öffnen. Am Ende muss der Source Code, also die Quellen, einem Audit standhalten. Sollte diese Hintertür dennoch gefunden werden, soll es eben aussehen wie ein Fehler. Bei dem Open-SSL-Fehler, der kürzlich öffentlich bekannt wurde, dieser Heartbleed-Attacke, kamen derartige Spekulationen auf. Da wurden die Thesen aufgestellt, dass der Programmierer – ein deutscher Open Source-Entwickler, der das irgendwie im Rahmen seines Studiums programmiert hat – für irgendwelche Dienste arbeitet. Das ist natürlich reine Spekulation und nicht gerade fair gegenüber diesem Open Source Entwickler. Man sollte diese Leute nicht an den Pranger stellen, gerade in so komplexen kryptografischen Funktionen, die ein guter
C-Programmierer zwar lesen, aber nicht verstehen kann, weil zu viel Mathematik dahinter steckt. Da kann man sehr viele Fehler einbauen, die nicht so offensichtlich sind, aber Seitenkanäle öffnen. Das heißt, dass man nicht direkt, aber über andere Kanäle Informationen erlangen kann, um ein System

am Ende zu kompromittieren. Ich denke, dass das auch eine Forschung ist die z. B. die NSA anstrebt. Es gibt diverse Entwicklungen bei der NSA. Darauf kann man aufgrund der Snowden-Veröffentlichung schließen. Da wurden Expertensysteme entwickelt, die quasi wie eine künstliche Intelligenz sind – nur nicht ganz so ausgereift. Das heißt, es gibt eine Wissensdatenbank und dieses Expertensystem. Das Expertensystem erweitert die eigene Wissensdatenbank permanent durch die massenhafte Überwachung des Internetverkehrs und ist am Ende selbstständig in der Lage, anhand bestimmter Muster Aktionen durchzuführen. Zum Beispiel eben das gezielte Angreifen von bestimmten Netzwerkkomponenten oder bestimmten Computern, die an einer Kommunikation beteiligt sind. Das ist natürlich ein ganz massiver Schritt in die Automatisierung von elektronischer oder digitaler Kriegsführung. Diese autonomen Drohnen, die überwachen und möglicherweise später auch Waffen abfeuern dürfen – das hier wäre quasi so ein System im Internet, in der digitalen Welt, welches in der Lage ist, autonom zu agieren. Die NSA hat ein riesengroßes Budget zur Verfügung, um solche Forschungen zu unterstützen. Das DATA und JAPA fördert auch ganz gezielt Open Source-Projekte und bringt sich da möglicherweise auch mit Ideen ein, die eventuell sogar schädlich sind. Aber das ist alles Spekulation. Man weiß nicht, was alles kompromittiert ist oder kompromittiert werden kann. Es kann grundsätzlich jedoch alles kompromittiert werden. Für die Geheimdienste sind natürlich vor allen Dingen auch Netzwerkkomponenten interessant. Das sind Knotenpunkte in Netzwerken, an denen man auch sehr gezielt Daten einleiten kann. Wenn beispielsweise man selbst oder eben dieses Expertensystem der Meinung ist, dass es da eine bestimmte Zielperson gibt, und es gibt ein riesengroßes Netzwerk, durch dass die Daten gehen, dann kann – zum Beispiel die NSA – an einem bestimmten Punkt in diesem Netzwerk initiieren, dass eine Hintertür auf dem Computer des Verdächtigten installiert wird, ohne dass ein richterlicher Beschluss vorliegt. Grundsätzlich ist das natürlich nicht nur die NSA, die diese Bestrebung hat. Ich denke, dass auch der inländische Geheimdienst ähnliche Interessen hat. Ich bin da auch der festen Überzeugung, dass die Bestrebung – die wir und auch das BSI haben – die Sicherheit grundsätzlich zu erhöhen, in einem großen Interessenskonflikt zu dem steht, was die inländischen Geheimdienste und Strafverfolgungsbehörden so wünschen. Damit möchte ich schließen.

Der **Vorsitzende**: Vielen Dank. Herr Neumann, Sie haben das Wort.

SV **Linus Neumann**: Darf ich jetzt nur auf die Frage von Frau Wawzyniak antworten oder auch auf die beiden Fragen von Herrn Dr. von Notz?

Der **Vorsitzende**: Bitte erst einmal nur auf die Frage von Frau Wawzyniak.

SV **Linus Neumann**: Das war die Frage nach dem Schengen-Routing. Hierbei geht es darum zu sagen, wenn unser unverschlüsselter Internetdatenverkehr innerhalb von Europa oder Deutschland durch die USA geleitet und dort analysiert wird, dann versuchen wir das dadurch zu verhindern, indem wir ihn nicht mehr da durchschicken. Das klingt zunächst nach einer ganz sinnvollen Maßnahme. Jetzt stellt man sich natürlich die Frage, wieso geht dieser Verkehr, dieses Datenpaket, das von einem deutschen Server an einen anderen deutschen Server gehen soll, überhaupt durch die USA? Der Grund dafür ist darin zu suchen, dass amerikanische Anbieter günstigere Angebote für Internetanbieter machen, Verbindungen zu jedem anderen Punkt im Internet herzustellen. Wir haben die Deutsche Telekom, die sagt, es gibt Pearing-Punkte in Deutschland, in Frankfurt, da legen alle ihre Kabel hin, stecken die dort aneinander und wir haben deutsches Internet. Die Telekom sagt, wir haben so viele Kunden, wir brauchen doch gar nicht unser Kabel dahin zu legen. Wer sich mit uns verbinden möchte, der kann doch bitte sein Kabel zu uns legen, denn wir haben unser Datenzentrum einfach woanders hingestellt. Das heißt, wir möchten nicht mit der Konkurrenz verbunden werden, wenn sie nicht bereit ist, dafür zu bezahlen. Wir haben außerdem noch das Dienstangebot, diese Kabel auch zu legen. Das heißt, der Grund für einen Anbieter, Traffic durch die USA zu senden, ist, dass die andere Möglichkeit, das mit der Telekom direkt zu machen, einfach zu teuer ist. Das ist ein ganz normaler Marktmechanismus, da musste die USA gar nichts tun. Das heißt, die deutschen Anbieter gehen hin und sagen, ok, wir pearen nicht mit der Telekom, wir zahlen da nichts für, sondern wir schicken unsere

Daten eben durchs Ausland. Das muss leider auch möglich sein, denn wenn sich jetzt ausgerechnet die Telekom hinstellt und sagt, macht doch Schengen-Routing, macht doch Deutschland-Routing, dann ist das natürlich eine Überlegung, hinter der auch wirtschaftliche Interessen stehen. Und das ist vor allem etwas, was genau diese Zentralisierung – die uns genau an diesen Punkt gebracht hat, an dem wir jetzt das Problem haben – vorantreibt. Das heißt, man lernt nicht aus dem Fehler des Paradigmas, dem gerade gefolgt wurde, sondern man zentralisiert es einfach noch mehr. Dies hat den Seiteneffekt – und darauf zielte die Frage ja auch ab –, dass dann immer mehr Daten in die Hände unserer Überwachungsinfrastrukturen gehen, dass die deutschen Dienste einen besseren statt einen schlechteren Ansatz haben zu überwachen. Wie macht man es nun richtig? Ziel von Sicherheit ist, dass der Transportweg egal ist. Wenn Ihnen ein System angeboten wird, bei dem der Transportweg nicht egal ist, dann hat dieses Sicherheitssystem ein Problem. Insofern halte ich diesen Vorschlag des Schengen-Routings für eine der vielen Maßnahmen der Deutschen Telekom, sich aus diesem Skandal, aus dieser Bedrohung für die deutschen Bürger, selbst einen wirtschaftlichen Vorteil zu verschaffen, der in diesem Falle dann mit Maßnahmen versucht wird zu erreichen, die sicherlich nicht besonders zielführend sind.

Der **Vorsitzende**: Vielen Dank. Auf die Fragen von Kollegen Reichenbach antworten Herr Dr. Gaycken und Herr Prof. Härting. Herr Gaycken, Sie haben das Wort.

SV **Dr. Sandro Gaycken**: Vielen Dank, Herr Reichenbach, für die Frage. Das ist natürlich eine der größten Fragen, die in dem Bereich bestehen und die auch international gerade in der Diskussion steht. Es gibt zum Beispiel am MIT (*Massachusetts Institute of Technology*) das Crashprogramm von Howard Throw, das auch entsprechende Technologien entwickelt und auch das Problem hat, diese Technologien auf den Markt zu bringen. Wir haben aber einige Bereiche, wo eine Implementierung, eine Neuimplementierung möglich wäre. Das gilt für Bereiche, die ein Security-Refitting brauchen, die also besonders sicherheitskritisch sind, zum Beispiel der Euro-Fighter oder die Führungsunterstützungssysteme der Bundeswehr, andere militärische Systeme, auch viele Systeme im Aero Space. Die machen sich jetzt sehr sorgfältig Gedanken darüber, wie sie sich etwas besser sichern können. Da nützt natürlich Verschlüsselung nicht viel. Denn wenn bei einer Ende-zu-Ende-Verschlüsselung die beiden Enden kreuzunsicher sind und mehrere hunderttausend kritische Sicherheitslücken drin haben – das haben wir leider im Moment in vielen kritischen Systemen –, dann nützt auch der Zwischenweg einer sicheren Kommunikation leider nicht viel. Das sind Bereiche, wo man durchaus sehr dankbar für entsprechende Ansätze wäre, die dann eine sehr viel höhere Basissicherheit liefern und Angriffe sehr viel schwieriger machen. Glücklicherweise haben wir im Moment einige neue Wellen der Innovation in IT, mit denen völlig neue Bereiche aufkommen. Bereiche, in denen man sozusagen noch einmal anfangen könnte, wenn man das wollte, und in denen auch neue Akteure auftreten, die sehr viel stärker sicherheitskritisch sind. Hier in Deutschland sind das vor allem die beiden Wellen „Industrie 4.0“ und „Smart irgendwas“, Smart-Cities, Smart-Autos, Smart-whatever. Und zum Zweiten auch die Welle der Informatisierung der Schwellen- und Entwicklungsländer. Die sind jetzt sehr intensiv dabei, sich damit auszustatten. Wir wissen, dass die erste, zweite und dritte Frage, die diese den IT-Lobbyisten immer stellen, die Frage nach der Sicherheit, der Sicherheit und der Sicherheit ist. Viele von diesen Ländern leben in einer etwas unbequemeren Sicherheitssituation als wir und machen sich da sehr viel umfangreicher Sorgen. Für uns bedeutet das, dass unsere deutsche Industrie – insbesondere in den Bereichen Maschinenbau, Aero Space, Defense und Autobau – diese neuen Paradigmen annehmen könnte und dort hochsichere IT in den Bereichen „Industrial IT“ und „Embedded IT“ einbringen könnte. Das sind also Bereiche, wo diese IT-Legacy aus Windows, Intel, SAP nicht so stark ist, wo diese auch zur Disposition steht und es schon viele Ansätze gibt, wo man Hochsicherheits-IT implementieren kann. Das sind im Moment so ein wenig die Hoffnungsträger, um dort eine hochsichere Hardwareebene, hochsichere Betriebssysteme – die im Übrigen auch schneller sind als kommerzielle Betriebssysteme – und hochsichere Anwendungsbereiche einzuziehen. Da wird sehr intensiv darüber nachgedacht. Man will diese Technologien dort eventuell entwickeln. Man ist dort gerade in der Prüfungs- und Konzeptionsphase, dazu dann auch

Strategien für eine Migration von unsicheren Systemen zu Systemen zu entwickeln. Ich mache eventuell für die NATO eine solche Studie für eine Migration von einer unsicheren NATO auf der Basis von Windows und Intel hin zu einer sicheren NATO auf Basis hochsicherer Komponenten. Das gleiche geht auch für die Bundeswehr, als eine ökonomische Strategie, bei der man schaut, wie man in einem Zeitraum von fünf bis acht Jahren mit den Mitteln, die man dafür zur Verfügung hat, einen entsprechenden Wechsel hinbekommt. Das ist also eine ökonomische Aufgabe. Glücklicherweise gibt es dafür jetzt – im Gegensatz zu vor zwei Jahren – eine Reihe von Interessenten. Es gibt vertiefte, konzeptionelle Gespräche zum Beispiel mit verschiedenen DAX-Unternehmen, auch mit den Militärs, die ein hohes Interesse und eine Strategie haben, um das zu realisieren. Das Interesse bei unseren Unternehmen, insbesondere im Maschinenbau, liegt natürlich im Export. Die haben ganz klar gesehen, dass das nicht nur eine Sache der Sicherheit ist. Das ist zwar schön und nett, aber dafür gibt man nicht so viel Geld aus. Denn so ein Refitting ist sehr teuer. Die haben erkannt, dass das auch eine ganz massive Lücke im Exportmarkt ist, die gerade von den konventionellen Spielern, die hier in Deutschland als Konkurrenz auftreten, nicht bedient werden kann. Keiner will hochsichere IT aus den USA, aus Russland oder aus China haben – egal, was die da versprechen und wie viel Transparenz die uns hinlegen. Frankreich macht auch viel Industriespionage. Der nächste große Akteur wäre Deutschland. Wir genießen ein großes Vertrauen. Nicht überall, aber unser BND ist zumindest nicht ganz so aktiv wie die anderen, und das ist für uns eine große Marktlücke. Es gibt also nicht nur eine Frage der Verantwortung, sondern auch eine große Opportunität in der Industrie.

Der **Vorsitzende**: Ja, vielen Dank. Wenn wir noch eine zweite Runde machen wollen, dann müssen wir uns doch ein bisschen kürzer fassen. Es kommt noch eine zweite Runde mit allen Fraktionen und die Beantwortung wird auch noch eine Weile dauern. Herr Prof. Härting, Sie haben das Wort. Vielleicht können Sie sich ein bisschen kürzer fassen?

SV **Prof. Niko Härting**: Das bitten Sie ausgerechnet einen Juristen.

Der **Vorsitzende**: In der Tat, eine Herausforderung.

SV **Prof. Niko Härting**: Ich versuche es trotzdem. Herr Reichenbach, wir unterhalten uns über Vorschriften, die auf europäischer Ebene geplant sind, die es Google unter Strafdrohung untersagen sollen, Daten europäischer Bürger an amerikanische Behörden weiterzugeben. Ich glaube nicht, dass es richtig ist, in diesem Zusammenhang von einer Public Private Partnership zu sprechen, sondern eher von einer Public Private Zwangsehe. Denn der Zwang kommt durch amerikanische Gesetze, die Google und andere Anbieter dazu verpflichten, diese Daten herauszugeben. Was würden wir eigentlich im umgekehrten Verhältnis sagen? Denn diese Public Private Zwangsehe haben wir in Deutschland auch. Die Telekom und andere Anbieter müssen in großem Umfang Daten herausgeben, wenn sie dazu aufgefordert werden, und dürfen darüber auch nicht plaudern. Was würden wir eigentlich sagen, wenn die Russen jetzt kommen und sagen, wir verbieten es der Telekom und anderen Telekommunikationsanbietern, Daten russischer Bürger an deutsche Behörden herauszugeben und sanktionieren das mit einer Strafe von fünf Prozent des Bruttoumsatzes, den die Telekom weltweit jedes Jahr macht. Was würden wir dann sagen? Insofern glaube ich nicht, dass es richtig ist, in diesem Zusammenhang von Partnership zu sprechen.

Der **Vorsitzende**: Vielen Dank. Herr Neumann, Sie haben jetzt noch zwei Fragen von Herrn Dr. Konstantin von Notz zu beantworten. Sie haben aber nicht die doppelte Zeit.

SV **Linus Neumann**: Die erste Frage zielte auf Ende-zu-Ende-Verschlüsselung ab. Dazu habe ich jetzt gerade schon zwei interessante Wortmeldungen gehört. Herr Dr. Gaycken sagt, Ende-zu-Ende-Verschlüsselung hilft nicht, wenn beide Enden kompromittiert sind. Kleiner Hinweis: Es reicht, wenn eins kompromittiert ist. Herr Kurschildgen sagt, es ist kompliziert, und man braucht Nutzerwissen dafür. Meine Herren, das Scheunentor ist offen, die Hütte brennt. Wir reden hier nicht von irgendeinem NATO-Einsatz. Wir reden von Massenüberwachung der gesamten Bevölkerung. Wenn wir dagegen etwas tun wollen, dann ist es

völlig in Ordnung, einfach opportunistisch zu verschlüsseln. Verschlüsselung für die Masse – zack, einfache Lösung. Es ist überhaupt gar kein Problem, das auszurollen. Die Lösungen dafür sind auch da. Schauen Sie sich das an. Ich kann heute an meinem iPhone in einen App-Store gehen und kostenlos Applikationen für Ende-zu-Ende verschlüsselte Kurznachrichtendienste und Ende-zu-Ende verschlüsselte Voice-Dienste bekommen. Eine dieser Applikationen wird bald von der Deutschen Telekom angeboten. Das heißt, wenn die das auch anbieten, dann kann man das jetzt wirklich machen. So, das heißt, indem ich mein Smartphone nehme, App-Store klicke und sage, „Einmal verschlüsseltes Telefon, einmal verschlüsselte Kurznachrichten“, wären wir bei der Ein-Tap-Lösung. Wofür ich aber plädieren würde, ist die Null-Tap-Lösung. Wenn ich das Ganze auf meinem Telefon installieren kann, dann kann es auf diesem Telefon auch schon drauf sein, wenn ich es im Laden kaufe. Genau das wird die Deutsche Telekom hoffentlich bald auch machen. Also Null-Klick Ende-zu-Ende-Verschlüsselung ist das, wofür ich plädiere. Und der Markt zeigt, dass wir diesen einen Klick auch noch wegbekommen. Die zweite Frage zielte darauf ab – das war, glaube ich, einer kleinen Anfrage der Linksfraktion zu verdanken, bei der Frau Wawzyniak auch nicht unbeteiligt war –, dass festgestellt wurde, dass die Firma Computer Sciences Corporation (CSC), die unter anderem gute Verbindung zu den US-amerikanischen Geheimdiensten hat, sowohl an der Entwicklung von De-Mail beteiligt war als auch an der Entwicklung des Staatstrojaners. Das heißt, wir haben hier zwei Paradigmen von Sicherheit. Einmal möchte sich der Bürger vor dem Staat oder vor einem Angreifer schützen, und einmal hält der Staat den Bürger für einen Angreifer. Diese beiden Paradigmen sind nicht in Einklang zu bringen. Man kann das sehr schön sehen, die Nutzer, die Menschen wollen ihnen ja vertrauen. Wenn das Bundesamt für Sicherheit in der Informationstechnik etwas sagt, dann möchten die Nutzer dem vertrauen. Die versuchen auch, diesen Empfehlungen zu folgen. Nur weil wir als CCC da irgendwie eine Minute draufgucken und sagen, das ist doch Quatsch, dann ist es natürlich auch ein Problem für die Nutzer, die hier nicht wissen, wem sie vertrauen sollen. Entschuldigung, wenn ich Sie da jetzt mal kurz zitiere, Herr Hanke. Sie wurden (*in Frage Nr. 7 des Fragenkatalog*) zur Initiative „E-Mail made in Germany“ gefragt. Sie sagen, die teilnehmenden Provider verschlüsseln E-Mails auf dem Transportweg, auf den Servern der Anbieter liegen die E-Mails dagegen in Klartext vor. Das ist die notwendige Antwort auf diese Frage. Damit ist das Thema auch erledigt, weil gesagt wird, wo die Sicherheitsschwachstelle liegt. Danach geben Sie dann zusätzlich zu diesen zwei Zeilen korrekter Antwort vier Zeilen Antwort, um irgendwie zu rechtfertigen, dass es schon ok ist, wenn die Deutsche Telekom das macht. Ich wünsche mir ein Bundesamt für Sicherheit in der Informationstechnik, das nicht gezwungen ist, irgendwie herum zu lavieren, um diese irgendwie halbsicheren Sachen irgendwie zu rechtfertigen. Deswegen hoffe ich, dass Sie bald in einer vollständig unabhängigen Behörde arbeiten, die nicht auf Weisungen des Bundesinnenministeriums Rücksicht nehmen muss.

Der **Vorsitzende**: Vielen Dank. Herr Hange, Sie sind angesprochen worden, haben Sie den Wunsch zu erwidern?

SV **Michael Hange**: Ja, das habe ich. Ich hatte ja in meinem Eingangsstatement noch einmal deutlich gemacht, dass die Kommunikationssicherheit, die Kryptografie, eine wichtige Bedeutung hat, dass aber der Schutz vor Cyberangriffen gleichwertig zu sehen ist. Das, was ich hier geschrieben habe, meine ich auch so. Das war nicht auf Weisung, sondern das meine ich so. Was oft nicht bedacht wird ist, dass es auch eine Konkurrenzsituation zwischen Verschlüsselung – also Kommunikationssicherheit – und Cybersicherheit gibt. Sie sind in einem großen Kommunikationsraum mit vertrauenswürdigen und nicht vertrauenswürdigen Teilnehmern. Wir gehen von mehr als einer Million infizierter PC oder IT-Systeme in Deutschland aus. Jeder Angriff – ich sage mal, jeder Cyberangriff – kann erst auf dem Endsystem auf entsprechende Schadprogramme untersucht werden, weil erst hier die Verschlüsselung wieder weggenommen wird. Das heißt nicht, dass ich keine Ende-zu-Ende-Verschlüsselung will. Es ist für mich nur eine etwas dogmatisch geführte Diskussion. Die Transportverschlüsselung, auch Ende-zu-Ende-Verschlüsselung, hat ihren Wert – und die Option hierzu muss auch auf jeden Fall vorhanden sein. Ich greife noch einmal das auf, was

Herr Härting gesagt hat: Digitale Signaturen. Wir waren begeistert dabei, haben einen ganzen Sommer mit allen Experten gerungen. Es sind nicht alleine die wirtschaftlichen Aspekte gewesen, sondern der Nutzer hat es nicht gewollt. Wechseln Sie einmal Zertifikate, das ist nicht so trivial. Es geht einfacher. Ich halte auch die Richtung für absolut richtig, dass wir versuchen, es einfacher zu machen. Aber selbst in der Verwaltung hatten wir ein Verschlüsselungskonzept für alle vorgesehen. Wir sind praktisch an dem Nutzerverhalten gescheitert, dass man sich mit der Zertifikatsstruktur nicht auseinandersetzen will. Warum nutzen wir alle SSL mit Webdiensten? Weil es einfach ist. Aber wir bauen damit auf das Vertrauen des Anbieters. Ich glaube, dies ist auch ein ganz wesentlicher Punkt bei der Kryptografie. Wir haben die Algorithmen im Griff, aber die Implementierung und auch die Infrastruktur dahinter haben wir nicht im Griff. Wenn man bedenkt, dass es in Browsern so und so viele Zertifizierungsstellen gibt, die wir gar nicht kennen, auch deren Sicherheit wir nicht kennen, haben wir ein Problem. Wir fahren – ich benutze jetzt auch ein Bild – im Grunde in einer Kutsche ohne Dach und hoffen, dass der Regen uns nicht erwischt. So ist es zurzeit mit E-Mail und auch mit GSM. Für mich ist es wichtig, jetzt nicht einen dialektischen Konflikt zwischen Experten zur Ende-zu-Ende-Verschlüsselung zu führen. Für mich hat beides einen Stellenwert. In den Regierungsnetzen haben wir auch die Transportverschlüsselung, um an verschiedenen Stellen – nicht nur beim Endnutzer – einfach Schadprogramme herausfiltern zu können.

Der **Vorsitzende**: Ja. Vielen Dank für die erste Runde. Ich würde vorschlagen, dass wir mit Blick auf die Zeit jetzt nur noch eine Frage stellen. Sonst schaffen wir die Beantwortung nicht mehr. Also eine Frage an einen Sachverständigen. Es beginnt Marian Wendt für die CDU/CSU-Fraktion.

Abg. **Marian Wendt** (CDU/CSU): Vielen Dank. Herr Kurschildgen und auch Herr Hanke, Präsident des BSI. Es geht uns um Aufklärungskampagnen, die Sie beide ansprechen, die Sie auch in Ihrer Behörde, im BSI, anbieten. Da ist meines Erachtens noch viel zu tun, Sie schildern es ja auch jeweils. Denn wir alle können viel machen. Der Staat hat umfangreiche Anlagen zum Schutz seiner Telekommunikation bzw. der Verwaltung. Aber im Endeffekt funktioniert das ganze System der Sicherheit im Internet ja nur, wenn auch der Nutzer, das schwächste Glied der Kette, eine gewisse Vorbildung hat. Sie sprachen von Schulbildungsplänen, da müssen wir noch mit Frau Wanka sprechen. Vielleicht könnten Sie jeweils kurz skizzieren, wie solche Aufklärungskampagnen oder Imagekampagnen aussehen könnten. Sie haben da ja bereits erste Erfahrungen. Sie haben ein Portal, aber es ist meines Erachtens noch nicht ganz so ausgeprägt. Die Frage ist auch, ob das eher durch Telekommunikationsunternehmen gefahren werden sollte oder zum Beispiel das Innenministerium entsprechende Kampagnen für mehr Sicherheit im Netz fahren sollte, um die Bürger auch auf die verschiedenen Dienste aufmerksam zu machen. Vielen Dank.

Der **Vorsitzende**: Herr Behrens, Sie haben das Wort.

Abg. **Herbert Behrens** (DIE LINKE.): Meine Frage geht an Thorsten Schröder. Es geht noch einmal – auch auf Grundlage der sehr konkreten Fragen, die wir an Sie gerichtet haben – um den Handlungsbedarf. Wo kommen wir mit welchen Instrumenten voran. Nun hat der Präsident, Herr Hange, in einer der Antworten darüber gesprochen, dass Identitätsdiebstähle am besten dadurch vermieden werden, wenn man – analog zum Verfahren beim elektronischen Personalausweis – diese Art der Sicherung nutzt. Auch das Beispiel De-Mail wird hier als mögliches empfehlenswertes Instrument genannt, was den vertraulichen Versand von Nachrichten betrifft. Mich würde Ihre Stellungnahme dazu interessieren. Ist es wirklich ein sicheres Instrument, über das wir hier diskutieren, wenn wir über den elektronischen Personalausweis reden? Oder gibt es möglicherweise Schwachstellen. Wenn ja, welche?

Der **Vorsitzende**: Frau Kollegin Kampmann für die SPD-Fraktion.

Abg. **Christina Kampmann** (SPD): Meine Frage war identisch mit der von Herrn Wendt, deshalb können wir das Verfahren an der Stelle abkürzen.

Der **Vorsitzende**: Dann ist jetzt Herr Janecek dran.

Abg. **Dieter Janecek** (BÜNDNIS 90/DIE GRÜNEN): Meine Frage richtet sich an Dr. Gaycken. Sie haben ja das Thema „Industrie 4.0“ adressiert und damit auch den Kontext dafür hergestellt, dass wir IT-Sicherheit unter dem Aspekt diskutieren, dass wir digitale Infrastrukturen in vielen Bereichen aufbauen. Da gibt es von der BITKOM diese fünf Säulen – Energie, Verkehr, Mobilität, Gesundheit – und eben auch die Industrie. Meine Frage ist, wenn ich jetzt zum Beispiel mit dem Deutschen Bankenverband spreche, dann sagen die mir, welche Beträge sie in die neuen Infrastrukturen investieren. Das wird dazu führen, dass es einen Verdrängungswettbewerb geben wird, dass auch manche Banken z. B. in diesem Bereich möglicherweise so nicht mehr existieren. Das betrifft auch andere Bereiche der Industrie. Siemens hat heute ganz klar gesagt, dass Industrie 4.0 unser Schwerpunkt ist. Aber beim gesamten Mittelstand, z. B. auch im Süden Deutschlands, wo ich herkomme, da ist das Thema nicht auf dem Schirm. Es stellt sich also die Frage nach den Kosten. Ist das ein Faktor, der auch im Wettbewerb zunehmend zu einem Thema für deutsche Unternehmen wird? Das ist die eine Frage. Und die andere Frage ist, dass ich ganz oft höre, die Deutschen hätten jetzt eine Chance im Bereich der IT-Security. Aber ist die IT-Security Branche in Deutschland so aufgestellt, dass diese wirklich zu einem Player werden kann, der machtvoll mit anderen konkurriert? Das ist bislang noch nicht mein Eindruck.

Der **Vorsitzende**: Die Frage für die SPD, die offen geblieben ist, kann Herr Schipanski jetzt stellen.

Abg. **Tankred Schipanski** (CDU/CSU**)**: Dann darf ich an unseren Sachverständigen, Herrn Kurschildgen, eine Frage richten. Diese bezieht sich auf die sehr gute schriftliche Stellungnahme, die Sie abgegeben haben. Darin unterscheiden Sie bei der Transportverschlüsselung zwischen unseren jetzigen Kommunikationsinfrastrukturen, bei denen wir gesetzte Standards haben – auch wenn die über 20 Jahre alt sind –, verweisen aber im gleichen Zusammenhang darauf, dass sich bei den mobilen Lösungen faktisch noch nichts entwickelt hat, dass wir da keinen etablierten Standard haben und es somit nicht ohne weiteres möglich ist, plattformübergreifend verschlüsselt zu kommunizieren. Vielleicht könnten Sie dazu noch einige erläuternde Ausführungen machen. Sie unterscheiden ferner zwischen der Transportverschlüsselung und der Verschlüsselung bei der Speicherung von Daten – anscheinend auf dem Rechner. Vielleicht können Sie da noch aufzeigen, ob dies das gleiche Verschlüsselungssystem betrifft oder ob es da wiederum andere Möglichkeiten gibt. Sie verweisen im gleichen Atemzug darauf, dass die Bundesdruckerei mit einem leicht zu bedienenden Personalausweis und Sicherheitszertifikaten einen unterstützenden Beitrag dabei leisten kann. Auch da wäre ich für eine Erläuterung dankbar.

Der **Vorsitzende**: Vielen Dank. Herr Präsident Hange, Sie beantworten bitte die Frage von Herrn Wendt.

SV **Michael Hange:** Es geht dort um Kampagnen, wie man IT-Sicherheit bewusster macht. Ich glaube, man muss es in beide Richtungen sehen. Man muss also zum einen in Richtung der Anbieter deutlich machen, was man erwartet – wobei ich das nicht alleine auf den Personalausweis abstelle. Auch Sicherheitstoken sind durchaus möglich. Das zweite ist, dass man sich in Sachen Kryptografie einmal anschaut, was vorhanden ist, auch unter Open Source, und dass man Initiativen unterstützt, in denen solche Software entwickelt wird. Das machen wir auch, jetzt auch auf Linux – also Open Source – ausgerichtet. Wir würden das gerne auch auf die anderen Betriebssysteme ausrichten, um eine breitere Anwendung zu ermöglichen. Ganz wesentlich, und das ist eine Gesamtaufgabe, ist wirklich, IT-Sicherheit als qualitätsdifferenzierendes Merkmal an die Anbieter heranzutragen und dass wir durch gesetzgeberische Maßnahmen sehr viel erreichen. Wir müssen Anreize schaffen, damit Sicherheit sich lohnt. Die Verkehrserziehung Anfang der 70er-Jahre gibt dort ein Beispiel. Ich kann mich daran erinnern, dass die Einführung des Sicherheitsgurtes im Grunde auch eine ähnlich dialektische Diskussion hervorgerufen hat. Ich glaube, wir müssen Anreize geben – sowohl für Anbieter wie auch für Kunden. Bei unseren Kampagnen zur Öffentlichkeitsarbeit – das sage ich selbstkritisch – erreichen wir ca. 10 bis 20 Prozent der Bevölkerung nicht. Diese lassen ihre Rechner ungeschützt. Das sind über eine Million Rechner. Diese eine Million Rechner stellen im Grunde auch eine Gefährdung für die anderen

dar, wenn sie z. B. in Botnetzen zusammengebündelt Systeme angreifen.

Der **Vorsitzende**: Jetzt hat das Wort der Herr Schröder für die Beantwortung der Frage von Herrn Behrens.

SV **Thorsten Schröder**: Vielen Dank. Ich versuche, mich kurz zu fassen. Die Frage ist, ob Verfahren wie De-Mail oder der neue Personalausweis geeignet sind, die Sicherheit der Kommunikation im Internet und unserer Online-Identität zu erhöhen. Ich möchte das nicht unbedingt bejahen. Grundsätzlich bietet der nPA Möglichkeiten, damit auch tolle Dinge zu machen. Aber es hat bislang noch keiner wirklich etwas Sinnvolles damit implementiert. Mit dem nPA bleiben Restrisiken, die von all den Herstellern und Institutionen, die diesen Personalausweis bewerben, bislang immer unterdrückt werden. Bei De-Mail und auch beim nPA gibt es sehr irreführende Werbung. Ich habe hier nur ein Zitat für De-Mail, welches ich kurz aus meinem Statement vorlesen möchte: „De-Mails können nicht von Dritten abgefangen und verändert werden, weil sie auf ihrem Weg durch das Internet immer verschlüsselt sind.“ Die Quelle ist die De-Mail-Webseite. Das steht da ganz groß drauf und suggeriert der Bevölkerung und den Anwendern, dass sie sich in Sicherheit wähnen können. Das gleiche gilt für den nPA. Während der Internet-Enquete hatten wir dieses Thema mit dem Identitätsdiebstahl schon einmal angesprochen. Der Mirko Manske vom Bundeskriminalamt (BKA) hatte berichtet, dass das eins der größten Themen ist, mit denen sich das BKA derzeit auseinandersetzt. Er stimmte mir auch ein Stück weit zu, dass der nPA den Online-Identitätsdiebstahl im Grunde auch ein bisschen begünstigt. Denn er zwängt der Bevölkerung quasi mehr oder weniger eine digitale Identität auf. Im Moment ist es eben nicht rechtlich vorgeschrieben, einen Signaturschlüssel auf der Karte zu haben, aber das könnte ja durchaus später noch einmal kommen. Das heißt grundsätzlich auch, dass den Leuten, die gar keine digitale Signatur oder eine Online-Identität benötigen, etwas aufgezwängt wird, obwohl es da Restrisiken gibt. Das gilt auch für andere Secure-Token-Verfahren. Das hatte ich vor Jahren schon einmal mit dem CCC demonstriert, als wir über entfernte Computer die entsprechenden Lesegeräte übernehmen und Signaturen leisten konnten. Es ist einfach die Frage, ob es vorteilhafter für die Opfer von solchen Straftaten oder Identitätsdiebstählen ist, die dann jedoch größere Schwierigkeiten haben zu widerlegen, dass sie irgendeine Signatur geleistet haben. Grundsätzlich denke ich, die Sensibilisierung sollte ausgebaut werden, so dass die Benutzer sich über Restrisiken bewusst sind und entsprechend vorsichtig handeln – auch mit vermeintlichen Sicherheitsfeatures. Ich würde behaupten, dass De-Mail – schon alleine, weil es ein sehr zentraler Dienst ist – nicht unbedingt geeignet ist, die Sicherheit merklich zu erhöhen.

Der **Vorsitzende**: Vielen Dank. Herr Dr. Gaycken, Sie beantworten bitte die Frage von Herrn Janecek.

SV **Dr. Sandro Gaycken**: Ein Wettbewerbsvorteil für kleine und mittlere Unternehmen ist durchaus gegeben. Im Moment müssen die großen Daxer den Kern machen, weil die Startinvestitionen minimal bei zwei Milliarden, im Idealfall bei drei Milliarden liegen. Das können die kleinen und mittleren Unternehmen natürlich nicht. Aber die Idee ist durchaus schon da, sie kommt jetzt in die Konzeptionsphase, wie man eine Dissemination, also eine Verbreitung des dafür notwendigen Wissens, in die Subunternehmer hinein bekommt. Denn das ist natürlich die Struktur, auf der die großen Unternehmen fußen. Dann muss es eine entsprechende Streuung geben, die es auch den mittleren Unternehmen ermöglicht daran mitzuarbeiten und mit diesen Werkzeugen zu arbeiten. Eine zentrale Maßnahme, die dabei wahrscheinlich ergriffen wird, ist, dass die Kerne davon einfach Open Source und damit allen zur Verfügung gestellt werden. Das ist auch für die großen Unternehmen im Moment die Idee, dass es für sie eigentlich maximal profitabel ist, wenn sie die Fachexpertise in den kleinen und mittleren Unternehmen dadurch abholen, dass sie diese Werkzeuge verfügbar machen. Sie selbst stellen die Kernstrukturen und können nach freien Marktprinzipien beliefert werden. Die Human Ressource ist natürlich ein riesiges Problem. Für die Entwicklung brauchen wir jetzt erst einmal nicht so viele Leute. Das kann man mit den Kreisen machen, die in der Forschung und Entwicklung vorhanden sind. Da gab es immer wieder viele kleine Projekte und Nischen, die man jetzt herausholen und in entsprechende Prozesse einbetten kann. Da

gibt es wahrscheinlich auch ein paar, aber nicht ganz so gravierende Probleme. Schwieriger ist es dann natürlich, wenn man diese Produkte in den Betrieb gibt, in die normale Welt oder auch in eine größere Gemeinschaft von Entwicklern. Da ist es sicherlich schwierig, eine entsprechende Kenntnis vorauszusetzen. Wir versuchen, diese Dinge so workforce-kompatibel wie möglich zu machen. Das ist eine der Prioritäten bei der Entwicklung. Das also wirklich auch der Operateur damit umgehen kann. Es wird aber schon noch ein wenig Spezialwissen nötig sein. Es wäre generell auch wünschenswert – dies vielleicht auch als Hinweis an den Bundestag –, generell mehr Wissen über IT-Sicherheit, über sichere Entwicklung an den Universitäten zu fördern. Die Nachwuchssituation in diesem Bereich ist insgesamt sehr schlecht.

Der **Vorsitzende**: Es ist noch eine Frage offen. Es sind zwar noch viele Fragen offen, aber eine ist noch für heute offen. Und zwar von Herrn Schipanski an Herrn Kurschildgen. Bitte.

SV **Pascal Kurschildgen**: Vielen Dank. Ich versuche, mich noch einmal kurz zu halten. Es ist ja eigentlich eine Frage nach der Erläuterung, was ich in meiner Ausführung gemeint habe. Das Zusammenspiel zwischen Transportverschlüsselung und lokaler Verschlüsselung. Es ist heute der Tag der Bildsprache. Wir haben heute eine Nachricht, eine Information, die wollen wir verschlüsselt übertragen. Das heißt, wir nehmen eine Information in einer Nachricht, schmeißen die Nachricht in ein Auto, einen Transporter hinein, schließen ab und behalten den Schlüssel. Wir wissen, auf der Gegenseite hat jemand anderes auch einen Schlüssel, um den Transporter aufzuschließen und um die Nachricht zu lesen. Das heißt, damit ist die Nachricht erst einmal grundsätzlich verschlüsselt. Und wenn ich das Ganze noch super absichern möchte, dann habe ich eine Transportverschlüsselung und fahre mit dem Transporter in einen Tunnel hinein, der vorne einen Wachmann hat, der aufpasst, dass keiner im Tunnel wartet und mich abfängt. Auf der anderen Seite habe ich auch wieder einen, der aufpasst, dass der Transporter, der vorne hineingefahren ist, hinten wieder herauskommt. Mittendrin passiert nichts. Das ist die Transportverschlüsselung. Auf dem Weg wird erst einmal nichts verändert. Jetzt haben wir das Problem der lokalen Verschlüsselung. Die lokale Verschlüsselung bedeutet, den Transporter, den ich vorher abgeschlossen und durch einen sicheren Tunnel gefahren habe, stelle ich über Nacht auf einen nicht gesicherten Parkplatz ab und hoffe, dass mir den keiner knackt und die Informationen klaut. Das heißt, hier greift jetzt die lokale Verschlüsselung. Ich muss natürlich auch die Nachricht, die ich transportiert habe, irgendwie lokal verschlüsselt ablegen, damit keiner während meiner persönlichen Abwesenheit diese Information lesen kann. Da kommt dann die Frage nach den Protokollen und was es da alles gibt. Bei der Transportverschlüsselung handelt es sich um die erste Schutzschicht, die man einsetzen muss und einsetzen kann. Das ist das, was „E-Mail made in Deutschland“ meint. Es tut mir manchmal weh, wenn ich das höre, aber generell ist das die Umsetzung eines alten Standards, der schon längst hätte Standard sein müssen, weil dieser eingesetzt werden kann oder eingesetzt wird. Das ist die Grundlage für die Transportverschlüsselung. Für die E-Mail-Verschlüsselung selbst müssen wir andere Programme nehmen. Da haben wir andere Verschlüsselungsalgorithmen. Da haben wir wieder die bekannten PGP, S-Mime und was es da so auf dem Markt gibt. Das sind wieder ganz andere Programme, mit denen der User sich dann befassen muss. Transportverschlüsselung muss der User sich aneignen. Bei der Inhaltsverschlüsselung und bei der lokalen Verschlüsselung reden wir dann wieder von einem anderen Produkt. Da reden wir über Produkte aus dem Open Source-Bereich, vielleicht Truecrypt. Da habe ich eine Festplattenverschlüsselung, die ich einsetzen muss, um den auf dem Parkplatz abgestellten Transporter auch so zu sichern, dass keiner die Information lesen kann. Da reden wir über viele Produkte, über viele Verschlüsselungslösungen, die man einsetzen kann. Das Problem ist immer noch die lokale Verschlüsselung, deswegen der Schwenk zur mobilen Sicherheit. Hier haben wir extreme Probleme, weil die Hersteller selbst nichts Übergreifendes anbieten und teilweise noch sehr große Sicherheitslücken bestehen. Dazu kam ja eben auch schon einmal – von Herrn Schröder, glaube ich – der Hinweis, dass mobile Sicherheit manchmal ein bisschen tricky ist. Ein aktuelles Beispiel: Jeder denkt, dass sein verschlüsseltes iPhone auch

sicher ist, und dass die drauf gespeicherten Informationen mit der Passwortverschlüsselung gespeichert sind. Das ist mitnichten der Fall. E-Mail-Anhänge liegen im Klartext auf jedem verschlüsselten i-Phone einfach so herum. Jeder kann die auslesen. Die kann sich jeder abholen, der das Ding in der Hand hält. Auch wenn es ein 18-Zeichen-Passwort gibt, ist es kein Hindernis, die E-Mail-Anhänge auszulesen. Da fängt es schon an. Da machen die sich einfach keine Gedanken drum. Oder die machen sich schon Gedanken, es ist aber schwer in der Umsetzung, weil das Userverhalten geändert werden muss. Das heißt, verschlüsselte E-Mail-Anhänge führen dazu, dass ich als User es wieder schwerer habe, an einen Nachrichteninhalt heranzukommen, mehr Passwörter eingeben muss. Das heißt, wir geben – und nicht nur wir, sondern die Hersteller der ganzen mobilen Branche – die Sicherheit ein wenig auf, um die Userexperience hochzuhalten, das heißt, die User einfach nur ein schönes Gerät in der Hand halten zu lassen, um schön und schnell kommunizieren zu können. Klar, wir können auch mit S-MIME E-Mails versenden, aber trotzdem kann ich auf meinem iPhone PGP E-Mails nicht lesen. Das geht nicht so einfach. Es geht schon, aber es tut weh. Es tut richtig weh, eine PGP-verschlüsselte Nachricht lesen zu wollen. Das ist gar nicht so einfach. Den nPA, den ich bei einer anderen Frage auch erwähnt habe, sehe ich als ergänzende Lösung als gar nicht so schlecht an. Ganz wichtig: Eine grundsätzliche Sicherheit kann nur gewährleistet werden, wenn ich mich an einem System mit einer Drei-Faktor-Authentifizierung anmelde. Das ist jetzt nichts Neues, das kennen wir alle. Wir kennen alle die Standardauthentifizierungsmöglichkeiten. Mit dem, was ich weiß, mit dem, was ich habe, und mit dem was ich bin, kann ich mich an einem System authentifizieren. Dummerweise haben viele gedacht, super, mit dem, was ich habe – nämlich mit dem elektronischen Ausweis – kann ich mich doch einfach irgendwo anmelden. Das geht aber nicht, weil die drei Mechanismen mit dem, was ich weiß, mit dem, was ich habe und mit dem, was ich bin, eigentlich zusammen eingesetzt werden müssen. Das heißt, ich muss mit dem, was ich weiß – ein Passwort eingeben –, mit dem, was ich habe – meinen nPA irgendwo vorhalten – und dem, was ich bin – vielleicht auch noch meinen Fingerdruck irgendwo abgeben. Diese drei Faktoren zusammengezogen sind eine recht gute Lösung, um sich eindeutig identifizieren zu können. Leider wird die Authentifizierung meistens auf einen Faktor reduziert. Standardmäßig ist das immer noch das Passwort. Es ist immer noch das Beste, denn auf etwas anderes können wir uns nicht reduzieren. Fingerabdrücke können wir nachmachen, das haben meine Kollegen aus dem CCC gezeigt. Es ist ganz einfach, einen Fingerabdruck nachzumachen. Darauf können wir uns nicht verlassen. Und sich nur auf den nPA verlassen, darauf, dass ich mich mit dem irgendwo anmelden kann, das sollte man auch tunlichst vermeiden. Das heißt, der nPA ist nur eine unterstützende Maßnahme. Er ist nicht das Sicherheitsmerkmal, aber er ist ein Baustein einer Sicherheitslösung. Ich denke, damit habe ich die Fragen kurz erläutert. Dankeschön.

Der **Vorsitzende**: Das war nahezu eine Punktlandung. Eineinhalb Stunden haben wir gebraucht, haben wir auch eingeplant für diese Veranstaltung. Es sind natürlich viele Fragen offen geblieben. Es zeigt sich, dass das Thema IT-Sicherheit eines der Topthemen bei der Digitalen Agenda bleiben wird. Um die Chancen im Internet und bei der Digitalisierung zu nutzen, brauchen wir ein sicheres Internet, damit sich Nutzer und Anbieter frei und sicher im Internet bewegen können. Ich bedanke mich ganz herzlich im Namen aller Fraktionen bei Ihnen, bei den Sachverständigen, für Ihre Auskünfte. Es ist immer gut, wenn man Fach- und Sachverstand vermittelt bekommt. Jetzt bleibt natürlich die Frage, was ist die Aufgabe der Politik? Da müssen wir eine Abwägung treffen. Das ist unsere Aufgabe. Nicht nur in diesem Ausschuss, sondern auch in den anderen Ausschüssen, insbesondere im Innenausschuss. Ich bedanke mich ganz herzlich für Ihre Zuarbeit bei den Fragen, für Ihre Antworten. Ich bedanke mich auch bei den Zuschauern hier auf der Tribüne, aber natürlich auch im anderen Saal, und insbesondere bei denen, die den Live-Stream verfolgt haben. Herzlichen Dank und alles Gute. Die Sitzung ist beendet.

Schluss der Sitzung: 16:12 Uhr

Jens Koeppen, MdB
**Vorsitzender**