Deutscher Bundestag

17. Wahlperiode

Enquete-Kommission

Internet und digitale Gesellschaft

Projektgruppe Zugang, Struktur und Sicherheit im Netz

Protokoll

des

öffentlichen Expertengesprächs

Berlin, den 28. November 2011, 15.00 – 19.00 Uhr

Sitzungsort: Berlin, Konrad-Adenauer-Str. 1, Paul-Löbe-Haus

Sitzungssaal: E. 400

Vorsitz: SV Harald Lemke

Vor Eintritt in die Tagesordnung

Der **Vorsitzende, SV Harald Lemke,** eröffnet die Sitzung und begrüßt namentlich die sechs eingeladenen Sachverständigen, die Mitglieder der Projektgruppe Zugang, Struktur und Sicherheit im Netz sowie die anwesende Öffentlichkeit.

Anschließend erläutert der **Vorsitzende** den formalen Ablauf des Expertengesprächs. Zunächst hätten die anzuhörenden Sachverständigen Gelegenheit zu einem fünfminütigen Statement. Im Anschluss daran könne jeder Fragen an die sachverständigen Anhörpersonen richten.

Nachdem es gegen das formale Vorgehen keine Einwände seitens der Projektgruppe gibt, leitet der **Vorsitzende** zum ersten Tagesordnungspunkt über.

TOP 1 Expertengespräch

Der **Vorsitzende** erteilt **Prof. Dr. Dirk Heckmann** das Wort.

Prof. Dr. Dirk Heckmann erklärt, er halte es für eine hervorragende Möglichkeit für die Wissenschaft, sich durch die Teilnahme am Expertengespräch in die Arbeit der Enquete-Kommission einbringen zu können. Er weist darauf hin, dass das von ihm eingereichte Gutachten zunächst dazu dienen solle, auf Inhalte hinzuweisen, die in einer mündlichen Sitzung nicht zur Sprache kämen. Wie es sich für einen Juristen gehöre, setze er an den Anfang seiner Ausführungen einen Disclaimer. Ihm seien drei Fragen gestellt worden. Er könne und wolle davon nur zwei tiefgründig beantworten, da die erste Frage nicht zu seinen Forschungsschwerpunkten gehöre. Allein die Ausgangsfrage, welchen Beitrag das Recht zu einem sicheren Internet leisten könne, sei sehr breit angelegt und kaum in kurzer Zeit zu beantworten. Bereits der Gegenstand des Schutzes müsse näher bestimmt werden. Auch die Frage, was das Internet unter dem Blickwinkel eines sicheren Internets sei, sei zu beantworten.

Auch für den Juristen gehe es diesbezüglich um die Infrastruktur, die Anwendungsebene sowie die Sicherheit von Software und Hardware. Dies sei natürlich sehr breit angelegt und je nach Ebene, die man in den Blick nehme, unterschiedlich zu beantworten. Der Begriff der Sicherheit sei ein unbestimmter und werde im Recht nur teilweise definiert. Es stelle sich die Frage, ob man über die Funktionsfähigkeit des Netzwerkes oder auch über den Schutz von Rechtsgütern, die durch die Internetnutzung gefährdet seien, spreche. Schließlich müsse erörtert werden, durch wen und wie das spätere Schutzniveau bestimmt werden solle. Die allgemeine Aussage, es gebe keine 100-prozentige Sicherheit, sei zwar korrekt, helfe aber in diesem Kontext nicht weiter.

Prof. Dr. Dirk Heckmann sagt, dass er vor diesem Hintergrund eine Konkretisierung vornehmen wolle. Internetsicherheit verstehe er als selbstreguliertes Risikomanagement der Nutznießer mit subsidiärer staatlicher Verantwortung. Dahinter stehe ein abgestuftes Schutzpflichtenkonzept, dass sich aus der Verfassung herleiten lasse, insbesondere aus dem so genannten IT-Grundrecht, welches das Bundesverfassungsgericht im Zusammenhang mit der Onlinedurchsuchung entwickelt habe. Zwar stehe die Schutzpflicht des Staates mittlerweile außer Frage. Problematisch sei aber Umfang und Umsetzung dieser Schutzpflicht, da ein erheblicher Gestaltungsspielraum des Gesetzgebers bestehe.

In seinem Gutachten habe er drei Stufen beschrieben, innerhalb derer die Schutzpflicht des Staates konkretisiert werden könne. Die erste Stufe und Pflicht sei die Entwicklung einer IT-Sicherheitsstrategie, welche Ausdruck eines verfassungsrechtlichen Rationalitätspostulates sei. Der Staat müsse rational handeln, auch und gerade wenn es um IT gehe. Ohne eine solche IT-Sicherheitsstrategie liege eine Verletzung des Untermaßverbotes vor. Seit 2009 existiere eine solche Strategie für den Bereich der kritischen Infrastrukturen. Hinzugekommen sei im Jahr 2011 die so genannte Cyber-Sicherheitsstrategie. Durch diese werde im Grunde die erste Stufe erfüllt. Da aus seiner Sicht verschiedene Aspekte in dieser bisherigen Strategie der Bundesregierung noch nicht ausreichend gewürdigt worden seien, müsse diese womöglich zu einer integrierten Gesamtstrategie weiterentwickelt werden. Es gebe

zum Beispiel den Konflikt zwischen Sicherheit und Komfort. In der heutigen Plug & Play-Umgebung, die zu einer zunehmenden Vernetzung führe, spielten Sicherheitsaspekte eine immer geringere Rolle. Dies liege daran, so erklärt er, dass sich Sicherheit gegen Nützlichkeit und Komfort solcher Umgebungen richte. Des Weiteren bestehe ein Dilemma zwischen Zurechenbarkeit und Anonymität. Es gebe zwar die Pflicht zur Anonymität, aber auch die Pflicht einer gewissen Zurechenbarkeit, wolle man Kriminalität wirksam bekämpfen. Vor dem Hintergrund der Frage, wie diese Konflikte aufzulösen seien, vermisse er strategische Ansätze.

In der zweiten Stufe gehe es um die Implementierung dieser Strategie in konkrete Mechanismen und Regeln. Institutionell werde diese Pflicht neuerdings durch das Nationale Cyberabwehrzentrum erfüllt. Regulatorisch gebe es eine Vielzahl von Einzelnormen, die sich im Laufe der Zeit – schon vor Internetzeiten – entwickelt hätten und nicht immer miteinander korrespondierten. Die Herausforderung bestehe von staatlicher Seite in der Schaffung eines IT-Sicherheitsgesetzes. Dieser Vorschlag, so betont er, sei als verbindende Klammer gedacht, um einige Grundsätze entwickeln zu können, durch die die Anwendung der bestehenden Vorschriften auch erleichtert werde.

Schließlich kommt **Prof. Dr. Dirk Heckmann** zur dritten Stufe, die er als Hilfe zur Selbsthilfe bezeichnen wolle. Da das Internet zunächst eine private Angelegenheit sei, dass durch Privatpersonen und private Unternehmen reguliert werde und reguliert werden könne, sei vom Staat Zurückhaltung geboten. Der Staat müsse die Personen jedoch in die Lage versetzen, selbst schützend tätig zu werden. Dies geschehe bereits in Einzelfällen, beispielsweise gebe es zum Thema Industriespionage Leitfäden der Verfassungsschutzämter, das BSI (Bundesamt für die Sicherheit in der Informationstechnik) stelle das Sicherheitsportal ‚BSI für Bürger' bereit und das Bundesministerium für Wirtschaft und Technologie betreibe die Task Force IT-Sicherheit in der Wirtschaft. Dies seien aber einzelne Themen und Projekte. Dort müsse aus seiner Sicht zunächst nicht mehr unternommen werden. Das Thema sichere Internetnutzung aus Sicht der Bürger sei jedoch bislang vernachlässigt worden. Hierzu habe er im Gutachten einige Ausführungen gemacht.

Der **Vorsitzende** dankt **Prof. Dr. Dirk Heckmann** für das Statement und übergibt das Wort an **Andreas Könen**.

Andreas Könen fasst noch einmal zusammen, dass sich die an ihn gerichteten Fragen einerseits mit Angreifern, andererseits mit der Weiterentwicklung bzw. Entwicklung von Cyberterrorismus und dem Schutz kritischer Infrastrukturen befassten.

Für das BSI stelle sich zunächst die Frage, wie Informationen zu Angreifern gewonnen werden könnten. Das BSI habe die Befugnis zum und gewinne seine Erkenntnisse vornehmlich aus dem Detektieren von Schadsoftware und Angriffen an den Eingängen des Regierungsnetzes. Diese wehre das BSI so gut es gehe ab und habe dadurch die Möglichkeit Angriffe zu analysieren sowie möglicherweise ihren Ursprungsort zu ermitteln.

Weiter führt er aus, dass die Kenntnisse, die das BSI dort gewönne, durch die Zusammenarbeit mit anderen Sicherheitsbehörden gestützt werde. Insbesondere seien das BKA (Bundeskriminalamt), der BND (Bundesnachrichtendienst) und der Bundesverfassungsschutz zu erwähnen, mit denen auch im Cyber-Abwehrzentrum zusammengearbeitet werde. Darüber hinaus dürfe man nicht vergessen, dass in der Zusammenarbeit mit den KRITIS-Unternehmen – mit dem UPKRITIS auf Basis des Nationalen Planes zum Schutz der Informationsinfrastrukturen – ein weiterer Kanal gegeben sei, den man im Rahmen der Cyber-Sicherheitsstrategie und ihrer Umsetzung vertiefen werde. Diese Informationen benötige das BSI dringend, um Angriffe – im Internet, wie es von der Wirtschaft und im Internet, wie es vom Bürger genutzt werde – beurteilen zu können. Man sei darauf angewiesen mit den großen Playern dieser Branche, insbesondere denjenigen, die die Netze zur Verfügung stellten, intensiv zusammenzuarbeiten. Es werde damit eine Lageinformation erzeugt, die im Lagezentrum des BSI bereitgestellt werde. Diese nutze das BSI in erster Linie zur Sicherung behördlicher Einrichtungen des Bundes und der Länder. Andererseits flössen die Informationen wieder zu den Partnern in der Wirtschaft zurück.

Hinsichtlich der Gefährdungslage durch Cyberterrorismus, sei dieser zunächst in einen größeren Zusammenhang einzubetten. Sofern man Cyberterrorismus als Angriffe über das Internet mit Personenschaden, hohem Sachschaden und Gefährdung der staatlichen Ordnung verstehe, sei Cyberterrorismus momentan nicht zu beobachten. Entscheidend sei, dass Cyberterrorismus in die Phänomene der Massenangriffe eingebettet werde, insbesondere in Phishing, Cyberspionage sowie –sabotage. Letztere scheine sich in einigen Bereichen durchaus anzukündigen. Diese weiter gefasste Definition bereite dem BSI insgesamt mehr Kopfzerbrechen als die Frage nach potenziellem Cyberterrorismus im engeren Sinne. Sofern Cyberterrorismus im weiteren Sinne gedeutet werde, so habe es einige Angriffe gegeben, beispielsweise auf Estland und Georgien.

Die dritte Frage, die **Andreas Könen** zugegangen ist, betreffe den zukünftigen Umgang mit kritischen Infrastrukturen. Im Moment spiele Informationstechnik und Sicherheit in der Informationstechnik bei den Aufsichtsbehörden noch keine ausgeprägte Rolle. Ein Blick in die entsprechende Gesetzgebung zeige, dass dort keine durchgängige Abbildung der ITK (Informations- und Telekommunikationstechnologie)-Strukturen erfolge. IKT sei nicht das Objekt, mit dem sich die Aufsichtsbehörden auseinandersetzten. Die Bundesnetzagentur sei hier stärker involviert, da sie sich unmittelbar mit den Providern beschäftige.

Andererseits seien – als Pendant zum Cyber-Abwehrzentrum – in der Wirtschaft ähnlich eingerichtete Institutionen als Single-Points-of-Contact notwendig, die einen relativ klaren Eindruck über die Gefährdungslage bei den Unternehmen gewönnen. Das BSI sei dadurch besser in der Lage, das Verhältnis von Cyberspionage, -sabotage und gegebenenfalls -terrorangriffen gegeneinander abzuwägen.

Er wage daher die Prognose, dass Sabotage durchaus zunehme und eventuell die momentan noch stärker vertretene Spionage überholen könne. Dies seien jedoch große Unsicherheiten, die auch davon abhingen, wie sich die gesamte ITK-Infrastruktur in den kommenden Jahren weiterentwickeln werde.

Diese Themen wolle er gerne diskutieren, auch im Hinblick auf Maßnahmen, die das BSI für kleinere, mittlere und größere Unternehmen in der Cyberzusammenarbeit plane.

Der **Vorsitzende** dankt **Andreas Könen** für das Statement und übergibt das Wort an **Prof. Dr. Jochen H. Schiller**.

Prof. Dr. Jochen H. Schiller erläutert einführend, dass er als Techniker seit etwa 20 Jahren mit dem Bereich Telekommunikation und Mobilkommunikation betraut sei. Der erste Themenkomplex Forschungsbedarf und Erkenntnisdefizite sei daher sehr interessant für ihn. Das Frustrierende sei jedoch, dass es technisch bereits sehr viel Wissen zum Thema Sicherheit gebe. Im Prinzip wisse die Wissenschaft schon seit geraumer Zeit, wie man Daten verschlüssele und Systeme kryptographisch sichere. DoS (Denial-of-Service)-Angriffe klammere er hier aus. Das Hauptproblem sei jedoch, dass das Wissen nicht konsequent umgesetzt werde. Im Bereich Mobilfunk werde heutzutage mit einem System gearbeitet, in dem die Standardisierung ganz klare Anweisungen erteile und Warnungen ausspreche, wann ein Sicherheitsrisiko eintrete. Trotz dieses Wissens halte sich niemand daran. Ein Beispiel sei das Datensystem im Mobilfunkbereich, welches mittels eines Dutzend Android-fähiger Handys lahm gelegt werden könne. Sicherheitskultur werde ebenso wenig gelebt wie Risikokultur. Da das System sehr komplex sei, müsse in der Forschung vor vereinfachten Statistiken zu Angriffsszenarien gewarnt werden. Alle extremen Ereignisse oder neuartigen Angriffe seien prinzipiell nicht mit Statistiken erfassbar , vor allem Domino- und Kaskadeneffekte nicht.

Es gebe folglich noch einige Wissenslücken, die insbesondere mit der Komplexität und Vermischung zusammenhingen. Die Abkehr von den klassischen Kommunikationssystemen hin zu „Alles ist das Internet“ bringe natürlich einige neue interessante Aspekte mit sich. Beispielsweise werfe es auch die Frage auf, wie eine Migration von diesem eigentlich veralteten System des Internets der 70er -und 80er-Jahre auf die neuen Anforderungen gestaltet werden könne. Insofern gebe es technisch in

der Tat noch einige offene Punkte. Interessanter seien natürlich die Fragen nach den Risiken und dem, was die Politik tun könne.

Der zweite Themenkomplex beziehe sich auf kritische Infrastrukturen. **Prof. Dr. Jochen H. Schiller** erläutert, dass dort das so genannte Verletzlichkeitsparadoxon existiere , welches auch in anderen Bereichen gelte. Die Gesellschaft verlasse sich immer stärker auf ein System, was zu einer größeren Verletzlichkeit führe. Im Falle einer Störung seien zunehmend mehr Menschen betroffen. Beispielsweise verließen sich gerade ältere Menschen – von den über 65 Jährigen nutzen über 75 Prozent ein Handy – immer häufiger auf ein automatisches Notrufsysteme. Das Erschreckende daran sei, dass die Netzbetreiber darüber zwar Kenntnis hätten. Die Mehrzahl der Netzbetreiber wisse nach eigenen Angaben eigentlich nicht, was in ihrem System los sei. Nur 10 Prozent der Netzbetreiber gäben zu, dass bis zu 30 Prozent ihrer mobilen Endgeräte vermutlich gekapert seien. Das Hauptproblem sei eine nicht gelebte Sicherheitskultur. Hier könne die Politik ein Initiator sein. Natürlich gehe dies auch nicht ohne Zwang. Mittels Ideen wie dem Cyber Incident Disclosure, also dem Melden gewisser Vorfälle, wie es in manchen Bereichen bereits üblich sei, könne aber sicherlich zu einer besser gelebten Sicherheitskultur beigetragen werden.

Der dritte Bereich beziehe sich auf den Umgang mit Unsicherheiten und die Kommunikation von Risiken. Sicherheitsmanagement höre sich immer gut an und sei ein wesentlicher Baustein der Arbeit des BSI. Im Bereich Sicherheitsmanagement gebe es zwar viele Möglichkeiten. Kleine und mittlere Unternehmen sowie Einzelunternehmer verfügten jedoch über kein Sicherheitsteam und kein großes Sicherheitsmanagement. Demzufolge müssten ganz neue Strategie erdacht werden. Wesentlich seien Strategien, die sich auf das Nichtfunktionieren eines Systems einstellten. Natürlich gebe es keine 100-prozentige Sicherheit, aber das Bewusstsein darüber helfe schon weiter. Gefährlich sei die vereinfachte Aussage, man müsse den risikobewussten Bürger schaffen, der wisse was er tue. Zum einen stelle Sicherheit aus Sicht der meisten Bürgern keinen Mehrwert dar. Zum anderen werde das Hauptproblem, wie sie risikobewußt werden könnten, von ihnen nicht verstanden. Es sei eine schlichte Überforderung für den „normalen“ Bürger, wenn man ihm sa-

ge, er solle ein Teil der Sicherheit werden. Denkbar seien zwar einfache Handlungsanweisungen, aber sicherlich keine komplexen Systeme.

Zuletzt weist **Prof. Dr. Jochen H. Schiller** noch auf die Rolle der Medien hin. Man könne gewisse Sicherheitsvorfälle nicht mehr unter Verschluss halten und hoffen, dass nur die offiziellen Medien darüber berichteten. Die vielen „neuen Medien" könnten sehr schnell die Deutungshoheit bei Vorfällen gewinnen und dies auch unabhängig davon, ob alle Aussagen stimmten. Eine gewisse Meinung und ein Handeln sei dann vorgeprägt und lasse sich nur schwer wieder korrigieren. Daher plädiere auch er als Techniker für eine Strategie in Richtung Sicherheitskultur.

Der **Vorsitzende** dankt **Prof. Dr. Jochen H. Schiller** für das Statement und übergibt das Wort an **Dr. Sandro Gaycken**.

Dr. Sandro Gaycken erklärt, dass er sich als Technik- und Sicherheitsforscher mit den strategischen und taktischen Fragen der Themen Sicherheit und IT-Sicherheit befasse.

Er wendet sich zunächst der ersten Frage nach der Art der Angriffe zu. Zielführend sei vor allem, sich nicht von Mediengeschichten treiben zu lassen, sondern systematisch anzusetzen und zu sehen, welche Angreifer es gebe und mit welchen Interessen und Fähigkeiten diese ausgestattet seien. Anhand der Identifizierung verschiedener Klassen von Angreifern, sei eine grobe Einteilung in zwei Gefährlichkeits- oder Risikostufen möglich. Dies seien zum einen die weniger gefährlichen, eher lästigen, aber dafür sehr sichtbaren Angreifer. Beispielsweise seien hier Kleinkriminelle, die Kreditkartenbetrügereien versuchten und Massen von Viren produzierten, aber auch Aktivisten und Hacktivisten zu nennen. Cyberterroristen könne man eventuell im Sinne eines Gespenstes als sichtbares, aber weniger gefährliches Phänomen beurteilen. Obwohl sie nicht wirklich existierten, geisterten sie sehr dominant durch die Medien. Diese drei Varianten von Angreifern stufe er als nur sehr mäßig gefährlich ein, weil sie in sehr kleinen Gruppen mit wenig Know-How arbeiteten. Ressourcen seien für sie nur schwer aufzubringen; Angriffsvektoren seien be-

grenzt. Folge seien vor allem DoS-Angriffe oder massenhaft Spam. Dies könne natürlich im Einzelfall gefährlich sein, wenn man auf ganz gravierende Sicherheitsmängel treffe. Sofern zum Beispiel die Steuerungsbereiche eines Kraftwerkes noch ordinär über das Internet erreichbar und nicht gut geschützt seien, könne dies Probleme verursachen. In der Regel gehe von den Akteuren aber keine große Gefahr aus. Sie seien lästig, aber nicht gefährlich.

Anders sehe es bei den drei oberen Gefährdungsstufen aus. Dies seien vor allem organisierte Kriminalität, staatliche Angreifer, Nachrichtendienste, Militärs und Söldner als eine noch kleinere Gruppe. Bei diesen gelte, dass sie generell sehr viel mehr Geld in die Hand nehmen und auf sehr gutes Know-How, auch auf wissenschaftliche Unterstützung, zurückgreifen könnten. Sie seien in der Lage Laboratorien aufzubauen, sehr gute Teams zusammenzustellen und hätten Nachrichtendienste zu ihrer Verfügung, die die Angriffe auch vorbereiten und transportieren könnten. Zudem stellten sie mehr Geld zu Verfügung, sodass pro Angriff ein Millionenbetrag ausgeben werden könne. Dies sei eine Größenordnung, die relativ neu sei.
Dr. Sandro Gaycken betont, dass dies aus seiner Sicht der bedeutendste Wandel sei, der sich in den letzten zwei bis drei Jahren in der IT-Sicherheitslandschaft vollzogen habe.

Die Angreifer der drei oberen Gefährdungsstufen hätten gemerkt, dass sie mit einer guten Truppe von Hackern zahlreiche Ziele – wirtschaftliche, machtpolitische – verfolgen könnten. Sie hätten sich umfangreich eingerichtet bzw. täten dies zur Zeit. Da diese Angreifer in alle System reinkämen, seien sie als sehr gefährlich einzustufen. Dazu müssten die Systemen noch nicht einmal im Internet sein, sodass es sich nicht um eine originäre Internetproblematik handle. Bei dem gegenwärtigen Stand der Technik sei es absolut unmöglich diese Angriffe abzuwehren. Darüber hinaus könne man in den meisten Fällen mit Strafverfolgung nichts ausrichten, da die Attribution sehr schwierig sei. Dies sei bereits bei den Kreditkartendieben nahezu unmöglich. Man habe es also mit einer Variante von Angreifern zu tun, die im Wachstum begriffen sei. Auf diese müsse sich die Gesellschaft schwerpunktmäßig einrichten.

Zu der zweiten Frage hinsichtlich der Angriffsszenarien äußert **Dr. Sandro Gaycken**, dass sich diese sehr starken Angreifern auf Hochsicherheitsbereiche konzentrierten. Angreifer in dieser Qualität hätten kein Interesse an einfachen Kreditkartenbetrügereien. Daher wollten sie einen Zugriff auf Rüstungsprojekte, große Ölfirmen, Finanzmärkten oder Banken erhalten. In den meisten Fällen sei das Internet dafür nicht entscheidend, viel häufiger werde mit Innentätern vorgegangen. Dies täten die Angreifer entweder aus Bequemlichkeit, weil der Zugriff auf Innentäter sowieso bestehe oder weil die anzugreifenden Strukturen aus Sicherheitsgründen nicht mit dem Internet verbunden seien. Allerdings passiere es auch immer wieder, dass Sicherheitsstrukturen oder Ziele noch immer aus Convenience-Gründen mit dem Internet verbunden seien. Ein Schutz vor Angriffen sei dadurch schwierig. Solche Systeme müssten entsprechend vom Internet entkoppelt werden. In derartigen Fällen sei für die Angreifer ein Zugriff auf Grund der niedrigeren Risiken und Kosten attraktiver. Ein besonderes Problem bestehe für die Wirtschaft und die Finanzmärkte. Diese seien inzwischen sehr intensiv vernetzt. Zudem hätten sie einen starken Bedarf an Datendurchfluss sowie sehr komplexe IT-Landschaften. Folglich sei es sehr schwierig Sicherheitsstrukturen zu etablieren, die gegen diese sehr starken Angreifer verlässlich funktionierten. Dies sei auch den starken Angreifer bekannt. Für Staaten als auch für organisierte Kriminelle sei es sehr interessant in der Wirtschaft zu spionieren und zu sabotieren. Dies treffe insbesondere auch auf die Finanzmärkte, Banken und Börsen zu.

Im Hochsicherheitsbereich müssten die Zügel ganz massiv angezogen und ein Schutz implementiert werden, der aktuell noch nicht entwickelt sei. Einen solchen gebe es in der theoretischen Forschung zwar schon seit den 60er-Jahren. Da jedoch immer billige und schnelle IT nachgefragt worden sei und keine sichere, habe in der Anwendungsebene keine Entwicklung stattgefunden.

Es gebe aber neue Ansätze zu hochsicheren Architekturen, die komplexe IT-Landschaften entsprechend vereinfachten und transparenter machten. Er denke hier an Mikrokernels und entsprechende Kontrollmechanismen. Es handle sich aber gewissermaßen um neue Konzepte für Hardware und Software. Demzufolge müsse die

vorhandene IT in diesen Hochsicherheitsbereichen entfernt und durch die hochsichere ersetzt werden. Im normalen Sicherheitsbereich müsse der Schutzbedarf sehr individuell ermittelt werden. Die Wirtschaft gehöre im Grunde zum normalen Sicherheitsbereich, könne jedoch auch von organisierten Kriminellen oder Nachrichtendiensten infiltriert werden. Dann sei auch dort ein Hochsicherheitsschutz erforderlich. Außerdem sei bei vielen kritischen Infrastrukturen nicht bekannt, welche Systeme dort mit dem Internet verbunden seien. Dies sei aktuell einer der schwierigste Punkte, bei den im Moment ein großer Wissensbedarf bestehe. Niemand wisse, was in welcher Art und Weise zu schützen sei. Bei privaten Anwendern sieht **Dr. Sandro Gaycken** den Schutz vor allem im Bereich der Sensibilisierung. Er sei skeptisch, ob man mit Mitteln wie Strafverfolgung viel erreichen könne. Diese Mittel hätten sehr schlechte Effizienzkriterien. Gerade bei der Vorratsdatenspeicherung oder ähnlichem, müsse man eventuell andere kriminalistische Techniken und vielleicht auch mehr Personal einsetzen. Seiner Kenntnis nach seien die Personalstände in den Kriminalämtern sehr schlecht.

Der **Vorsitzende** dankt **Dr. Sandro Gaycken** für das Statement und übergibt das Wort an **Thorsten Schröder.**

Thorsten Schröder teilt mit, er könne in erster Linie aus der Praxis berichten. Er arbeite seit etwa einem Jahrzehnt in der IT-Security Branche und wisse, was in Unternehmen unterschiedlicher Größe hinsichtlich IT-Sicherheit unternommen werde. Er vergleiche den Sollzustand, basierend auf Richtlinien, die für den Betrieb von kritischen Infrastrukturen vorgeschrieben seien, mit dem Istzustand. Er sei lange Zeit auch beim TÜV Rheinland in der Secure IT tätig gewesen und habe dort Sicherheitsüberprüfungen bei Firmen, beispielsweise Banken, durchgeführt. Diese Firmen seien zu solchen Überprüfungen verpflichtet. Er habe aber auch viele Sicherheitsüberprüfungen bei Firmen durchgeführt, die ein Zertifikat erlangen wollten, um damit werben zu können.

Dieses Prüfsiegel solle und könne den jeweiligen Unternehmen neue Märkte eröffnen. Was jedoch viele der Firmen oftmals nicht erwarteten, sei, dass die Untersu-

chung gründlich durchgeführt werde. Als Prüfer müsse er seine Prüfergebnisse letztlich gegenüber den Verantwortlichen rechtfertigen und verteidigen. Dies sei eigentlich der Normalzustand, da viele dieser Firmen oftmals nicht in der Lage seien, Fehler einzugestehen. Sie befürchteten einen Gesichtsverlust und ignorierten letztlich viele Sicherheitshinweise. Dies führe dazu, dass viel Energie für die Vertuschung von Fehlern aufgewandt werde, anstatt die Probleme zu verinnerlichen. Jenes Verhalten erlebe er nicht immer, aber oft in der Praxis.

Thorsten Schröder erklärt zum Thema Zertifizierung und Compliance, dass er nicht grundsätzlich gegen solche Zertifizierungen und Richtlinien sei. Er halte solche Regeln, wie sie vom BSI vorgegeben würden für durchaus sinnvoll. Diese böten einen Grundschutz. Es gebe aber keinen branchenübergreifenden Grundschutz, da dieser immer sehr individuell ausgearbeitet werden müsse. Er habe Einblick in viele Branchen erhalten und vor allem gelernt, dass man sich in jeder Branche auf ganz andere Bedrohungsszenarien einlassen müsse. Zertifikate und Compliance Checks seien auch ein Druckmittel. Es gebe zum Beispiel die PCI-Regulatorien [Payment Card Industry Data Security Standard, PCI DSS, Anm. d. Sek.], die von einem Konsortium verabschiedet würden. Firmen, die etwa Kreditkartendaten verarbeiteten, müssten also mit bestimmten Voraussetzungen konform gehen. Im Endeffekt sei PCI das so genannte Druckmittel, um den Firmen die Möglichkeit der Verarbeitung von Kreditkartendaten zu entziehen, falls sie sich nicht an die Regeln hielten. Im Fall von Sony sei offensichtlich massiv gegen diese Richtlinie verstoßen worden. Er frage sich, warum dieses Druckmittel dort nicht in der Form eingesetzt werde, wie es gegen einen kleinen Online-Handel erfolge. Im Endeffekt sei Sony ein Beispiel dafür, dass dieses Verhalten seit langer Zeit eine tickende Zeitbombe gewesen sei. Am Ende sei diese explodiert, aber richtige Konsequenzen habe offenbar niemand ziehen müssen. In einem solchen Fall sei zumindest zu prüfen, ob eine stärkere Sanktionierung notwendig sei. Natürlich müsse dabei immer abgewogen werden. Er habe auch keine Patentlösung für die Probleme, mit denen man dort zu kämpfen habe. Jedoch sei es bei Fahrstühlen und Rolltreppen auch selbstverständlich, dass der TÜV diese stilllege, sofern nicht die Mindestanforderungen erfüllt seien. Gleiches müsse auch für den Betrieb von Rechneranlagen gelten, die private oder sensible

Daten verarbeiteten. Dies sei das Druckmittel und die Motivation, die in Unternehmen und Konzernen geschaffen werden müsse, um in diesen Bereich zu investieren.

Weiter führt **Thorsten Schröder** aus, dass es sich bei der ziemlich kaputten PKI (Public Key Infrastructure)-Infrastruktur ähnlich verhalte. Der Einbruch in die CA (Certificate Authority, dt.: Zertifizierungsstelle) DigiNotar, sei weltweit bekannt geworden. Obwohl mittlerweile jeder wisse, dass es sich um ein sehr kaputtes Modell handle, setzten immer mehr Institutionen, auch die Bundesregierung, verstärkt auf die PKI. Dies sei ein Vertrauensmodell, welches aus seiner Sicht alles andere als zeitgemäß sei. Es gebe CAs, die in der freien Wirtschaft angesiedelt seien und sehr intransparent agierten. Passierten dort Fehler, seien diese nicht transparent und könnten kaum korrigiert werden. Dies fange bei der Implementierung einer CA an, unabhängig davon, ob es eine interne oder eine von der Bundesregierung betriebene sei. Wenn es schon bei der Erstellung der Root-Zertifikate zu Fehlern in den Krypto-Algorithmen komme oder einfach nur die falschen Parameter verwendet würden, könne es durchaus sein, dass alles auf dem Zertifikatsbaum aufbauende ungültig sei. Eventuell könne später ein Root-Zertifikat neu berechnet und könnten digitale Identitäten gefälscht werden.

Es gebe, so merkt er an, überhaupt keine Überlegungen, wie man damit umgehe, sollten die Zertifikate der digitalen Identität des Personalausweises gefälscht sein. Er frage sich, wie mit – auch rückwirkend – rechtskräftigen digitalen Unterschriften, umgegangen werde, sollte nachgewiesen werden, dass die Basis dieses Modells defekt sei. Hier könnten sehr viele Fehler gemacht werden. Es sei beispielsweise nicht sicherzustellen, ob der Zufallszahlengenerator einer kryptologischen Implementierung einwandfrei sei oder ob nicht eventuell für die Erstellung kryptografischer Keys ungeeignete Zufallsdaten genutzt würden. Der Einbruch bei DigiNotar habe auch gezeigt, wie wenig Firmen und auch Staaten vorbereitet seien.

Der Einbruch in einer CA sei gleichzusetzen mit einem Einbruch in einer Fertigungsstelle für Personalausweise und Reisepässe. In dem Moment, in dem jemand

Zutritt zu diesen Anlagen oder Techniken habe, könne er Identitäten erstellen oder sich aneignen. Dieses stelle auf dem elektronischen Weg ein weit größeres Schadenspotenzial dar.

Wirtschaftsunternehmen, die eine CA betrieben und an einer Ausschreibung teilnähmen, erhielten in Bezug auf die Wirtschaftlichkeit viel zu viele Zugeständnisse. Aber genau dies führe zur Vernachlässigung der Sicherheit. Sicherheit sei immer auch mit Mehraufwand oder mehr Kosten verbunden. Im diesen Bereich könne man es sich nicht erlauben, auf Wirtschaftlichkeit zu achten.

Das gesamte Vertrauensmodell einer CA, wie man es heute kenne, sei nicht zeitgemäß. Dort werde Vertrauen vererbt, was für Benutzer jedoch völlig intransparent sei. CAs könnten unterwandert werden oder in staatlicher Hand seien. Auch das wirtschaftliches Interesse einer CA, in einen Trusted CA-Store eines Webbrowser zu gelangen, sei zu beachten. Dies habe mit Sicherheit nicht viel zu tun.

Thorsten Schröder bezieht sich auf die Aussagen von **Prof. Dr. Jochen H. Schiller**, der die Frage in den Raum gestellt habe, wie die Migration oder Integration der vorhandenen, ziemlich alten und kaputten Infrastruktur in eine neuere, moderne vollzogen werden könne. Er finde die Idee, die dieser Frage zugrunde liege, grundsätzlich gut und bezeichne es als den Sollzustand. Er habe aber in der Praxis diesbezüglich schlechte Erfahrungen machen müssen. Einmal habe er bei einem Energieversorger ein einen Windows-Server, der nicht gepatched worden sei, vorgefunden. Dies sei katastrophal gewesen, aber den verantwortlichen Mitarbeitern seien die Hände gebunden. Die Software- und Steuerungsgerätehersteller drohten mit dem Verlust der Garantie, sofern ein Patch installiert werde. Dabei sei bekannt, wie wichtig es sei Systeme mit getesteten Patches zu betreiben, um gegen die grundsätzlichen Gefahren, das Grundrauschen der Angriffe, geschützt zu sein. Firmen, die Software herstellten, müssten in die Haftungspflicht genommen werden. Sie müssten von Anfang an klar vorlegen können, wie sie auf Sicherheitslücken reagieren wollten. Es könne nicht sein, dass bei kritischen Infrastrukturen, wie einem Energieversorger, Ausnahmen gemacht würden.

Er geht über zum Thema Cyber Incident Disclosure und merkt an, dass er dafür einen anderen Begriff wählen würde. Cyber Incident Disclosure gebe es tatsächlich und werde auch geleakt. Im Bankenumfeld in der Schweiz habe er dies selbst kennengelernt. Dort setzten sich Verantwortliche unter Ausschluss der Öffentlichkeit an einen Tisch und berichteten sich gegenseitig über Verfahren, mit den sie gehackt worden seien. Eine derartige Offenlegung gegenüber der Konkurrenz halte er für sehr mutig.

Der **Vorsitzende** dankt **Thorsten Schröder** für das Statement und übergibt das Wort an **Mirko Manske.**

Mirko Manske bemerkt eingehend, dass er in Bezug auf das Internet und die neuen Kommunikationswege zunächst sehr viel Düsteres sehe. Schließlich komme die Polizei immer dann, wenn etwas nicht funktioniere.

Seit 2005 beobachte das BKA stetig steigende Fall- und Opferzahlen. Es gebe deutlich komplexer und immer technisch werdende Ermittlungen, bei denen das notwendige Personal nicht immer in ausreichendem Maße zur Verfügung stehe . Es werde festgestellt, dass die Angreifer zügig auf dem Weg in die Dienstleistungsgesellschaft seien. Was vor vier bis fünf Jahren von einer festgegründeten Tätergruppe von Anfang bis Ende abgewickelt worden sei, zerfasere sich heute in viele kleine Dienstleister, die sich um das Rekrutieren von wahren Agenten, von Human Proxies, von Geldwäschern, kümmerten. Diese begingen allerdings gleichzeitig andere Teiltaten völlig autark, wie beispielsweise das Bereitstellen anonymer Kommunikationsinfrastrukturen.

Ferner sehe man immer mächtiger werdende Trojaner, die heute im Umlauf seien. **Dr. Sandro Gaycken** habe zuvor von den Kleinkriminellen gesprochen. Schätzungen des BKA zufolge seien im letzten Jahr im Online-Banking-Bereich in der Bundesrepublik Deutschland ca. 60 Millionen Euro an trojanerbasierten Schäden entstanden. Er gehe davon aus, dass die Finanzindustrie dies mit einem gewissen Schmerz gesehen habe.

Außerdem, so fährt **Mirko Manske** fort, gebe es Adaptionen altbekannter Geschäftsmodelle an die neue digitale Welt. Früher seien Pizzerien um Schutzgeld erpresst worden. Heute seien große Unternehmen, die auf die Hochverfügbarkeit im Netz angewiesen seien, DDoS (Distributed-Denial-of Service)-Angriffen ausgesetzt, bis sie letztendlich im Netz nicht mehr erreichbar seien. Wenige Tage später konfrontierten die Angreifer sie mit entsprechenden Geldforderungen. Erfüllten sie diese nicht, gingen die Angriffe weiter. Für einen E-Commerce Anbieter sei es sicherlich problematisch aus diesem Grund seinen einzigen Vertriebsweg zum Kunden zu verlieren.

Cybercrime wirke sich aber auch auf Prozesse in der realen Welt aus. Das Modell der DDoS-Angriffe könne auch dort angeführt werden. Ein weiteres Beispiel seien massive Manipulationen von Wertpapierkursen mittels übernommener Depots, die letztendlich konkrete Auswirkungen auf Unternehmenswerte hätten. Beispielsweise durch das Handeln von Penny Stocks oder das Abstoßen von Werten bestimmter Institutionen in großem Maße. Zudem gebe es, zum Beispiel im Speditionsgewerbe, Angriffe auf konkurrierende Unternehmen. Dort brächten die Angreifer gezielt Schadsoftware auf Servern von Unternehmen ein, um an Informationen zu Kunden, internen Preismodellen oder Preiskalkulationen zu gelangen.

Strafverfolgungsbehörden stünden vor allem einer Vielzahl von rechtlichen Schwierigkeiten gegenüber. Diese seien aus Sicht des BKA knapp mit einem nicht mehr zeitgemäßen Katalog des §100a StPO – vor allem im Bereich der Datendelikte – zu umreißen. Es fehle die Umsetzung des Artikels 16 der Cybercrime Convention. Das BKA habe keine Möglichkeit Data Preservations durchzuführen. Dies seien Vorabsicherungen von Daten im Vorgriff auf Rechtshilfemaßnahmen anderer Staaten in Deutschland. Zudem fehle eine gesetzlich verordnete 24/7-Erreichbarkeit der deutschen Provider, die diese freiwillig nicht bereitstellten. Außerdem existiere die Problematik des §14 BKAG (Bundeskriminalamtsgesetz), welche es der deutschen Polizei schlichtweg unmöglich mache, Informationen mit privaten Stellen im Ausland auszutauschen. Dies sei aus Sicht des BKA in Zeiten, in denen das Internet gänzlich global sei und die Daten der deutschen Gesellschaft wahrscheinlich weni-

ger in deutschen Rechenzentren als vielmehr in Palo Alto und Mountain View lägen, nicht mehr zeitgemäß.

Der **Vorsitzende** dankt **Mirko Manske** für das Statement und eröffnet die Fragerunde.

Abg. Thomas Jarzombek (CDU/CSU) stellt drei Fragen. Die erste Frage richtet er an **Thorsten Schröder** und **Andreas Könen**. Sein Eindruck aus der gelebten Praxis werde durch die Aussagen der Experten bestätigt. Es sei nicht nur eine Frage von komplexen Angriffen. Das zumindest die grundsätzlichen Gefahren nicht eliminiert würden, liege zuweilen auch daran, dass eine Reihe von Systemadministratoren recht nachlässig mit dem Thema Sicherheit umgingen. Dies sehe man auch im Deutschen Bundestag, wo teilweise erst nach einem dreiviertel bis einem Jahr Patches aufgespielt würden. Man brauche also nicht so weit schauen. Ein solches Verhalten liege nicht nur an der Motivation, sondern manchmal auch an fehlendem Wissen oder Bewusstsein. Im gesamten IT-Bereich gebe es in diesem Bereich kaum Qualifikationen.

Deshalb wolle er wissen, ob die beiden Experten das Angebot einer postgraduierten berufsbegleitenden Qualifikation oder Zertifizierung von Administratoren für sinnvoll hielten. Diese solle aber einigermaßen niedrig gehalten sein, sodass sich Administratoren berufsbegleitend in diesem mindestens erforderlichen Level qualifizieren könnten. Er denke an eine Marke, die in der Breite des Marktes nachgefragt und als Standard für Grundwissen und Problembewusstsein im Bereich Internetsicherheit angesehen werde. Er habe häufig erlebet, dass dies fehle.
Er wendet sich an **Mirko Manske**. Dieser habe verschiedene Paragraphen angesprochen. Die globale Cybercrime-Industrie betreffend, stelle er sich die Frage, ob diese über alle Standorte gleich verteilt sei oder ob es gewisse Präferenzen in Bezug auf das Vorhalten von Angriffsinfrastrukturen – beispielsweise auf Grund der Aufzeichnungsfristen – gebe. Ihn interessiere, welcher Eindruck aus Sicht des BKA hinsichtlich des Standorts Deutschland bestehe – ob dieser besonders gut, schlecht oder durchschnittlich sei. Er wundere sich, ob es eine Art Standortliste gebe, aus

der man herauslesen könne, wo sich die Kriminellen mit ihren Infrastrukturen niederließen.

Seine dritte Frage richtet er auch an **Andreas Könen.** Er führt aus, dass die von Google und Facebook gespeicherten personensensiblen Daten teilweise noch viel bedeutsamer seien , als die Daten, die der Staat speichere. Zudem sei es mit diesen Daten viel eher möglich, einzelne Individuen zu kompromittieren. Er wolle wissen, wie **Andreas Könen** die Sicherheitsstandards, die bei diesen Unternehmen vorlägen, beurteile. Des Weiteren interessiere ihn, wie hoch er die Gefahr einschätze, dass Täter möglicherweise auch Personen des öffentlichen Lebens desavouierten und sich unberechtigten Zugang zu den internen Informationen bei Facebook oder Google verschafften, um damit Personen gezielt erpressen oder kompromittieren zu können.

SV Constanze Kurz fragt bei **Abg. Thomas Jarzombek (CDU/CSU)** nach, ob er sich die von ihm angesprochene Administratorenausbildung als Pflicht- oder Kann-Lösung vorstelle.

Abg. Thomas Jarzombek (CDU/CSU) wolle die Beurteilung, ob eine solche Ausbildung optional oder verpflichtend sein solle, den Experten überlassen. Möglicherweise seien auch Anreize zu setzen, die so deutlich ausfielen, dass dadurch aus dem „Kann“ quasi ein „Muss“ werde.

Thorsten Schröder antwortet, dass er die Frage zur Zertifizierung von Administratoren oder von Personal, welches für IT-Sicherheit verantwortlich sei, für nicht grundsätzlich zu beantworten halte – insbesondere, falls eine Prüfung abgelegt werden solle. Es gebe Zertifikate, die Systemadministratoren auch in Bezug auf IT-Sicherheit erwerben könnten. Auch wenn er sich kritisch gegenüber einer Zertifizierung äußere, sage diese aus seiner Sicht nicht besonders viel über die Qualität der Arbeit seines Inhabers aus. Es könne durchaus sein, dass er sich diese Themen angeeignet habe und sein Wissen im Endeffekt wiedergebe, aber letztlich die erarbeiteten Punkte nicht lebe. Dies könne daran liegen, dass er von seinen Vorgesetz-

ten gebremst werde oder durch das Budget, für welches er sich möglicherweise auch noch rechtfertigen müsse.

Verantwortliche für IT-Sicherheit hätten in einem Unternehmen immer die schlechtesten Karten, da sie eigentlich nur Kosten verursachten und nicht für den wirklichen Umsatz sorgten. Zudem müsse eine Zertifizierung regelmäßig wiederholt werden. Es müsse wiederum einen sehr branchenspezifischen Lehrgang geben. Da fingen die Probleme an, weil es keine Anhaltspunkte gebe, woran man die Lehrgangsinhalte fest machen könne – für die eine Firma könnten andere Punkte wichtig sein, als für eine andere.

Thorsten Schröder merkt an, dass in der Realität der Datenschutz in Unternehmen, der durchaus positiv sei, der IT-Sicherheit entgegenstehe. Ein Administrator könne und dürfe beispielsweise sein eigenes Netzwerk gar nicht testen, da es dabei möglicherweise zum Zugriff auf Datensätze von Mitarbeitern kommen könnte. Hier schreite der Datenschutzbeauftragten eines Unternehmen ein und dies sogar zu Recht. Daher ziehe man externe Dienstleister hinzu, die regelmäßig ein Monitoring vornähmen. Dies sei zum Beispiel bei Banken der Fall. Hinzu komme, dass ein Administrator, der sich unternehmensintern mit der Thematik auseinandersetze, auch die entsprechenden Werkzeuge beschaffen müsse. Hier sei der Hackertoolparagraph erwähnt. Er kenne zwar bisher keinen Fall, aber grundsätzlich bewege man sich hier – möglicherweise – in einer rechtlichen Grauzone. Ein Administrator müsse sich die so genannten Hackerwerkzeuge beschaffen oder diese eigenständig entwickeln, um die unternehmensinterne Infrastruktur damit penetrieren zu können.

Der entscheidende Punkt sie jedoch die Motivation. Diese spiele eine sehr große Rolle in diesem Bereich. Der Beruf des Hackers oder Sicherheitsspezialisten könne nicht einfach erlernt werden, weil dies gerade notwendig sei. Es gebe keinen Lehrgang, keine Ausbildung oder dedizierten Studiengang, sondern erfordere in erster Linie eigene Motivation. Daher halte er eine Zertifizierung für grundsätzlich schwierig. Trotz alledem sei es definitiv ratsam, dass es in einer Systemadministration dedizierte Ansprechpartner für Bereiche wie IT-Sicherheit gebe, denen auch

entsprechende Budgets eingeräumt würden, um sich weiterzubilden und andere Mitarbeiter zu sensibilisieren. Er denke jedoch, dass damit nicht alle Probleme zu lösen seien.

Andreas Könen betont, er könne **Thorsten Schröder** nicht zustimmen. Nur weil das Problem so komplex sei, hielte er für vollkommen falsch, es nicht anzugehen. Tatsache sei, dass es solche Zertifizierungen gebe. Es gebe bereits für den Bereich des Bundes die Zertifizierung von IT-Sicherheitsbeauftragten. Es würden auch eine Vielzahl von Ausbildungsserien für Systemadministratoren im Sicherheitsbereich des Bundes angeboten. Für IT-Sicherheitsbeauftragte seien diese Ausbildungen verpflichtend. Sie fänden bei der Bundesakademie für öffentliche Verwaltung in Brühl statt und seien als gestaffeltes Modell aufgebaut. Es entspreche einer klassischen Fachhochschulausbildung in drei Stufen. Im Grunde enthielte diese die Punkte, die **Thorsten Schröder** angemahnt habe. In gewissen Zeitabständen müsse sie erneuert werde. Die Ausbildung, welche am Ende mit einer Prüfung und einer Arbeit beendet werde, schließe mit einem dem Grad ab, der dem Bachelor ähnlich sei. Zutreffend sei, dass diese Tätigkeit in den Behörden mit einem Budget und der Möglichkeit diese in Fragen der Informationssicherheit auszuüben, untermauert werden müsse.

Im UP Bund sei dies entsprechend implementiert worden. Die IT-Sicherheitsbeauftragten verankerte man bei der Hausleitung und gewährte ihnen auch ein direktes Vorspracherecht. Im Moment versuche das BSI, diese Art von Zertifizierung von IT-Sicherheitsbeauftragten als Modell in die verschiedenen Hochschulen des Landes zu tragen. Man führe mit Hochschulen Gespräche, die in den Ausbildungen der BAköV schon präsent seien und habe dort das Ansinnen geäußert, genau solche Personenzertifizierungen in größerem Maße in die Wirtschaft zu transportieren. Es gebe in diesem Bereich tatsächlich eine ganze Reihe von Ausbildungsgängen an Universitäten und in der Wirtschaft. Natürlich sei dies nicht so strukturiert und standardisiert, wie sich dies das BSI vorstelle. Auf der Basis von Grundschutz in den Zertifizierungen, die nach § 9 BSI-Gesetz (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) möglich seien, könne man sich dieses Modell –

auch für die Wirtschaft – zum Vorbild nehmen. Zum Thema Systemadministrator fügt er hinzu, dass es eine ganze Reihe von Universitäten, etwa die Ruhr-Universität Bochum, gebe, die gerade im Informationssicherheitsbereich entsprechende Ausbildungsgänge anböten. Er halte die Verknüpfung von Sensibilisierung und Ausbildung für den geeigneten Weg, um in diesem Bereich wirklich weiterzukommen.

Andreas Könen sagt, dass man in Bezug auf den Standort von kriminellen Infrastrukturen hinsichtlich des betrachteten Teils der Infrastruktur differenzieren müsse. Bei Malware sei eine starke Häufung in Osteuropa – der russischen Föderation, der Ukraine, Weißrussland und teilweise auch den östlichen Ausläufern des Baltikums– zu beobachten. Aus Sicht des BSI sei dies darauf zurückzuführen, dass diese Länder auf Grund ihrer gesellschaftlichen Historie immer stark im naturwissenschaftlichen Bereich gewesen seien. Sie verfügten über viele talentierte Programmierer , die als Freelancer in diesem Bereich weitaus mehr Geld verdienten, als mit einer regulären Tätigkeit. Als Freelancer schrieben sie nicht nur einfache Malware, sondern rollten teilweise komplette Franchise-Modelle aus. Die Trojanerfamilie Gozi beispielsweise werde inklusive der Finanzagenten und Bulletproof-Hosting geliefert.

In anderen Bereichen sehe das BSI zwar auch Südostasien mit einer gewissen Relevanz, es gebe aber kulturelle Unterschiede zwischen Asien, dem europäischen und dem US-amerikanischen Markt. Viele der in Europa und den USA verbreiteten Geschäftsmodelle, wie zum Beispiel eBay, seien in Thailand und Südkorea nicht bekannt. Die Gesellschaft funktioniere dort anders, weshalb auch die Malware anders funktionieren müsse.

Zu den von **Abg. Thomas Jarzombek (CDU/CSU)** angespielten Speicherfristen, teilt **Andreas Könen** mit, dass nach seinem Kenntnisstand alle für die Bekämpfung von Cybercrime relevanten internationalen Partner in der Lage seien IP-Adresseninhaber zu identifizieren. Sie machten dies auf unterschiedliche Weise. Teilweise gebe es so genannte Mindestspeicherfristen. Teilweise speicherten die Unternehmen diese Informationen erlaubterweise freiwillig , wie in den USA. Die Strafverfolgungsbehör-

den könnten dann im Moment des Informationsbedarfes – im Rahmen der gesetzlichen Möglichkeiten – auf diese Bestände zugreifen. In der Front der Aktivposten der Cybercrime-Bekämpfung, zu denen er die Bundesrepublik Deutschland definitiv zähle, liege Deutschland momentan relativ weit hinten. Dies liege auch daran, dass es bis auf wenige Provider nicht möglich sei, die Adressinhaber von dynamischen IP-Adressen zu identifizieren. Er weise nachdrücklich darauf hin, dass häufig nur die repressiven Maßnahmen in Betracht gezogen würden. Es gebe aber auch keine Möglichkeit Opfer zu identifizieren.

Als Beispiel führt **Andreas Könen** die Operation Ghostclick des FBI an, bei der aufgedeckt worden sei, dass hunderttausende Rechner in Deutschland mit einer Schadsoftware infiziert gewesen seien. Diese habe die DNS-Einstellungen auf den lokalen Geräten manipuliert und dadurch das Internet verfälscht dargestellt. Der Nutzer bekomme andere Suchergebnisse von Google sowie andere Werbeeinblendungen angezeigt. Alle 15 Minuten bekomme das BSI aus den USA eine Liste mit deutschen Opfer-IPs – allerdings mit einem Tag Versatz, weil die Behörden in den USA einen Tag bräuchten, um die Datenmengen aufzubereiten. Das BSI könne die Opfer jedoch nicht identifizieren und darauf aufmerksam machen, dass ihre Rechner infiziert seien.

Andreas Könen geht auf die Frage der Handhabung von Sicherheitsmaßnahmen von Providern sozialer Netze ein. Das BSI habe in diese Firmen und deren Sicherheitsgebaren keinen Einblick. Sicherlich gebe es Fälle, in denen man Einzelinformationen bekomme, insbesondere, wenn das BSI in der Lage sei Warnungen zu Sicherheitsgefährdungen auszusprechen. Grundsätzlich bekomme man aber keine Informationen über die von den Firmen ergriffenen Sicherheitsmaßnahmen. Dies treffe auch dann zu, wenn die Firmen auf deutschem Boden aktiv seien, wie dies bei Google und Facebook der Fall sei.

Der **Vorsitzende** dankt **Thorsten Schröder**, **Andreas Könen** und **Mirko Manske** für ihre Ausführungen und gibt das Wort an **SV Constanze Kurz**.

SV Constanze Kurz wendet sich an **Prof. Dr. Dirk Heckmann** und **Thorsten Schröder.** In mehreren Statements seien die Pflichten der Unternehmen, wie die Mitteilung von Sicherheitsvorfällen an Betroffene, angesprochen worden. Sie interessiere, wie Haftungsfragen in Zukunft so geregelt werden könnten, dass Unternehmen und Behörden einen Anreiz erhielten mehr in IT-Security zu investieren. Zudem wolle sie wissen, wie der Gesetzgeber im Umgang mit Software Liability sinnvoll agieren könne.

Abg. Dr. Reinhard Brandl (CDU/CSU) knüpft die Frage bezüglich eines IT-Sicherheits-TÜV an. Er bitte **Thorsten Schröder** zu erklären, wie er sich einen solchen vorstelle und ob dieser verpflichtend sein solle. Zudem wolle er wissen, welchen Anreiz Unternehmen zur Durchführung des TÜV erhalten könnten. Als Beispiele nenne er Haftungsveränderungen oder die Einführung eines Siegels. Des Weiteren bitte er **Prof. Dr. Dirk Heckmann** um eine Bewertung aus rechtlicher Sicht. Bezogen auf das von ihm vorgestellte Stufenmodell frage er sich, ob es sich um Maßnahmen im Rahmen der zweiten Stufe – der Gesetzgeber müsse Anreize zu IT-Sicherheit in eine wie auch immer geartete IT-Sicherheitsgesetzgebung einarbeiten – oder um Stufe drei – Hilfe zur Selbsthilfe – handle.

Prof. Dr. Dirk Heckmann fasst die Frage von **SV Constanze Kurz** zusammen. Er habe diese dahingehend verstanden, inwiefern bei IT-Sicherheitsvorfällen, bei denen beispielsweise personenbezogene Daten offengelegt worden seien, die für diese Daten Verantwortlichen die Betroffenen – entweder die Unternehmen, um deren Geschäftsgeheimnisse es gehe oder die Öffentlichkeit generell – zu informieren hätten. In § 42a BDSG (Bundesdatenschutzgesetz) sei zwar bereits eine Vorschrift zur Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten angelegt, diese werde aber kritisiert, weil dies als unvollständig angesehen werde. Sie stelle auf bestimmte Daten ab, die durch bestimmte Stellen, beispielsweise durch nichtöffentliche und wenige öffentliche Stellen, gehackt worden oder anderweitig betroffen seien. Die erste Kritik sei, dass es nicht generell eine Informationspflicht für sämtliche Behörden gebe. Diese müsse auf sämtliche Stellen ausgeweitet werden, da es für die Betroffenen nicht erheblich sei, wer die Daten verwalte und ein Datenleck

verursacht habe. Letztendlich wolle man schlichtweg informiert werden, wenn die eigenen Daten in den Umlauf geraten. Das hieße also für die rechtlichen Möglichkeiten §42a BDSG zu ergänzen oder den Anwendungsbereich zu erweitern. Dies sei ein normativer Ansatz. Allerdings könne man auch über das von ihm bereits angesprochene IT-Sicherheitsgesetz nachdenken. Auch in der juristischen Literatur, beispielsweise durch Prof. Dr. Gerald Spindler, werde für ein solches IT-Sicherheitsgesetz plädiert. Es sei zu überlegen, nicht fernab des Bundesdatenschutzgesetztes sowie der Landesdatenschutzgesetze in einem vor die Klammer gezogene IT-Sicherheitsgesetz solche Grundsatzfragen zu beantworten und damit auch bestimmte Weichen zu stellen.

Prof. Dr. Dirk Heckmann erklärt, dass es eine Grundsatzfrage sei, ob ein Betroffener den Anspruch habe bei IT-Sicherheitsvorfällen informiert zu werden. Dies begrüße er grundsätzlich. Allerdings müsse aus seiner Sicht auch ein kleiner Ausnahmekatalog hinzugenommen werden, beispielsweise hinsichtlich des Zeitpunktes der Veröffentlichung. Es gebe Fälle, in denen zum Beispiel ein schwerwiegenden Angriff vorliege und die Sicherheitsbehörden in den Ermittlungen steckten. Eine Veröffentlichung dieses Umstandes könne auf die Ermittlungen erschwerend wirken. Hier sei ein Stillhalten angebracht, allerdings auch nur um die Täter zu ermitteln. Solche gewissen Ausnahmen dürften jedoch kein Freibrief für das Zurückhalten von Informationen sein.

Mit der Informationspflicht korrespondiere die Frage der Haftung. Diese spiele im IT-Sicherheitsrecht, für das es bisher nur wenige Konturen gebe, generell eine Rolle. Die Haftung könne jedoch nicht generalisierend angeführt werden, da die Haftungsgrundsätze je nach Vorfall unterschiedlich seien. Beispielsweise könne ein Verschulden eines Unternehmens oder einer Behörde vorliegen, die diese Daten sorgfältiger behandeln hätten müssen. Es gebe aber auch Angriffe, die unvermeidbar seien. Man könne dort allenfalls im Rahmen einer Gefährdungshaftung zu einer Haftung kommen, wenn man eine solche einführe wolle. Eine Unterscheidung zwischen verschuldensabhängig und -unabhängig sei deshalb erforderlich. Eine weitere Variante sei es, den Betroffenen nicht zu informieren. Man könne bei Haftungsfra-

gen keine pauschale Aussage treffen. Zu prüfen sei immer der Haftungsanlass und der Haftungsmaßstab. Allerdings könne man Informationspflichten auch dahingehend sanktionieren, indem man eine Haftungsnorm anschließe. Es könne festgelegt werden, dass man für die Schäden hafte, die dem Betroffenen daraus erwachsen seien, dass er keine eigenen Vorsorgemaßnahmen habe treffen können, weil man ihn nicht rechtzeitig über einen sicherheitskritischen Vorfall informiert habe. Dies sei nicht allzu schwierig, wenn diese Informationspflicht im Gesetz verankert sei und daran anknüpfte, dass solche IT-Sicherheitsvorfälle in zumutbarer Weise bekanntgegeben werden müssten. In diesem Fall sei die Haftungsfolge auch sehr plausibel.

Thorsten Schröder geht auf die Worte seines Vorredners bezüglich der sicherheitsrelevanten Vorfälle ein. Es sei die Rede von einem Freibrief gewesen, den die Unternehmen im Moment hätten – dieser heiße Allgemeine Geschäftsbedingungen. Durch speziellere Regelungen hinsichtlich der Pflichten bei IT-Sicherheitsvorfällen könnten die Autoren von AGBs eingeschränkt werden. Als Nutzer von Soft- und Hardware müsse man auch proaktiv vom Unternehmen über solche Vorfälle unterrichtet. Möglicherweise könne man als Maßstab an den Datensätzen festhalten, welche nach Bundesdatenschutzgesetz auf Auskunftssuchen ohnehin freigeben werden müssten. Möglicherweise könne im Rahmen des § 42 a BDSG der Freibrief für die Unternehmen beseitigt werden. Im Moment könnten sich die Unternehmen jedenfalls alles erlauben. Sollte es zu einem Vorfall kommen, Software beschädigt oder in ein Netzwerk eingebrochen werden, wiesen sie die Schuld von sich und sagten der Benutzer habe zugestimmt. Einzig der Reputationsverlust schade den Unternehmen. Es müsse eine Pflicht zur Rechtfertigung geben, aus welchen Gründen Daten abhanden gekommen seien.

Bezugnehmend auf die Frage des IT-Sicherheits-TÜV führt er aus, er sei nicht grundsätzlich ein Befürworter von Prüfsiegeln. Er finde es grundsätzlich gut, dass es die Richtlinien des IT-Grundschutzes des BSI gebe. Es existierten weitere speziellere Richtlinien, nach denen sich Unternehmen richten könnten, aber er wisse, dass Ist- und Sollzustand in der Praxis sehr weit auseinanderlägen. In vielen Fällen müs-

se man sich dafür rechtfertigen eine Sicherheitslücke gefunden zu haben, da man immer wieder mit Verantwortlichen konfrontiert sei, die die Schuld nicht auf sich nehmen wollten. Eine Rolle spielten dabei teilweise Ahnungslosigkeit und teilweise Ignoranz. Dies sei kein konkreter Vorwurf, aber er bezweifle, dass eine Art TÜV-Siegel für den Betrieb solcher Anlagen sinnvoll sei.

Dr. Sandro Gaycken knüpft an die Ausführungen zum IT-Sicherheits-TÜV an. Er wisse aus der Praxis, dass es häufig Probleme gebe die Spezifikationen gut genug zu fassen. Sehr oft würden diese reaktiv aufgefasst. Gegenmaßnahmen spezifiziere man anhand eines bereits aufgetretenen Vorfalls. Es dauere allerdings relativ lange, bis diese in eine rechtliche Form gefasst seien, anschließend in eine technische Spezifikation gegossen und produktisiert würden. Ein solches Problem habe beim IT-Projekt Herkules in der Bundeswehr existiert, da dort sehr lange Zeiträume zwischen Spezifikation und Akquise herrschten. Die aus rechtlicher Perspektive notwendigen sehr präzisen Spezifikationen seien jedoch veraltete, wenn sie auf den Markt kämen und umgesetzt würden. Deshalb sei zu überlegen, für eine Sicherheitsgesetzgebung oder einen Sicherheits-TÜV, dynamische oder offene Sicherheitsstandards zu formulieren. Die Unternehmen seien folglich verpflichtet, die bei in Kraft treten des Gesetzes aktuellen Sicherheitsmaßnahmen zu ergreifen. Dies sei sinnvoll, aber aus juristischer und vertraglicher Perspektive mit den IT-Sicherheitsfirmen auch sehr kompliziert. Unternehmen setzten bei Änderung der Spezifikationen oftmals neue Verträge auf, was dann mehrere Millionen koste.

Ein weiteres Problem sei die Incentivierung. Haftung sei begrenzt tragfähig. Er wisse aus dem Bereich kritischer Infrastrukturen aus einigen IT-Sicherheitsabteilungen, dass es dort Abwägungen zwischen den Kosten eines mehrtägigen Stromausfalles und der Haftungsgrenze gebe. Eine wirklich solide IT-Sicherheit sei sehr viel teurer als die bestehende Haftungsgrenze. Aus ökonomischer Perspektive sei klar, was entschieden werde.

Auch die von **SV Constanze Kurz** angesprochene Software Liability sei mit Probleme verbunden. Auch dies sei ein schwieriges Thema, erklärt **Dr. Sandro Gaycken**,

da sich die Softwarehersteller diesbezüglich sehr sträubten. In konventionellen kommerziellen Produkten gebe es immer viele kritische Sicherheitslücken. Eine weitgehende Haftung triebe diese Hersteller schnell in den Ruin. Daher sei der Einwand berechtigt, solle aber die Entwickler nicht davon abhalten sauberer zu programmieren. Eventuell könne man hinsichtlich der Haftung bei Entwicklungsstandards ansetzen.

Insgesamt empfehle er die Veröffentlichung von Datenlecks als wirksamste und effiziente Maßnahme. Schließlich werde es von vielen Firmen und Behörden nicht gerne gesehen, in der Öffentlichkeit als jemand wahrgenommen zu werden, der mit seiner IT-Sicherheit zu lasch umgegangen sei. Dies sei das Einzige, wovor die Unternehmen Sorge hätten. In den USA habe Senator Rockefeller vor wenigen Wochen einen Disclosure Act durchgebracht, von dem sich der Senat viel verspreche. Nun seien Behörden und Unternehmen dazu verpflichtet alle Sicherheitspannen zu veröffentlichen.

Prof. Dr. Dirk Heckmann knüpft an die Ausführungen zur Softwarehaftung von **Dr. Sandro Gaycken** an. Diese Thema werde auch bei den Zivilrechtlern sehr stark diskutiert. Es sei nicht ausgeschlossen, dies zu konstruieren. Es werde auch im Rahmen der Produkthaftung überlegt, inwiefern dies auf Softwareprodukte Anwendung finden solle. Aber selbst wenn dies getan werde, sei das eigentliche Problem noch nicht gelöst. Viele Schadensfälle entstünden aus dem Zusammenwirken verschiedener Softwareprodukte. Daher stelle sich dann die Kausalitätsfrage, ob ein bestimmter Schaden auf ein bestimmtes Produkt zurückzuführen sei. Jeder versuche es auf den anderen Hersteller schieben.

Ein weiteres Problem sei die Frage des Nachweises. Wer habe die Beweislast? Wie könne dies überhaupt bewiesen werden? Der Betroffene werde im Zweifelsfall die Zusammenhänge gar nicht richtig darlegen können, weshalb man theoretisch eine Beweislastumkehr benötige. Ob man so weit gehen wolle, sei die Frage. Ferner gibt er zu Bedenken, dass die Hersteller dies dann auch in ihre Kalkulationen einbezögen und Software mit anderen Garantien auslieferten. Sie könnten vorab Warnun-

gen für bestimmte Funktionen und Einsatzfelder herausgeben, um sich so abzusichern. Wie man die Haftung regele, falls die Handhabung bestimmter Software-Funktionen auf eigenes Risiko geschehe, sei fraglich. Er wolle als Hersteller auch keinen Freibrief für hundertprozentige Funktionsfähigkeit geben, da es sich um sehr komplexe Vorgänge handele und Kausalzusammenhänge auslösen könnte.
Prof. Dr. Dirk Heckmann stellt fest, dass die Softwarehaftung zwar umsetzbar, aber sehr problembehaftet sei.

Er greift die von **Thorsten Schröder** angesprochene Frage zu § 42 a BDSG auf. In der Tat sei die Informationspflicht bei IT-Sicherheitsvorfällen sehr begrenzt. Diese beziehe sich nur auf vier Ziffern: besonders sensible Daten – dies sei in § 3 Abs. 9 BDSG konkretisiert –, Daten die einem Berufsgeheimnis unterlägen, Daten die sich auf strafbare Handlung bezögen und Daten in Bezug auf Bank und Kreditkartenkonten. Es gebe also Branchen, die davon nicht betroffen seien. Es handle sich um einen sehr begrenzten Anwendungsbereich – sowohl hinsichtlich derer die zur Auskunft verpflichtet seien, als auch der davon betroffenen Fälle. Die Frage von **SV Constanze Kurz**, inwiefern eine stärkere Informationspflicht mit dem Interesse der Betroffenen auf der einen und als Druckmittel gegen die Hersteller auf der anderen Seite zu begründen sei, sei sehr berechtigt. Es stelle einen ökonomischen Anreiz dar, die Systeme sauber zu halten. Er weist darauf hin, dass er normalerweise nicht für alles eine Regulierung fordere.

Bei dem von **Abg. Dr. Reinhard Brandl (CDU/CSU)** angesprochenen IT-Sicherheits-TÜV müsse man differenzieren, auf wen sich dieser beziehe – auf private Rechner, Unternehmens- oder Behördenrechner. Dies seien unterschiedliche Fallgestaltungen. In der Bundesverwaltung etwa gebe es schon Standards, die das BSI wohl mitgestalte. Bei Unternehmen existierten indirekte Pflichten, weil Haftungsfälle vorkommen könnten. Es gebe generell die IT-Sicherheitsgewährleistung, über die der Vorstand – etwa einer AG oder GmbH – im Rahmen seiner Pflicht zur Frühwarnung wachen müsse. Bei Privaten sei es anders und gehe mit der Frage einher, wie man dies umsetzen wolle. Es sei zu überlegen, ob dies objekt- oder personenbezogen erfolgen solle, schließlich könne man Rechner auch kurzfristig und wiederholt aus-

tauschen. Die Frage sei, ob man also einen IT-Sicherheits-TÜV oder einen IT-Sicherheitsführerschein benötige. Auch die Frage, inwiefern der Einzelne in die Pflicht genommen werden solle, für die Sicherheit seiner eigenen Umgebung zu sorgen, stehe im Raum. Damit schlage man eine Brücke zur Medienkompetenz. Dies habe er auch im Gutachten in These 13 ausführlicher dargestellt.

Er plädiere stark dafür, die Arbeitsergebnisse der Projektgruppe Zugang, Struktur und Sicherheit im Netz mit denen der Projektgruppe Medienkompetenz zu kombinieren. Diese zwei Dinge gehörten seines Erachtens zusammen, da langfristige Sicherheit nur dadurch hergestellt werden könne, dass die beteiligten Akteure überhaupt in der Lage seien ihren Beitrag zur Sicherheit zu leisten. Im Internet seien sehr viele Privatpersonen gefährdet, aber oftmals ginge von ihnen auch eine Gefahr aus. Daher seien sie auch in besonderer Weise zu befähigen, mit diesem Thema umzugehen. Dies müsse schon in den Schulen beginnen und sei auch sehr hoch anzusetzen, nicht nur als zweistündiges Fach. Das Thema müsse in den gesamten Schulalltag integriert werden. Wenn man in einer digitalen Gesellschaft lebe und Kinder später auch in komplexen IT-Strukturen – sei es im E-Government, im E-Commerce oder in anderen Kontexten – agieren sollten, sei es zwingend erforderlich, damit umgehen zu können. Im Moment scheine das Gegenteil der Fall zu sein, dies müsse sich grundsätzlich ändern.

Der **Vorsitzende** dankt **Prof. Dr. Dirk Heckmann**, **Thorsten Schröder** und **Dr. Sandro Gaycken** für ihre Ausführungen und übergibt das Wort an **Abg. Gerold Reichenbach (SPD)**.

Abg. Gerold Reichenbach (SPD) bittet **Prof. Dr. Dirk Heckmann** um Erläuterung seiner Ausführungen. Er erkundigt sich bei ihm, ob man Haftungsrechte abstufen könne. In vielen Bereichen sei die Technik vorhanden, aber es fehle an Sicherheitsbewusstsein. Im Automobilbereich traue sich auch niemand zu sagen, dass die Sicherheitstechnik vorhanden sei, es aber an Bewusstsein fehle. Als über Personenschutz im Fahrzeug – konkret Sicherheitsgurte – gesprochen worden sei, habe dies der Gesetzgeber geregelt. Er richtet die Frage, ob es in der IT-Sicherheit möglich sei

abzuschichten, auch an **Thorsten Schröder** und **Dr. Sandro Gaycken**. Als Vergleich zieht er den Begriff der Verkehrssicherheit heran, der im Gesetz definiert werde. Dort werde nicht die Fahrzeugtechnik festgelegt, da diese in wenigen Jahren wieder veraltet sei. Er wolle wissen, ob der Gesetzgeber im ITK-Bereich technikneutrale Bereiche definieren könne, wo regulatorisch eine bestimmte, allgemein definierte Sicherheit verlangt werden könne. Diese könne auch in die Haftung hineinspielen. Weiter führt er aus, dass die Unterscheidung Hardware, Software und Nutzer angesprochen worden sei. Eine solche werde im Automobilbereich nicht getroffen. Es gebe eine allgemeine Haftung. Zudem müssten Automobilunternehmen Fahrzeuge mit bestimmten Sicherheitsstandards garantieren, da sie sonst keine Zulassung bekämen. Außerdem gelte das Produkthaftungsprinzip. Daher sei seine Frage, ob man technikneutrale Bereiche abschichten und technikneutrale Sicherheitsanforderungen, ggf. auch gesetzlich, festlegen könne. Zudem wolle er wissen, wo diese anzusetzen seien.

Thorsten Schröder konstatiert, dass es sich um eine komplexe Frage bezüglich des Themas Computer im Kraftfahrzeug handle. Es müsse hier zwischen dem Entertainment im Kraftfahrzeug, welches optional sei und dem, welches in die Steuerung eingreife unterschieden werden. Für viele der älteren Ingenieure, die für die Produktsicherheit verantwortlich seien, sei schwer zu verstehen, dass ein kleiner Softwarefehler durchaus fatale Auswirkungen auf das Gesamtverhalten des Fahrzeuges haben könne. Er glaube, dass es sehr schwierig sei, in diesem Bereich konkrete rechtliche Vorgaben zu machen. Eindeutige Vorgaben, wie die eines Entertainmentherstellers, der vorgebe, dass gespeicherten Multimediadaten verschlüsselt sein müssten, ließen sich leichter umsetzen. Es handle sich in Fahrzeugen um vollwertige Computer, die im Endeffekt über die gleichen Probleme wie ein Heim-PC verfügten. Er glaube, es gebe in diesem Bereich definitiv Handlungsbedarf, könne dafür aber in diesem Moment Handlungsempfehlung vorlegen.

Dr. Sandro Gaycken sagt, es sei überhaupt kein Problem verschiedene Schichten einzuziehen. Es sei aber zu überlegen, wie man die Kritikalität entsprechend definiere. Man könne verschiedene kritische Schichten in Einzeltechnologien für den

Betrieb identifizieren. Zunächst müsse eine Definition von kritischen Schichten innerhalb dieser Strukturen erfolgen, bevor diese verschiedenen Strukturen nach unterschiedlicher Kritikalität beurteilt werden könnten. Dies mache man bereits bei den kritischen Infrastrukturen. Dort bedürften bestimmte Kernbereich eines besonderen Schutzes. Dies könne man auf die kritischen Prozesse und anschließend auf die kritischen Technologien als Ermöglicher dieser kritischen Prozesse herunterbrechen. Diese Fragen seien jedoch alle noch nicht beantwortet. Es gebe aktuell kein gutes Konzept für kritische Infrastrukturen. Im Moment führe man diese katalogisch auf. Bei genauerer Betrachtung finde man weitere Strukturen, die ebenfalls kritisch einzustufen seien, wie z. B. aus dem Bereich Logistik. Darüber hinaus sei für viele kritische Infrastrukturen ihre kritischen Prozesse nicht bekannt. Außerdem wisse man auch nicht, wie die Technologien verbaut seien. Dies sehe man bei Kraftwerken, die über 30 Jahre organisch gewachsene seien und unterschiedliche Hersteller aufwiesen. Mehrere Generationen von Ingenieuren hätten diese Kraftwerke gewartet und repariert. Deshalb sei es schwierig zu sagen, wo die kritischen technischen Prozesse lägen und man Fehler identifizieren könne. Eine Variante, wie man sich dem Thema Kritikalität und der Definition der schutzbedürftigen Schichten nähern könne, sei das Aufstellen staatlicher Tiger-Teams bestehend aus sehr guten Hackern. Deren Aufgabe sei es, zu versuchen in verschiedene Systeme einzudringen, um zu sehen wie leicht man über welche Vektoren eindringen könne und welche Bereiche noch schutzbedürftig seien.

Prof. Dr. Dirk Heckmann begrüßt die Frage des **Abg. Gerold Reichenbach (SPD)**. Er habe in seiner Stellungnahme dargelegt, dass er nicht nur die Möglichkeit, sondern auch die Pflicht sehe, eine Abstufung und Abschichtung vorzunehmen. Im Bereich der IT-Sicherheit betrachte man vieles zu pauschal. Man schütze Bereiche, die nicht unbedingt schutzwürdig seien, mit einem wirtschaftlich nicht vertretbaren Aufwand. Dafür vergesse man andere wichtige Systeme besser zu schützen, obwohl dies möglich sei.

Er führt aus, dass IT komplexer als der Straßenverkehr funktioniere. Im Wesentlichen lägen gleichgerichtete Interessen vor – alle Verkehrsteilnehmer wollten gesund

ihr Ziel erreichen. Der Straßenverkehr funktioniere auch deshalb so gut, weil die Teilnehmer im Zweifelsfall versuchten einen Schaden durch Bremsen abzuwenden und auch mehr Rücksicht nähmen. Dies sei in der IT nicht der Fall, da die Interessen der Nutzer und Unternehmen verschiedene seien. Einen Unfall in der IT bemerke man zunächst nicht, einen Autounfall bemerke man sehr schnell. Dies bedeute, dass in der IT auch anders abzuschichten sei als im Straßenverkehr. Es müsse zumindest zwischen gleichgerichteten und unterschiedlichen Interessen unterschieden werden. Ein gemeinsames Interesse der Provider und Nutzer sei, dass die Leitungen funktionierten und Nachrichten verschickt werden könnten. Dies werde allenfalls durch Kriminelle kompromittiert. Die Verfügbarkeit als ein IT-Sicherheitsziel sei gesellschaftlich unstreitig.

Anders verhalte es sich bei der Vertraulichkeit. Dort gebe es gesellschaftlich brisante Bereiche – beispielsweise Meinungsäußerungsfreiheit versus Persönlichkeitsrechtsverletzung. Das IT-Sicherheitsziel der Vertraulichkeit werde durch Postings kompromittiert, die im Rahmen der Meinungsäußerungsfreiheit getätigt würden. Dies sei durch den Gesetzgeber nicht einfach zu lösen, da er zwei Ziele in Einklang miteinander zu bringen habe. Hier müsse eine Abwägung stattfinden.

Weiter führt er das Thema der Integrität an. Die elektronische Kommunikation müsse sicher gemacht werden, aber wie sicher sei nicht bekannt. Das Projekt De-Mail habe im Endeffekt auch die Grundsatzfrage aufgeworfen, welches Sicherheitsniveau man anstreben wolle. Nehme man die Ende-zu-Ende-Verschlüsselung zu ernst, komme es eher zu einer kontraproduktiven Entwickelung der IT-Sicherheit. Für den Straßenverkehr habe der Gesetzgeber in Form des Sicherheitsgurtes ein mittleres Schutzniveau mit Erfolg durchgesetzt. Ähnliches sei für die IT überlegenswert. Wichtig sei die Akzeptanz der Betroffenen.

Der **Vorsitzende** dankt **Thorsten Schröder, Dr. Sandro Gaycken** und **Prof. Dr. Dirk Heckmann** für ihre Ausführungen und übergibt das Wort an **Abg. Jerzy Montag (BÜNDNIS 90/DIE GRÜNEN)**.

Abg. Jerzy Montag (BÜNDNIS 90/DIE GRÜNEN) richtet seine erste Frage an **Prof. Dr. Dirk Heckmann** und **Andreas Könen.** Er geht auf den erwähnten Spannungsbogen zwischen Zurechenbarkeit und Anonymität ein und bittet um nähere Erläuterung der Kriterien für die Abgrenzung dieser beiden Prinzipien. Schließlich sei im privaten Bereich – zum Beispiel beim Kauf und Verkauf auf eBay – als auch vom Staat in manchen Bereichen Zurechenbarkeit notwendig. Auf der anderen Seite bestehe die Anonymität, die sich die Teilnehmer im Internet wünschten. Er wolle wissen, wie dieses Verhältnis konkreter gefasst werden könne.

Seine zweite Frage richtet er an **Mirko Manske.** Er habe von stetig steigenden Fallzahlen gesprochen. Dies sei ein Thema, mit dem sich die Enquete-Kommission intensiv beschäftigen müsse. Er sagt, dass sich ein Teil des Lebens in das Internet verschiebe. Deshalb interessiere ihn, in welchem Maß es sich bei der vom BKA festgestellten Internetkriminalität um einen echten Anstieg handle und inwieweit es Phänomene der Verschiebung seien, die sich durch die immer größere Bedeutung des Internets ergäben.

Eine dritte Frage stellt er an **Thorsten Schröder**. Dieser sei für die schriftlichen Stellungnahmen zum § 202 c StGB (Strafgesetzbuch) befragt worden. **Abg. Jerzy Montag (BÜNDNIS 90/ DIE GRÜNEN)** berichtet, dass es im Bundestag vor Einführung dieses Paragraphen eine kontroverse Debatte gegeben habe. Die kritischen Stimmen seien der Auffassung gewesen, dass dieser Paragraph die Tendenz habe, kleine Unternehmer sowie rechtstreue und ehrliche Programmierer an oder über die Grenze der Kriminalität zu zerren. Die Befürworter meinten, der Paragraph sei so ausgestaltet, dass er eben jene überhaupt nicht berühre und diese durch mehrere Ausgestaltungen des Gesetzes geschützt seien. Vor dem Hintergrund der Argumente beider Seiten beleuchtet er die schriftliche Stellungnahme von **Thorsten Schröder**. Nach dessen Aussage gebe es eine so genannte IT-Security-Szene und unabhängige Sicherheitsforscher, die früher ungefragt Sicherheitslücken aufgedeckt hätten, um sich damit in der Öffentlichkeit zu profilieren. Nachdem sie dies nicht mehr könnten oder wollten, gäben sie ihre Wissen an Kunden, wie Kriminelle, Geheimdienste und andere schattige Organisationen weiter. **Abg. Jerzy Montag (BÜNDNIS 90/DIE**

GRÜNEN) wolle deshalb wissen, wer mit der IT-Security-Szene und den unabhängigen Sicherheitsforschern gemeint sei.

Prof. Dr. Dirk Heckmann hält fest, dass das Spannungsfeld zwischen Zurechenbarkeit und Anonymität durch das Grundgesetz aufgelöst werde. Es gebe ein Grundrecht auf Anonymität als Ausfluss des Rechts auf freie Persönlichkeitsentfaltung (Artikel 1 in Verbindung mit Artikel 2 GG). Zwar gehe das Bundesverfassungsgericht zu Recht von einem Leitbild des gemeinschaftsgebundenen Individuums aus, dennoch könne jeder sein Leben nach seinen Wünschen gestalten. Ein solches Grundrecht kenne jedoch Schranken. Seine Credo laute deshalb, die Gewährleistung anonymer Internetnutzung sicherzustellen solange und soweit die Zurechenbarkeit nicht aus vorrangigen Gründen erfolgen müsse. Auch Rechtsgeschäfte könnten im Internet getätigt werden, ohne die Identität vollständig preizugeben. Ebenso gebe es beim Verwaltungshandeln Abschichtungen. Bei Auskünften etwa benötige man keinen Personalausweis. Anders sehe es bei Verwaltungsakten und Anträgen aus.

§ 13 Abs. 6 TMG (Telemediengesetz) erfordere nach aktuellem Telemediendatenschutzrecht sogar die Pflicht, anonyme Nutzung von Telemedien zu ermöglichen. Deshalb sei es selbstverständlich, Bewertungsportale und Foren anonym zu bedienen. Dies möge legitim sein. Das Problem bestehe aber darin, dass es Fälle geben könne in denen die Identität von staatlichem Interesse sei, wie etwa bei der Begehung von Straftaten. Im Falle der kompletten „digitalen Vermummung“ gebe es keine praktische Möglichkeit zur Bekämpfung von Kriminalität. Psychologisch sei zu hinterfragen , wie sich die Hemmschwelle einzelner Täter verändere, wenn sie anonym handelten. Bei der Vorratsdatenspeicherung werde die Frage diskutiert, ob ein Instrument benötigt werde, um Personen die Anonymität zu nehmen. Die politische Diskussion drehe sich aktuell um die Frage nach dem besten Instrument. Er wolle keinen konkreten Vorschlag dazu machen. Er mache jedoch darauf aufmerksam, dass die Gestaltungsmöglichkeiten vielfältig seien. Recht, Technik und Organisation könne man zusammenführen.

Zuletzt weise er darauf hin, dass alle Bemühungen obsolet seien, wenn diejenigen, die nicht erkannt werden wollten, das Internet über Anonymisierungsdienste nutzten. Solange die Technik für sie spiele, indem sie die Zurechenbarkeitsinstrumente unterlaufen könnten, führe man die gleiche Diskussionen um die Umgehung von Netzsperren wie im Digital Rights Management im Urheberrecht oder dem Zugangserschwerungsgesetz. Dann seien die rechtlichen Möglichkeiten irgendwann ausgeschöpft.

Andres Könen hält fest, dass dieses Spannungsverhältnis aus Sicht des BSI ein doppeltes sei. Einerseits gebe es – zum Beispiel dort, wo das BSI entsprechende Dienste für den Kontakt zu Behörden bereitstelle – ein Repertoire von kryptographischen und informationssicherheitstechnischen Lösungen, um die Zurechenbarkeit zu gewährleisten. Andererseits gebe es kryptographische Mechanismen, die Anonymisierung gewährleisteten. Insgesamt gesehen sei dies aus Sicht des BSI die informationssicherheitliche Präventivseite.

Wenn man sich der Angriffsseite zuwende und beispielsweise an den Zugängen des IVBB (Informationsverbund Berlin-Bonn) überprüfe, wem ein Angriff zuzurechnen sei, kehre sich das Problem um. Dann zeige sich, dass das Internet in seiner aktuellen Form sehr starke, fast unfreiwillig vorhandene Mechanismen für einen Angreifer biete, so dass man ihm einen Angriff nicht nachweisen könne – dies sogar ohne die Nutzung entsprechender Dienste wie Tor. Es sei durch eine clevere Nutzung der Struktur des Internets möglich, sich außerhalb der Nachvollziehbarkeit zu bewegen und der Strafverfolgung zu entziehen. Dies beschäftige das BSI in hohem Maße.

Thorsten Schröder merkt zunächst an, dass er unter „schattigen“ Organisationen solche verstehe, die intransparent seien. Wenn es um die IT-Sicherheits-Szene und Sicherheitsforscher gehe, spreche er in erster Linie von Hackern, welche ohne Auftrag Sicherheitslücken aufspürten. Sie brächen nicht aktiv in Systeme ein und berichteten darüber, sondern analysierten die Software, mit denen jeder täglich arbeite. Entweder suchten sie gezielt nach Sicherheitslücke oder stießen zufällig auf diese. Der Sinn dahinter sei die Veröffentlichung ihrer Forschungsergebnisse. Sofern

jemand sehr lange dafür gebraucht habe ein Sicherheitsproblem zu beweisen, erwarte er Anerkennung und Respekt, nicht unbedingt Geld. Ansonsten hätte er seine Ergebnisse auch an irgendwelche Organisationen verkaufen können.

Es gebe einen offenen Markt für Exploits – Programme und Verfahren, um Schwachstellen in Software und Netzwerken auszunutzen. Diese würden offen auf Plattformen wie eBay gehandelt. Dabei werde beschrieben, welche Schwachstelle mit dem Exploit umgangen werden könne. Der Wert der Exploits auf dem freien und dem Schwarzmarkt sei dabei sehr unterschiedlich. Ein so genannter Zero-Day-Exploit – also ein Verfahren, welches noch nie der Öffentlichkeit vorgestellt worden sei – sei entsprechend wertvoll, insbesondere für Geheimdienste oder kriminelle Organisationen. Diese könnten damit sicherstellen, dass sich ein Ziel ganz sicher noch nicht gegen eine Schwachstelle geschützt habe. Sobald eine Schwachstelle öffentlich werde, gebe der Hersteller der Software einen Sicherheitspatch heraus, um die Lücke zu schließen. Geschwindigkeit sei daher – neben der Software, auf die gezielt werde – ein entscheidenden Faktor in diesem Markt.

Er sei der festen Überzeugung, dass u.a. § 202 c StGB (Strafgesetzbuch) oder zumindest die damit verbundene Diskussion dazu geführt habe, dass viele der unabhängigen Sicherheitsforscher das persönliche Risiko nicht mehr eingehen wollten. Viele sähen es nicht ein, dieses Risiko zu tragen und ihre Ergebnisse auf einem Kongress zu veröffentlichen, wenn gleichzeitig die Möglichkeit bestehe auf dem Markt viel Geld damit zu verdienen. Er schiebe nicht die komplette Schuld auf § 202 c StGB, aber er befürchte, die Debatte um die Strafbarkeit von Forschung und den Besitz von Schadsoftware, schrecke die Hackerszene ab. Dies seien keine kriminellen Organisationen, sondern Sicherheitsforscher, die dies in ihrer Freizeit gerne machten, aber auch solche, die dieser Tätigkeit beruflich nachgingen.

Mirko Manske geht auf die Frage ein, ob es sich bei Internetkriminalität um wachsende Kriminalität handle oder nur eine Verschiebung von Kriminalität ins Internet erfolge. Dies sei, so erklärt er, nicht leicht zu beantworten. Beim Überfall auf eine Bank brauche der Täter die unmittelbare Nähe zum Tatort und müsse körperlich

einigermaßen fit sein. In der digitalen Welt sei dies nicht mehr notwendig, da hier eine Straftat auch aus einer tausend Kilometer weiten Entfernung, im Keller oder Internetcafé sitzend, begangen werden könne. Banküberfälle seien jedoch durch Phishing gegen deutsche Online-Banking-Kunden nicht ausgeblieben. Es handle sich hier um eine unterschiedliche Klientel an Straftätern. Durch das Internet und E-Commerce-Dienste, sei ein neuer Tätertyp entstanden. Bestimmte Taten seien früher, aus Angst vor Strafverfolgung, nicht begangen worden. Teilweise finde sich das BKA, wenn ein so genanntes Underground Economy Forum aufgelöst werde, in Jugendzimmern von 17- oder 18-Jährigen, teilweise noch jüngeren Tätern wider, die wahrscheinlich niemals mit einem Baseballschläger in eine Tankstelle gegangen wären. Häufig werde diese Art der Kriminalität jedoch nicht mehr als Kriminalität begriffen, da die Bank, so die Attitüde der Täter, den Einkauf mit den gestohlenen Kreditkartendaten bezahlen werde.

Im Bereich der Cybercrime, so führt er aus, handle es sich tatsächlich um neue Kriminalität. Im klassischen Betrugsumfeld sei der Modus Operandi unverändert, lediglich das Transportmedium sei ein anderes. Hier könne man von einer Verschiebung sprechen. In anderen Bereichen handle es sich um neue Kriminalität. Teilweise seien alte Modelle, wie die Schutzgelderpressung, auf das neue Medium Internet übertragen worden. Vielfach seien Delikte wie digitaler Identitätsdiebstahl aber ohne das Internet auch nicht möglich. Im Internet sei es überhaupt kein Problem, eine andere Identität anzunehmen.

Problematisch sei, wie auch **Prof. Dr. Dirk Heckmann** angesprochen habe, der Umgang mit Dienstleistern wie Click and Buy oder PayPal. Denen gebe der Internetnutzer seine Kreditkartendaten im Glauben, seine Identität werde geschützt. In der Underground Economy sei das Angebot von Kreditkartendaten sehr, sehr groß. Die Nachfrage aber relativ gering, weil Kreditkarten heutzutage schwierig „auszucashen“ seien. Die Click and Buy-Accounts, T-Pay-Accounts von der Telekom und PayPal-Accounts seien begehrter, weil dahinter scheinbar verifizierte Identitäten lägen. Ein Kreditkartendatensatz koste momentan ungefähr 80 US-Cent. Das Einkaufen damit sei jedoch schwierig, da, zum Beispiel bei Amazon, zunächst

Fragen zu beantworten seien, die nur der Karteninhaber kenne. Viel geschickter sei es daher, den PayPal-Account eines Internetnutzers zu übernehmen, weil in dem PayPal-Account sowohl eine verifizierte und per Lastschrift bestätigte Bankverbindung als auch eine Kreditkarte liege. Mit dieser Ausprägung der digitalen Identität, auf die sich alle verließen, sei es deutlich einfacher „einzukaufen".

Mirko Manske teilt mit, dass aus seiner Sicht darüber nachgedacht werden müsse, ob es eine gute Idee sei, dass die Internetnutzer den drei, vier Global Playern in diesem Markt all ihre Daten anvertrauten. Ein Unternehmen wie Google verfüge bereits über viele Informationen einer Person und sei, dank des Bezahlproduktes Google Checkout, letztendlich in der Lage ihr Konsumverhalten nachzuvollziehen. Als Enduser müsse man sich fragen, ob man nicht die gute ehrliche Kreditkarte bevorzugen sollte. Im Betrugsfall könne man so einfach eine neue Karte bestellen.

Prof. Dr. Dirk Heckmann weist bezüglich seiner zuvor gemachten Ausführungen daraufhin, dass diese nicht als Empfehlung für einen der genannten Dienstleister aufzufassen seien, sondern lediglich als Beschreibung des Phänomens dienten.

Dr. Sandro Gaycken greift die Frage nach der Zurechenbarkeit auf, um hier einen weiteren Gesichtspunkt hinzuzufügen. Unumstritten sei, dass Zurechenbarkeit nicht gerichtsfest hergestellt werden könne. In Analysen sei zwar feststellbar, dass ein Angriff aus Russland oder China komme. Dies dürfe und könne jedoch niemals, – auch bei den Analysten im nachrichtendienstlichen Bereich – so verstanden werden, dass dadurch eine Handlung gerechtfertigt werde. Dies sei eine ganz wichtige Einsicht, weil dadurch nämlich verschiedene Elemente unseres Rechtssystems wegfielen. Eine Regulierung und Strafverfolgung sei nicht möglich und internationales Recht nur sehr begrenzt anwendbar. Dadurch, dass der Angreifer nicht reguliert werden könne, müssten folglich die betroffenen potenziellen Systeme viel stärker reguliert werden. Dies sei zu berücksichtigen.

Der **Vorsitzende** dankt **Prof. Dr. Dirk Heckmann, Andreas Könen, Thorsten Schröder, Mirko Manske** und **Dr. Sandro Gaycken** und für ihre Ausführungen und übergibt das Wort an **SV Annette Mühlberg**.

SV Annette Mühlberg richtet ihre Fragen an **Mirko Manske**, **Prof. Dr. Jochen H. Schiller** und **Thorsten Schröder**. Ihre erste Frage greife das Thema der kritischen Infrastrukturen auf. Sie sei daran interessiert zu erfahren, ob angesichts des zunehmenden Risiko- und Schadenspotenzials im Rahmen der Nutzung von Netzkommunikation nicht auch gewisse Abhängigkeiten vermieden werden könnten. Sie interessiere, wo unnötige Risiken eingegangen würden. Ihre Frage ziele hier nicht nur auf AKWs (Atomkraftwerk), sondern auf verschiedene Branchen. Des Weiteren wolle sie wissen, ob nicht auch ein Rat gegeben werden solle, wo unnötigerweise einem Hype nachgegangen und dadurch eine Sicherheit, die bereits vorhanden gewesen sei, aufs Spiel gesetzt werde.

Sie bittet die Sachverständigen um ihre Einschätzung, inwieweit die Einrichtung einer nationalen Kontaktstelle Cybercrime-Bekämpfung im Rahmen einer solchen institutionalisierten Public-Private-Partnerships wirklich hilfreich sei oder inwieweit nicht auch dort neue Risiken entstünden. Sie stellt die Frage in den Raum, ob es gewisse Interessen, vielleicht auf Seiten des Staates, gebe dort auch eine eigene Rolle im Sinne der Informationserlangung wahrzunehmen.

Mirko Manske führt aus, dass bei der Beantwortung der Frage, ob heutzutage Systeme ins Internet geschoben werden, die da gar nicht zwingend hingehörten, der Kostenaspekt eine wichtige Rolle spiele. In Gesprächen, sowohl mit Teilen der Verwaltung als auch mit der Privatindustrie, werde immer auf die Kosten verwiesen. Online-Banking sei von den Banken nicht vorangetrieben worden, weil es sich um ein tolles Produkt handle, sondern weil für 5000 neue Online-Banking-Kunden im ländlichen Bereich eine Filiale geschlossen werden könne. Bestimmte Tendenzen dazu seien auch in der öffentlichen Verwaltung erkennbar.

In einigen Foren, die das BKA beobachte, seien die ersten Anbieter von Elster-Datenströmen aufgetaucht. Dies bedeute, dass von einem Trojaner die komplette Steuererklärung, die jemand SSL-verschlüsselt an seine Finanzverwaltung übermittelt habe, mitgeschnitten worden sei. Der Angreifer, der die Daten nun besitze, habe das häufig auftretende Problem, die Daten nicht unmittelbar monetarisieren zu können. Daher werde in der Community nachgefragt, ob dort die Daten verwenden könne.

In Hamburg sei es, so führt **Mirko Manske** aus, mittlerweile möglich Fahrzeuge an-, um-, und abzumelden ohne noch tatsächlich auf der Zulassungsstelle zu erscheinen. Man bekomme einen Brief mit einer PIN zugeschickt und könne dies online erledigen.

Da das Thema Kostendruck auch in der öffentlichen Verwaltung omnipräsent sei, könne er sich gut vorstellen, dass auch Gemeinden oder Bundesländer die Idee, die Kunden die Arbeit machen zu lassen, aufgriffen. Die Privatwirtschaft setze dies schon seit 10 Jahren um. Banken beispielsweise beschäftigten keine Mitarbeiter mehr, um Überweisungsträger entgegenzunehmen, einzugeben und letztendlich dafür zu sorgen, dass Computer untereinander Geld hin- und herschöben. Der Kunde könne dies tun. Dafür berechne man ihm nur die Hälfte der Kontoführungsgebühren. Es sei nicht undenkbar, dass auch in der öffentlichen Verwaltung in Zukunft noch andere Ideen entstünden.

Ein weiteres damit unmittelbar zusammenhängendes Problem sei fehlende Medienkompetenz. Die neue Generation, die mit Macht ins Netz dränge – die Generation 3.0 – sei mit all diesen Diensten, mit der 24/7-Erreichbarkeit und 24/7-Kommunikation aufgewachsen und habe ein relativ geringes Schutzbedürfnis für ihre Informationen. Sie begreifen – zumindest in den jüngeren Jahren – nicht, dass ihre Daten etwas Wert seien. Diese Generation werde mit hoher Wahrscheinlichkeit hinsichtlich neuer Modelle aus der Wirtschaft als auch der Verwaltung bestimmte kritische Fragen nicht mehr stellen. Für sie sei es völlig normal ihr ganzes Leben bei Facebook offenzulegen.

Abschließend geht er auf die Frage bezüglich der erwähnten institutionalisierten Public-Private-Partnership ein. Die Idee sei, das bestehende Kommunikationsproblem zu lösen. Er wolle als Beispiel das Aufkommen von Phishing im Jahre 2005 heranziehen. Das BKA habe damals zwar bei den Banken nachgefragt, wie schlimm Phishing sei. Es habe jedoch einige Zeit gedauert, bis die erste Bank eingesehen habe, ihre Kunden vor Phishing warnen zu müssen. In der Branche sei danach ein Aufatmen zu hören gewesen. Endlich habe eine Bank das Problem benannt, welches auch bei den anderen aufgetreten sei. Die betroffenen Akteure kommunizierten nach wie vor nur unzureichend miteinander. Es bestehe die Angst, offen zu sagen, dass man als Unternehmen angegriffen bzw. kompromittiert worden sei. Dies habe zu der Idee geführt, eine Informationsbörse einzurichten, wo in einer vertrauensvollen Atmosphäre derartige Informationen ausgetauscht werden könnten. Die Idee sei, Informationen zusammenzuführen, die andernfalls nicht zusammenfänden.

Prof. Dr. Jochen H. Schiller stellt dar, dass es sich beim Entstehen kritischer Infrastrukturen oftmals um einen schleichenden Prozess handle. Viele wissen beispielsweise nicht, dass es eigentlich kein Telefonsystem mehr gebe, mit dem im Ernstfall ein Notruf abgesetzt werden könne. Plötzlich habe das Telefon bei einem Stromausfall nicht mehr funktioniert. Es werde immer stärker vernetzt, wodurch auf einmal etwas zur kritischen Infrastruktur werde. Da helfe auch keine Aufklärung; die Zusammenhänge seien einfach zu komplex.

Des Weiteren schlichen sich auch neue Prozeduren ein, beispielsweise die mTAN (mobile TAN) als Ersatz für den papierbasierten TAN Brief. Dieser Medienbruch sei sinnvoll gewesen – das Papier liege sicher beim Nutzer in der Schublade. Eine SMS abzufangen sei trivial und die mTAN könne leicht aus der SMS ausgelesen werden. Eine GSM-Basisstation koste heutzutage vielleicht 600 Euro, eine UMTS-Basisstation circa 1 000 Euro. Man gehe neue unnötige Risiken ein, gewinne dadurch aber natürlich an Komfort. Durch eine Entnetzung erfahre man einen Komfortverlust. Diese stelle jedoch ehrlicherweise die einzige Option dar.

Als Beispiel wolle er die Röhn-Klinikum AG anführen. Hier habe man sich beim Bau einer neuen Klinik bewusst dafür entschieden eigene Leitungen für ein klassisches Telefonnetz zu legen. Ein Bewußtseinswandel sei notwendig. Zunächst müsse man klären, was eigentlich die Schutzziele seien. Es müsse eindeutig gesagt werden, welchen Wert man der ständigen Verfügbarkeit gewisser Funktionen beimesse. Die Frage sei, ob sich der Aufbau einer eigenen Infrastruktur lohne. Kein Netzbetreiber könne heute mit Gewissheit sagen, wie sein Netz wirklich aussehe. Man könne also nicht bestimmen, was man schützen wolle. Um diesem schleichenden Prozess entgegenzuwirken, sei es daher wichtig die Schutzziele zu bestimmen.

Thorsten Schröder schließt seine Anwort an die Ausführungen von **Mirko Manske** an. Dieser habe bereits angedeutet, dass Kosten eine große Rolle spielten. Kosteneinsparungen gingen immer mit weniger Sicherheit einher. Auch Komfort wirke sich negativ auf die Sicherheit aus. Als Analogie nennt er Überwachungskameras, die als Mittel der Kosteneinsparung auf Bahnhöfen Personal ersetzten.

Weiter führt er aus, dass die Entwicklung des elektronischen Personalausweis teilweise auch den Identitätsdiebstahl begünstige. Möglicherweise sei die Technik heute noch nicht so ausgereift, dass großflächige Angriffe durchgeführt werden könnten – auszuschließen sei dies aber nicht. Im Vergleich zur digitalen Signatur enthalte die normale Unterschrift Metadaten. Im Streitfall könne anhand dieser ein vom Gericht bestellter Gutachter nachweisen, ob es sich um die fragliche Handschrift handle. Bei einer digitalen Signatur habe man diesen Rettungsanker nicht. Jede digitale Signatur sehe gleich aus. Hier stelle sich auch die Frage, wie sich jemand, dessen Identität missbrauch worden sei, rechtfertigen könne eine Unterschrift nicht geleistet zu haben.

Früher dienten die unbezahlbaren Ausgaben im Endeffekt auch als Schutzmechanismus. Heute sei es möglich einen GSM-Access-Point für 400 Euro auf eBay zu erwerben. Im Laufe der Zeit hätten sich die Kosten für Angriffswerkzeuge minimiert. Dies könne möglicherweise auch mit dem nPA (neuer Personalausweis) geschehen.

Bereits heute seien unabhängige Sicherheitsforscher in der Lage, aus sicher geltenden SmartCard Chips die geheimen Schlüsselmaterialien zu extrahieren. Genau dies solle jedoch nicht möglich sein. Die Kosten für das Klonen einer SmartCard, wie sie zum Beispiel im nPA verwendet werde, beziffern sich ungefähr auf 80 000 US-Dollar. Natürlich erfordere dies den physikalischen Zugriff auf die Karte. Man könne jedoch die Karte, die vom Benutzer am Computer angeschlossen werde, über das Internet missbrauchen. Diese Angriffsszenarien erschienen heute vielleicht ein bisschen konstruiert. Denkbar sei, dass in ein paar Jahren diese Angriffe so durchgeführt würden, wie man heutzutage E-Mails mit Phishing-Aufforderungen verschicke.

Mirko Manske greift die Ausführungen von Thorsten Schröder auf. Er stimme zu, dass sich ein User beispielsweise mittels nPA autorisieren könne. Beim Online-Banking sei es aber durch Echtzeitmanipulation, die durch lokal installierte Software ausgelöst werde, bereits heute möglich, dass ein autorisierter Kunde anstatt seiner Mietüberweisung unbemerkt eine manipulierte Überweisung auslöse. Hier stelle sich nicht mehr die Frage, ob jemand eine Transaktion durchgeführt habe, sondern ob die getätigte Transaktion wirklich die gewesen sei, die er auslösen wollte. Durch die einmalige Identifizierung werde fälschlicherweise eine Sicherheit vorgegaukelt. Aus seiner Sicht fehle sowohl dienstlich als auch privat eine vernünftige Transaktionsabsicherung über einen nicht angreifbaren Kanal. Unterschiedliche Unternehmen, mit denen er Gespräche geführt habe, sähen dafür keinen Markt. Aus Sicherheitsgründen sei jedoch eine digitale Einbahnstraße nötig. Diese sei mit Hilfe eines Devices, welches nur Daten von bestimmten Absendern empfangen könne, herzustellen. Auf diese Leseeinheit könne beispielsweise Amazon oder eine Bank Daten senden und dem Anwender die Möglichkeit geben, seine Transaktion noch einmal zu überprüfen.

Der **Vorsitzende** dankt **Mirko Manske, Prof. Dr. Jochen H. Schiller** und **Thorsten Schröder** für ihre Ausführungen.

Der **Vorsitzende** stellt zwei Fragen. Die erste Frage richtet sich insbesondere an **Dr. Sandro Gaycken** und **Thorsten Schröder**. Laut der bisherigen Ausführungen sitze man auf einer Infrastruktur und einem System, die bzw. das im Kern faul (engl. rot) sei. Was müsse insbesondere durch die Enquete-Kommission und die Politik getan werden, um diesen Zustand schnellstmöglich zu überwinden?

Weiter führt er aus, dass eine Erhöhung der Sicherheit immer mit zwei Nachteilen verbunden sei: höheren Kosten und Unbequemlichkeit. Im Rahmen der zweiten Frage bittet er **Prof. Dr. Jochen H. Schiller** und **Andreas Könen** um einen Rat, wie man die Menschen davon überzeugen könne, Unbequemlichkeit auf sich zu nehmen und womöglich auch höhere Kosten für mehr Sicherheit zu akzeptieren.

Thorsten Schröder plädiert dafür, die potenziellen Sicherheitsrisiken auch öffentlich zu thematisieren und nicht immer nur grundsätzlich abzulehnen. Er halte Sensibilisierung und Bildung für wesentliche Punkte. Dem Anwender müsse erklärt werden, dass er sich nicht bedingungslos auf seinen Computer verlassen könne. Eine gewissen Skepsis müsse vorhanden sein. Eine konkrete Lösung für diese umfangreichen Probleme vorzuschlagen, falle ihm schwer.

Dr. Sandro Gaycken sagt, er halte das Problem des ‚rotten cores' für relativ einfach zu lösen. So führt er aus, dass es in Hochsicherheitsbereichen Konzepte für hochsichere IT gebe. Diese seien jedoch noch nicht am Markt und müssten erst entwickelt werden. Zudem seien sie mit sehr starken Einbußen an Bequemlichkeit und mit sehr hohen Kosten verbunden. Allerdings könne festgelegt werden, dass ein solches Konzept auch nur in sehr bestimmten Bereichen anzuwenden sei. Der Durchschnittsnutzer brauche keine Hochsicherheits-IT, um Online-Banking durchzuführen. Aber in Bereichen wie Kraftwerken, Rüstungsgütern, Geheimschutz oder ähnlichem, müsse man diese Überlegungen anstellen. Andererseits seien auch solche sehr hochsicheren Systeme noch angreifbar. Aus dem nachrichtendienstlichen Bereich seien einige Angriffe auf sehr abgeschlossene Hochsicherheitsbereiche bekannt, in denen andere Nachrichtendienste fingierte Hardwarekomponenten in die Gebäude rein- und raustragen ließen.

Eine triviale Einsicht sei zwar, dass es hundertprozentige Sicherheit nicht gebe, aber in der IT könne eine zweiprozentige Unsicherheit immer noch eine hundertprozentige Schadensfolge nach sich ziehen. Sofern der Angreifer einen kleinen Vektor in das System finde, könne er noch immer maximal Daten abziehen und das System kompromittieren. Gerade im Hochsicherheitsbereich führe dies zu Überlegungen stärker von Vernetzung und IT insgesamt Abstand zu nehmen. In vielen Hochsicherheitsbereichen, insbesondere in den USA, überlege man, wie auch ohne IT noch die gleiche Effizienz erzielt werden könne und welche alternativen Prozesse dafür einzuführen seien. Es müsse geprüft werden, welche abgestuften Konzepte für Bereiche, die keinen Hochsicherheitsschutz benötigten, avisiert werden könnten. Hier könne man auch langfristige Ziele formulieren.

Ein bedeutender Punkt sei auch das Programmieren sicherer Software. Es müsse den Unternehmen aufgezeigt werden, dass für sichere Produkte eine Nachfrage entstehen könne. Auch den Informatikern müsse beigebracht werden, sauber und sicher zu programmieren. Sicherheit müsse zu einem Bestandteil des Entwicklungsprozesses werden. So komme man auch in den Alltagsbereich hinein. Wichtig sei aber, so unterstreicht er, sich bewusst zu sein, dass IT immer ein gewisses Sicherheitsrisiko berge. Durch die Komplexität der damit verbundenen Prozesse sei Kontrolle und Transparenz relativ schwer zu erreichen. Es bestehe immer ein Risiko. Bei großen Netzwerken sei auch eine größere Anbindung an potenzielle Angreifer gegeben. Hier sei vielleicht gesellschaftlich zu hinterfragen, ob eine Vernetzung in diesem exzessiven Maße notwendig sei. Vor allem, wie **Mirko Manske** dargelegt hat, da vieles nur aus Kostenersparnisgründen stattfinde.

Prof. Dr. Jochen H. Schiller erklärt, dass er einen Dreiklang für sinnvoll halte. Zunächst müsse der Staat für die Netzbetreiber verpflichtend festlegen, dass beispielsweise der Notruf immer zu funktionieren habe. Dadurch entfalle im Hintergrund vieles, das von den Netzbetreibern zur Zeit aus Bequemlichkeit gemacht werde. Für dieses zu schützende Ziel müsse daher eine Verpflichtung bestehen.

Zweitens müsse Sicherheit ein Wettbewerbsvorteil werden. Firmen könnten beispielsweise damit werben, dass sie im Monat weniger Angriffe als eine andere Firma erführen. Dies müsse natürlich getestet werden, ähnlich den ADAC-Tests von Fahrzeugen. Schließlich würden bei Bit pro Sekunde auch Vergleiche gezogen. Er frage sich daher, warum dies nicht auch bei Angriffe pro Monat geschehe. Es entstünde ein Wettbewerbsvorteil.

Als Drittes führt er die Aufklärung des Bürgers an. Man solle nicht mahnend an den Bürger herantreten, da die Materie viel zu komplex sei. Aber eine gewisse Aufklärung, dass wie auch immer geartete Gütesiegel oder Vergleiche tatsächlich einen Vorteil für die Bürger brächten, sei anzuraten. Er fasst zusammen, dass diese drei Stufen von der Verpflichtung bis zur Aufklärung notwendig seien.

Andreas Könen erklärt, dass Built-in-Security vor allem für Bürger sowie kleine und mittlere Unternehmen sinnvoll sei. Dies bedeute, dass Sicherheit auch unmittelbar mit der IT mitgeliefert werde und der Nutzer entsprechend sensibilisiert und vorgebildet sei. Gefordert seien die Unternehmen, die solche Angebote im IT-Bereich für kleine und mittlere Unternehmen erstellten. Die dafür notwendigen Grundlagen der IT-Sicherheit seien längst vorhanden und könnten gewährleistet werden.

Anders stelle es sich bei den kritischen Infrastrukturen dar. Bevor Maßnahmen ergriffen und die damit verbundenen Kosten bewertet werden könnten, müssten für die kritischen Infrastrukturen zunächst die entscheidenden Kernbereiche identifiziert werden. Diese seien hoffentlich separiert. Anderenfalls könne dort schon mit entsprechenden klaren Maßnahmenpaketen für eine Trennung gesorgt werden. In Standards und Richtlinien müsse beschrieben werden, wie ein solches System aussehen müsse. Die Umsetzung sei – auch mit Auflagen versehen – in die identifizierten kritischen Bereiche hineinzubringen. Für den Bereich des Geheimschutzes werde dies in der Bundesrepublik Deutschland zum Glück noch sehr straff gehandhabt. Für alle Informationen oberhalb des Verschlussachengrades ‚Vertraulich' erfolge genau diese Trennung der informationstechnischen Systeme. Menschliche Fehlent-

scheidungen mögen vorkommen, aber dort, wo das BSI für Geheimschutz verantwortlich sei, werde diese Trennung stringent durchgehalten.

Der **Vorsitzende** fragt nach, ob **Andreas Könen** hier den Staat in der Verantwortung sehe. Er bittet auch **Prof. Dr. Dirk Heckmann** um Antwort.

Andreas Könen führt aus, dass es im Bereich des Geheimschutzes eine klare Befugnis des BSI gebe. In den zuvor genannten Bereichen könne das BSI nur Standards und Richtlinien als Empfehlung weitergeben. Der Gesetzgeber müsse entscheiden, welche Befugnisse das BSI im Bereich kritische Infrastrukturen erhalten solle.

Prof. Dr. Dirk Heckmann weist darauf hin, dass es immer auf die Resultate solcher Maßnahmen ankäme. Seien damit Grundrechtseingriffe oder sonstige Nachteile verbunden, so geschehe dies ohnehin immer unter dem Gesetzesvorbehalt. Der Gesetzgeber müsse tätig werden. Soweit dies nicht der Fall sei, gebe es einen Gestaltungsspielraum. Dort plädiere er eher für Subsidiarität des Staates, welcher versuchen solle, die Selbstregulierungskräfte der Wirtschaft und auch der Gesellschaft zu stärken. Solle dies nicht gelingen, schließe er gesetzliche Maßnahmen nicht aus.

Der **Vorsitzende** dankt **Dr. Sandro Gaycken, Prof. Dr. Jochen H. Schiller, Thorsten Schröder, Andreas Könen und Prof. Dr. Dirk Heckmann** für ihre Ausführungen und übergibt das Wort an **SV padeluun**.

SV padeluun richtet seine erste Frage an **Prof. Dr. Jochen H. Schiller** und **Andreas Könen**. Er wolle wissen, ob es Möglichkeiten gäbe Bürgerinnen und Bürgern Werkzeuge zur Verfügung zu stellen, mit denen sie auf einfache Weise feststellen könnten, ob ihr Rechner beispielsweise mit einem Trojaner infiziert sei. Er spreche hier nicht vom üblichen Virenscanner – wie auch immer ein solches Werkzeug aussehen könne. Etwas Ähnliches habe man im Jahr 2003 probiert als durch das Wirtschaftsministerium das Projekt GnuPG (GNU Privacy Projekt, GnuPP) mitfinanziert worden sei. Dieses Projekt sei jedoch nicht sehr erfolgreich gewesen. Das BSI betreibe

eine gute Webseite mit Informationen und stelle auch CDs zur Verfügung. Er frage sich, ob dies ausgebaut werden könne.

Er bittet **Dr. Sandro Gaycken** um Beantwortung der zweiten Frage. Er wolle wissen, inwiefern man Facebook, Google, Passenger Name Records, SWIFT oder EDS auch schon als einen Spionageangriff werten müsse. Des Weiteren interessiere ihn, ob er es für vorstellbar halte, Whistleblowing auszubauen, um denjenigen, die Sicherheitslücken entdeckten, auch eine Möglichkeit zu geben diese mitteilen zu können – ohne Sorge haben zu müssen dafür belangt zu werden. Über viele Jahre hätten sich diese Personen an den Chaos Computer Club oder FoeBuD gewandt, um solche Informationen weiterzugeben.

Nun wendet er sich an **Mirko Manske**. Er bittet ihn zu erläutern, ob das BKA neben der Erfassung von Taten mittels Internet auch Taten mittels Brief oder mittels Auto erfasse. Von Polizisten, die er kenne, höre er, dass es an Personal mangele. Es interessiere ihn, wie viele Polizisten aus seiner Sicht fehlten und wie viel Kosten aufgewendet werden müssten. Insbesondere frage er sich, wie viele Polizisten notwendig seien, um an anderer Stelle sehr viel Überwachung oder Vorratsdatenspeicherung einsparen zu können. Er sei erklärter Gegner von Vorratsdatenspeicherung, könne aber auch nicht mehr sagen, als das man mehr Beamte brauche. Er habe gehört, dass auch das Beförderungsrecht verändert werden müsse, damit die qualifizierten Personen in diesem Feld arbeiten könnten und nicht nur in verwaltende Positionen befördert würden.

Eine letzte Frage richtet er an **Thorsten Schröder**. Er habe die unternehmensinterne Zertifizierung angesprochen. Er bittet ihn auszuführen, wie eine dezentrale Zertifizierung realisiert werden könne.

Prof. Dr. Jochen H. Schiller sagt, er könne vorrangig etwas zu Werkzeugen sagen. Es sei gefragt worden, ob es etwas für den Bürger gebe, dass derzeit in der Entwicklung sei und über einen Virenscanner hinausgehe. Er stellt klar, das Hauptproblem seien in der Zukunft – aber auch bereits heute – Handys und Smartphones mit ak-

tuell 5,8 Milliarden Nutzern. Das normale Internet und klassische PCs stürben letztlich aus. Die Forschungsgemeinschaft entwickle zur Zeit Werkzeuge, die dem Bürger im einfachen Ampelmodell sagten, was auf seinem Gerät los sei. Dies solle dazu dienen, dass man den Entwicklern von Viren nicht immer hinterherlaufe, so wie dies der normale Virenhersteller mache. In der Tat werde – gefördert vom Bundesministerium für Bildung und Forschung – an solchen Werkzeugen gearbeitet.

Andreas Könen erklärt, es gebe die Initiative botfrei.de. Der Bürger könne dort eine Software abrufen und mit dieser prüfen, ob sein System von Schadsoftware befallen sei. Dies sei ein interessantes Beispiel, denn es zeige, dass eine solche Initiative nur funktioniere, wenn die technischen Ansätze des BSI mit irgendeiner Form unternehmerischer Initiative gepaart würden. Ansonsten habe man nicht die erforderliche Reichweite, die man brauche um 80 Millionen Deutsche mit Informationssicherheit zu versorgen. Dies sei ein Grund, aus dem das bereits zitierte GnuPG-Projekt nicht flächendeckend erfolgreich gewesen sei. Es gebe bereits ein Resultat namens Gpg4win, welches durchaus auch erhältlich und nicht gänzlich erfolglos sei. Allerdings habe es auch nicht die Publicity erreicht, die es mit einem potenten Partner hätte haben können. Daher verweise er erneut auf das Modell, welches er bereits beschrieben habe. Es müsse der vorkonfigurierte Rechner mit den von **Prof. Dr. Jochen H. Schiller** beschriebenen Funktionen auf den Markt gebracht werden. Dies sei entscheidend.

Dr. Sandro Gaycken führt aus**,** dass Facebook, SWIFT usw. Werkzeuge seien, die von den Nachrichtendiensten infiltriert würden. Auch Software und Hardware sei bereits infiltriert, aber natürlich weigerten sich die Hersteller sehr nachhaltig dies offiziell bekannt zu geben. In den USA gebe es ein Abkommen, welches die Hersteller verpflichte, die NSA (National Security Agency) teilweise an der Entwicklung zu beteiligen. Es gehe zunächst nur um das Domestic Law Enforcement, da man im eigenen Land diese Kommunikationskanäle kontrollieren können möchte. Es sei jedoch nicht bekannt, ob dies anschließend ausgebaut werde. Es sei festzuhalten, dass viele Produkte und technische Verfahren wie SWIFT, aber auch Soft- und

Hardware, prinzipiell nicht vertrauenswürdig seien, wenn sie in anderen Ländern unter unklaren Konditionen hergestellt würden.

Man wisse auch von sehr vielen Diensten und organisierten Kriminellen, dass diese die durchaus plausible Überlegung anstellten, statt in ein fertiges Produkt bereits in ein unfertiges einzubrechen, also die Entwicklungsabteilung von Software- und Hardwareherstellern zu infiltrieren. Dort an der Entwickelung beteiligt zu sein, sei besonders lukrativ. Dies treffe vor allem zu, wenn man besonders früh in die Entwicklungsphase eintrete. Es sei in der Tat ein Problem, das sehr viele – wenn nicht alle – etablierten Produkte unter Umständen schon eine Hintertür für Dienste eingebaut hätten. Dies betreffe insbesondere Produkte aus den USA und China und sei ein großes Problem, da inzwischen fast alle Hardware aus diesen Ländern komme. Es sei dringend zu überlegen, wie Hardware integer hergestellt werden könne. Er wisse, dass das BSI im Bereich Routing bereits solche Überlegungen anstelle.

Das von **SV padeluun** angesprochene Security Whistleblowing sei sicherlich wünschenswert, insbesondere da die Neigung zum freiwilligen Disclosure in den Firmen sehr niedrig sei. Einerseits hätten die Verantwortlichen einer IT-Abteilung massive Bedenken dem CEO mitzuteilen, dass es ein Problem gegeben habe, weil sie im Missverständnis ihrer Aufgabe häufig entlassen würden. Andererseits wolle auch ein CEO die Öffentlichkeit nicht von Problemen unterrichten, da er einen Imageverlust fürchte. Es sei allerdings schwierig, den Whistleblowern eine verlässliche Plattform zur Verfügung zu stellen. Er habe gehört, es bestünden sehr große Bedenken bezüglich der Vertrauenswürdigkeit der technischen Prozesse und der Integrität der involvierten Personen – insbesondere nach den Problemen mit Wikileaks und Openleaks. Zu erwägen sei möglicherweise die Initiierung eines Forschungscalls, der versuche Mechanismen bereitzustellen mit denen man Sicherheitsprobleme öffentlich machen könne, falls diese verschwiegen würden. Hier seien vielleicht Universitäten oder Nichtregierungsorganisationen als Ansprechpartner für solche Plattformen gefragt.

Mirko Manske sagt, es gebe keinen Merker ‚Brief' in der Polizeilichen Kriminalstatistik (PKS). Der sogenannte Merker ‚Tatmittel Internet' sei vor vielen Jahren eingeführt worden als das Internet zunehmend wichtiger geworden sei. Ursprünglich sei dieser dafür gedacht gewesen ein Messbarkeitskriterium zu entwickeln, anhand dessen die Polizei beurteilen könne, ob das Internet ein Problem sei. Damals habe es – insbesondere im monetären Bereich – diese Vielzahl von Straftaten noch nicht gegeben. Der Merker sei erhalten geblieben, aber es habe auch keine wesentliche Weiterentwicklung in der PKS gegeben. Die PKS könne bis heute nicht ausdrücken, was eigentlich bei Phishing passiere. Phishing könne nicht gezählt werden. Die einen zählten es als Geldwäsche, die anderen als Computerbetrug, der Dritte zähle es nur als Ausspähung von Daten. Es gebe keine Tat Phishing, da dies strafrechtlich mehrere unterschiedliche Einzeltaten seien.

Die Frage, wie viele Beamte die Vorratsdatenspeicherung ersetzten, sei nicht zu beantworten. Die Schwierigkeiten, die es heute im personellen Bereich gebe, hingen damit zusammen, dass erst vor zwei bis drei Jahren begonnen worden sei, für diese neue Welt strukturiert Personal auszubilden. Gehe heute jemand in Düsseldorf auf eine Wache und sage, er sei ein Phishing-Opfer, werde die Anzeige in der Regel von einem uniformierten Beamten aufgenommen. Schicke man diesen an einen Tatort für ein Kapitaldelikt, wisse er, was er zu tun habe, weil im das vor 20 Jahren beigebracht worden sei. In dieser Phase befinde man sich zur Zeit für die neue Welt. Bund und Länder hätten sich auf den Weg gemacht, aber dieser sei lang. Er stimme der Aussage zu, dass sich etwas am Beförderungswesen ändern müsse. Wolle man sich im Bereich Cybercrime wirklich effektiv wehren, dürfe man nicht erwarten, dass man einen guten Programmierer für vergleichsweise wenig Gehalt anwerben könne. Er glaube aber auch, dass der Staat schon dabei sei, diese Spezialistenlaufbahnen zu schaffen. Man müsse allerdings auch anerkennen, dass man als Beamter – wie er im Alter von 39 Jahren – bereits am Ende der Karriere angekommen sein könne, weil man das, was auf Grund der Qualifikation möglich sei, bereits erreicht habe. Hier könne man über eine stärkere Durchlässigkeit nachdenken. Ein wesentlicher Kritikpunkt sei früher der Rotationszwang beim BKA gewesen. Nach vier bis fünf Jahren seien die Mitarbeiter in andere Abteilungen versetzt worden,

um eine breitere Verwendung zu erhalten. Es sei aber bei der Polizei mittlerweile das Bewusstsein entstanden, dass die Ausbildung von qualifiziertem Personal langwierig sei und dieses in einem Bereich bleiben sollte.

Er stellt klar, dass Vorratsdatenspeicherung und die Anzahl an Polizisten nicht zusammenhingen. Die Vorratsdatenspeicherung aus Strafverfolgungssicht sei für den Bedarfsfall relevant. Wenn eine Straftat passiere, könne man in der Zeit zurückgehen und die Frage stellen, wer zu diesem Zeitpunkt für eine IP-Adresse verantwortlich gewesen sei. Man könne die aktuelle Situation auch in die reale Welt übertragen. Man stelle sich vor, dass die Fahrzeuge auf der Autobahn keine Kennzeichen hätten und ein Unfall passiere. Der Bürger erwarte von der Polizei, dass sie ihm mitteile, gegen wen er seine zivilrechtlichen Ansprüche geltend machen könne. Wenn also ein Provider sechs Monate retrograd sagen könne, welcher Anschluss zu einem bestimmten Zeitpunkt für eine IP-Adresse verantwortlich gewesen sei, gebe es der Strafverfolgung die Möglichkeit die Ermittlungen fortzusetzen. Er kenne alle Argumente. Er frage sich jedoch, welche Möglichkeit die Deutsche Telekom anderenfalls habe, mitzuteilen wer zu einem bestimmten Zeitpunkt für eine IP-Adresse verantwortlich gewesen sei, um beispielweise einen Kunde zu informieren, dass sein PC mit einer Malware infiziert sei oder um weiterführende Ermittlungsmaßnahmen anzusetzen.

In den alten Zeiten, als es die Vorratsdatenspeicherung noch gegeben habe, konnten Täter ermittelt werden, weil sie sich permanent freie WLANs genommen hätten oder in WLANs eingebrochen seien. Aus verschiedenen Ermittlungsschritten sei man auf eine Schnittmenge gekommen, die zum Täter geführt habe. Aus Sicht des BKA sei es eine unzulässige Verkürzung zu sagen, über die IP-Adresse komme man immer direkt zum Täter. Die IP-Adresse sei für das BKA in vielen Fällen der erste und zentrale Ermittlungsansatz, an dem es ansetze.

Thorsten Schröder kann auf die gestellte Frage keine pauschale Antwort geben. Anderenfalls müsse er auch einen Lösungsansatz für die Reparatur der kaputten PKI-Infrastruktur präsentieren.

Der **Vorsitzende** dankt **Prof. Dr. Jochen H. Schiller, Andreas Könen, Dr. Sandro Gaycken, Mirko Manske** und **Thorsten Schröder** für ihre Ausführungen und übergibt das Wort an **Abg. Jimmy Schulz (FDP)**.

Abg. Jimmy Schulz (FDP) teilt mit, er habe sich bei Twitter nach Fragen der twitternden Zuhörer erkundigt. Eine dieser Fragen stellt er an **Andreas Könen**. Er wolle wissen, ob die Behörden in Deutschland seiner Meinung nach ausreichend gegen Attacken abgesichert seien. Zudem interessiere ihn, ob die Daten jedes Einzelnen in Deutschland oder in den USA sicherer seien.

Eine weitere Frage stellt er **Thorsten Schröder**. Er wolle wissen, ob zum Beispiel der Hackerparagraph, der den Einsatz von wichtigen Tool strafbar mache, in Deutschland ein Hinderungsgrund für Unternehmen sei, sich mit dem Thema zu beschäftigen oder Abwehrmaßnahmen zu ergreifen.

Andreas Könen sagt, es komme auf die Frage an, welche Daten mit welchem Schutzbedarf unter welchen Angriffen betrachtet würden. Es sei definitiv so, dass sich die Bundesverwaltung nach wie vor gewisser Spionageangriffe erwehren müsse. Die Angriffszahlen seien bekannt. Diese lägen, insbesondere bei personalisierten Angriffen auf bestimmte Mitarbeiter der Bundesverwaltung, bei ungefähr fünf pro Tag. Damit müsse sich das BSI auseinandersetzen. Allerdings sei der Datenabfluss, der registriert werde, extrem niedrig. Dies weise darauf hin, dass die Maßnahmen, die das BSI ergreife, im Wesentlichen ausreichend seien. Das BSI müsse aber sensibilisiert bleiben, um neue Angriffsmuster zu detektieren und sich auf neue Schemata einzurichten, damit es präventiv tätig werden könne.

Thorsten Schröder erläutert, dass die Unternehmen indirekt von § 202 c StGB betroffen seien. Sie könnten es sich in der Regel nicht leisten eigene Sicherheitsforscher zu beschäftigen, die den ganzen Tag nichts anderes täten, als an potenziellen Schwachstellen zu arbeiten. Die Unternehmen, die in dieser Branche tätig seien oder die interne Infrastrukturen absicherten, seien auf die veröffentlichten Ergebnisse von freien Sicherheitsforschern angewiesen. Sofern diese ihre Ergebnisse

nicht mehr publizierten, könne sich auch niemand öffentlich informieren. Dies bedeutete im Endeffekt, dass die Unternehmen diese Arbeit durchführen müssten.

Der **Vorsitzende** dankt **Andreas Könen** und **Thorsten Schröder** für ihre Ausführungen und übergibt das Wort an **SV Prof. Dr. Hubertus Gersdorf**.

SV Prof. Dr. Hubertus Gersdorf stellt zwei Fragen an **Prof. Dr. Dirk Heckmann.** Die erste Frage betreffe das abgestufte IT-Sicherheitskonzept. Er stimme uneingeschränkt zu, dass der Staat verpflichtet sei, für ein hinreichendes Maß an IT-Sicherheit Sorge zu tragen. Dies betreffe den Gesetzgeber, aber es betreffe auch die Administration. Doch was bedeute dies? **Prof. Dr. Dirk Heckmann** habe die Kategorien des abgestuften Sicherheitskonzepts genannt. Ihn interessiere, nach welchen Kriterien er die einzelnen Sicherheitsstandardstufen bestimmen wolle. Er führt eine These an, die im Zusammenhang mit Datenschutz formuliert worden sei. Diese laute, dass alle Daten, die der Öffentlichkeit Preis gegeben worden seien, prinzipiell nicht mehr schutzwürdig seien. Zur Öffentlichkeit gehöre auch die Teilöffentlichkeit, soweit es sich um einen unbegrenzten, personell nicht näher bestimmbaren Kreis handle. Er wolle wissen, ob **Prof. Dr. Dirk Heckmann** dieser These zustimme und sie in eine Kategorie eingeordnet werden könne.

Die zweite Frage betreffe das Spannungsfeld zwischen Anonymität und Zurechenbarkeit. Er wolle es so ausdrücken, dass das Spannungsfeld eines sei, welches den hinreichenden Rechtsgüterausgleich zum Gegenstand habe. **Prof. Dr. Dirk Heckmann** habe sicherlich zu Recht darauf hingewiesen, dass es zunächst ein Recht auf Anonymität gebe. Die Freiheit des Einen ende jedoch dort, wo die Freiheit des Anderen beginne. Folglich stelle sich die Frage, ob und inwieweit auch berechtigte Interessen Dritter oder der Allgemeinheit durch das anonyme Sichentfalten im Internet beeinträchtigt seien. Es gebe eine solche Auflösung schon in der Rechtsordnung, soweit es um Medien gehe. Die Medien unterlägen seit jeher einer Impressumspflicht. Da gebe es kein Recht auf Anonymität. Er frage sich, was dies für Jedermann-Medien bedeute. Sei nicht jeder, der im Internet tätig sei, zugleich ein Medium? Müsse er sich daher nicht auch den Rationalitäten der Medien unter-

werfen? Diese Fragen müssten beantwortet werden. Selbst wenn man nicht so weit gehe, zu klären, wie man im Internet, in einer Atmosphäre und Kultur der Anonymität, den notwendigen Betroffenenschutz sicherstellen könne. Man wisse seit jeher, dass die Freiheitsentfaltung des Einen auch zur Verletzung von Rechten Dritter führen könne. Die Frage sei, wie die Rechte des Dritten nun wirksam geschützt werden könnten. Bislang habe dafür das Merkmal der Zurechenbarkeit gedient. Ihn interessiere, wie man im Internet überhaupt einen wirksamen Betroffenenschutz sicherstellen könne, wenn man für Anonymität plädiere. Er frage sich, wie die Rechtsordnung hierauf reagieren könne. Er habe ein großes Verständnis für das Recht auf Anonymität, aber er sehe als Jurist, der der Güterabwägung verpflichtet sei, auch die Rechte der Betroffenen.

Prof. Dr. Dirk Heckmann pflichtet **SV Prof. Dr. Hubertus Gersdorf** bei, dass dies die ganz entscheidenden Fragen seien, die auch viele Juristen umtrieben. Er habe auch keine endgültige Antwort, wolle aber Hinweise aus seiner Forschung mitteilen.

Zunächst wendet er sich der Frage zu, welches die Kriterien der Abstufung seien. Er habe die Abstufung deshalb vorgenommen, weil man zwar natürlich von der Schutzpflicht des Staates ausgehen könne, aber auch konzedieren müsse, dass der Staat dies alles gar nicht leisten könne – sowohl teilweise aus organisatorischen, technischen und finanziellen Gründen als auch aus Kapazitätsgründen nicht. In der Diskussion seien bereits viele Beispiele genannt worden, bei denen es auch in der Wirtschaft keine Lösung gebe. Warum also solle der Staat dies können? Doch selbst wenn der Staat hier handle, sehe er sich bei all seinen IT-Sicherheitsbemühungen neuen Spannungsfeldern gegenüber gestellt. Der Staat müsse berücksichtigen, dass er neue Gefährdungstatbestände schaffe, wenn er an anderer Stelle regulierend eingreife.

Ein Instrument wie die Onlinedurchsuchung etwa, könne natürlich sicherheitsförderlich sein, weil man ein bestimmtes Kriminalitätsfeld angehen könne. Andererseits schaffe man damit ein Instrument, welches aus rechtlichen Gründen wiederrum problematisch sein könne. Entscheidungen des Bundesverfassungsgerichts hin-

sichtlich der Grenzen solcher sehr intensiven staatlichen Eingriffe müssten berücksichtigt werden. Zudem gebe es auch rein tatsächliche Problem, wie die aktuelle Trojaner-Diskussion zeige. Es könnten auch rein faktisch neue Schwachstellen geschaffen werden, so dass der Staat durch den Einsatz solcher Instrumente sogar selbst die IT-Sicherheit schwäche.

Prof. Dr. Dirk Heckmann betont, dass er auf der einen Seite zwischen dem Schutz kritischer Infrastrukturen unterscheide, der auf Grund eines überragenden Allgemeinwohlinteresses sehr hoch angesehen werden müsse. Die Gesellschaft sei auf diese kritischen Infrastrukturen angewiesen, weshalb konsensual sei, dass Bemühungen finanzieller, rechtlicher und technischer Art sehr sinnvoll seien. Auf der anderen Seite gebe es bei dem weiten Begriff der IT-Sicherheit auch viele Sachverhalte, die der Selbstregulierung überlassen werden könnten. Es gehe dort um Rechtsgüter, die zwar für den Einzelnen wichtig sein mögen, aber in der Abschichtung nicht weit oben gesiedelt werden müssten. Entweder könnte sich der Einzelne um seine eigene sichere Umgebung bemühen oder aber ein intermediärer IT-Dienstleister könne dies übernehmen. Dies sei der Aspekt der Abschichtung nach der Bedeutung des gefährdeten Gutes. Innerhalb dessen könne man weiter hinsichtlich der Bedeutung der Daten unterscheiden. In der aktuellen Datenschutz-Diskussion sei von den Anwälten Schneider und Härting über die Deutsche Gesellschaft für Recht und Informatik e. V. (DGRI) ein Reformmodell vorgestellt worden, welches sich von der Aussage des Bundesverfassungsgerichtes, dass es keine belanglosen Daten gebe, lösen wolle. Laut der Darstellung dieser Anwälte gebe es sehr wohl belanglose Daten – man brauche nur ins Internet zu schauen. Er formuliere absichtlich überspitzt, dass dort der Datenschutz wirksamer gestaltet werden solle. Dies sei ein weiterer Aspekt der Abstufung.

Eine weitere Überlegung sei, nicht sofort Gesetze zu erlassen, sondern eine Strategie für IT-Sicherheit zu entwickeln. Diese solle im Rahmen der Öffentlichkeitsarbeit bekannt gemacht werden. Es solle aufgezeigt werden, dass IT-Sicherheit wichtig sei und der Staat dies quasi zur Chefsache erklärt habe. Es seien staatliche Ziele zu entwickeln; Wirtschaft und Gesellschaft seien einzubinden. Diese Möglichkeiten

der Abstufung habe er auch in seiner Stellungnahme angeführt. IT-Sicherheit könne nicht staatlich mittels Gesetzt, Verbot oder Zwangsmaßnahme verordnet werden. Die Akzeptanz der Beteiligten sei wichtig, da im IT-Sicherheitsrecht außerordentlich hohe Anforderungen gestellt würden. Eine weitere Frage bezog sich auf die These, dass Daten, die an die Öffentlichkeit gelangt seien, nicht mehr schutzwürdig seien. Entscheidend sei, an welcher Stelle der Schutz gesiedelt werden solle. Gehe es um die Vertraulichkeit und die Daten seien bereits öffentlich zugänglich, so liefe der Schutz ins Leere. Die Frage sei, wie mit Teilöffentlichkeiten, beispielsweise den tausend Freunden bei Facebook, umzugehen sei. Dort sei es Ausdruck der informationellen Selbstbestimmung des Nutzers, selbst zu entscheiden, welche Daten er welchem Personenkreis zur Verfügung stelle. Dies bedeute nicht, dass der Nutzer in eine Veröffentlichung über diesen Kreis hinaus einwilligen müsse, wenngleich die Gefährdung, dass die Daten an Dritte gelangten, so groß sei, dass der Schutz nahezu gegen Null tendiere. Es stelle sich auch die Frage, was mit diesen Daten darüber hinaus geschehe. Es gehe nicht um die Kenntnis als solche im Rahmen der Vertraulichkeit, sondern um die Integrität dieser Daten in einem anderen Kontext. Er empfinde die angesprochene These als zu weitgehend.

Zum Spannungsverhältnis Anonymität und Zurechenbarkeit wolle er nur einige Punkte nennen. Die Impressumspflicht der Medien sei natürlich ein beliebtes Argument in Bezug auf Blogger. Bei diesen möge es durchaus noch zutreffend sein, soweit sie auch tatsächlich meinungsbildend als Medium aufträten. Bei jedem Einzelnen bezweifle er dies jedoch. Ein Klarnamenzwang beispielsweise in Bewertungsportalen mit dem Argument einzuführen, dass man zur Meinung beitrage, würde das Recht des Beitragenden sozusagen umkehren. **Prof. Dr. Dirk Heckmann** sagt, er sehe den Einzelnen nicht als Medium wie Presse oder Rundfunk an – auch, weil er nicht deren Reichweite habe. Sicherlich könne es auch eine Onlinezeitung geben, die nur von einer Person betrieben werde, aber man könne nicht sagen, dass jeder, der sich im Internet äußere, einer Impressumspflicht unterliege. Dies ginge aus seiner Sicht zu weit.

Die angesprochene Kultur der Anonymität berge sicherlich ein Gefährdungspotenzial. Umgekehrt sei auch eine Kultur des Klarnamenzwangs, also die jederzeitige Zurechenbarkeit problematisch. Auch dies führe zur Verletzung von Rechten, beispielsweise wenn man in einem Ärztebewertungsportal einen Arzt bewerten wolle, ohne die eigene Krankheitsgeschichte offenlegen zu wollen. Aus seiner Sicht sei diese Pauschalität nicht haltbar. Eine Lösung sei wahrscheinlich zwischen diesen beiden Positionen zu finden. Auch das Grundrecht auf Anonymität sei nicht unbeschränkt. Hier seien Schranken bei den Rechten Dritter zu ziehen. Die Frage sei jedoch, wo diese Rechte Dritter begönnen. Man müsse schauen, wie beispielsweise bei einem Straftatbestand eine Zurechenbarkeit ermöglicht werden könne. Man müsse beiden Seiten gerecht werden, vielleicht mit technischen Mitteln oder im Rahmen eines technischen Rechtsschutzes. Er wolle keiner dieser beiden Positionen den absoluten Vorrang einräumen.

Der **Vorsitzende** dankt **Prof. Dr. Dirk Heckmann** für seine Ausführungen und übergibt das Wort an **SV Dr. Bernhard Rohleder**.

SV Dr. Bernhard Rohleder richtet seine erste Frage an **Thorsten Schröder**. Er komme auf die Feststellung zurück, dass die IT-Sicherheitsanbieter die vertraglichen Verhältnisse mit ihren Kunden weitgehend frei gestalten könnten und auch nicht in der Haftung seien. Bei IT-Sicherheitsanbietern handle es sich um einen stark mittelständisch geprägten Markt mit vielen kleinen mittelständischen Häusern mit vielleicht 50 bis 300 Mitarbeitern. Oftmals hätten diese ein deutsches Mutterhaus. Diese Unternehmen verkauften zum großen Teil in den öffentlichen Bereich, da gälten die Ergänzenden Vertragsbedingungen für die Beschaffung von Informationstechnik (EVB-IT) und es seien eindeutige Haftungsregelungen vorgesehen. Des Weiteren verkauften sie an große industrielle Anwender, die im gewerblichen IT-Bereich für etwa 70 Prozent der Nachfrage stünden. Dies seien die hundert größten gewerblichen IT-Kunden. Diese diktierten die Auftragsbedingungen und ein mittelständisches Softwarehaus habe dort hinsichtlich der Haftungsbedingungen kein Mitspracherecht. Es bestehe nur die Wahl, den Auftrag abzulehnen. Auch im Privatkundenbereich gebe es eine gesetzliche Regelung. Er wolle daher wissen, worauf seine

Einschätzung basiere, dass sich dies so anders verhalte, als er es tagtäglich von den Firmen mitgeteilt bekomme.

Die zweite Frage bezieht sich auf den angesprochenen Technologiebezug aus dem internationalen Raum. Er wendet sich an **Andreas Könen**. Es sei bereits eine Art IT-Sicherheits-TÜV angesprochen worden. Das BSI führe etwas Ähnliches für den öffentlichen Bereich durch. Dies habe zur Folge, dass es nur zwei lizensierte Anbietern für die unterste Vertrauensstufe gebe – der dritte Anbieter NCP habe vor kurzem seine Lizenz verloren. Die Möglichkeit einen Technologielieferanten für den öffentlichen Bereich auszuwählen sei folglich sehr beschränkt. Seine Frage beziehe sich auf den Umstand, dass das BSI eigentlich nicht in der Lage sei die komplexen Technologien, die in den Netzen als auch beim Privatkunden eingesetzt würden, derart weitgehend zu verstehen und zu durchdringen, dass es überhaupt eine wirklich valide Einschätzung treffen könne. Er wolle wissen, ob diese Einschätzung zutreffend sei und was dagegen unternommen werden könne.

Andreas Könen erläutert, dass das BSI einen IT-Sicherheits-TÜV auf drei Wegen durchführe. Erstens lasse das BSI Informationssicherheitsprodukte für den Geheimschutzbereich, das heiße für den Einsatz zur Wahrung der Vertraulichkeit von VS-NfD (Verschlusssache – Nur für den Dienstgebrauch) oder höher eingestuften Dokumenten, zu. In diesem Bereich der vertrauenswürdigen Übermittlung von Daten zwischen Mobilgeräten und Servern existierten drei Produkte. Für das von **SV Dr. Bernhard Rohleder** erwähnte Produkt habe es niemals eine echte Zulassung gegeben, sondern eine zeitlich beschränkte Einsatzempfehlung. Diese habe das BSI auf Grund neuer Erkenntnisse zur Informationssicherheit zurückziehen bzw. auslaufen lassen müssen.

Weiter gebe es den Bereich der Zertifizierungen nach § 9 BSI-Gesetz, also die Zertifizierung von IT-Sicherheitshardware oder –software nach den Common Criteria. Hier würden insbesondere Sicherheitskomponenten, wie Chips und Kartenleser, zertifiziert. Diese benötige man im Umfeld der Großprojekte. Sie müssten nach technischen Richtlinien jeweils eine solche Zertifizierung besitzen. In diesem Be-

reich arbeite das BSI sei Jahren mit Dienstleistern wie TÜViT oder T-Systems zusammen, die als akkreditierte Sicherheitsdienstleister Kompetenzen aufbauten. Das BSI könne diese aus Kapazitätsgründen nicht vorhalten.
Seit der Novellierung des BSI-Gesetzes im Jahre 2009 gebe es noch einen dritten Weg. Dies seien die Mindeststandards nach § 8 BSI-Gesetz. Diese Mindeststandards nach § 8 BSI-Gesetz bedeuteten, dass das BSI für den Einsatz unterhalb des Verschlussdatenbereiches in der Bundesverwaltung Kriterien für bestimmte Produktsektoren festzulegen habe, nach denen in europaweit stattzufindenden Ausschreibungen Produkte beurteilt würden. Dazu definiere man in den Ausschreibungen eindeutige Kriterienkataloge.

Dies sei sozusagen das Komplement zu den andere Zertifizierungswege. Auch dort bediene sich das BSI externer Gutachter und Analyselabore um letztlich die Sicherheit einschätzen zu können. Es sei also vollkommen korrekt, dass das BSI nicht alle Kompetenzen im Hause habe. Der Prozess werde aber so gesteuert, dass das BSI das Wissen einkaufe und dezidiert an den Stellen anbringe, an denen es benötigt werde.

Thorsten Schröder räumt ein, dass es auch Beispiele gebe, bei denen es mit der Haftung auch gut funktioniere. Als Berater weise er größere Firmen auch darauf hin, dass sie bei ihren Zulieferern eindeutige Vorgaben hinsichtlich der Haftungsbedingungen und ABGs machen müssten. Er selbst sei auch schon in der Situation gewesen, ABGs ablehnen zu müssen, die er nicht habe beeinflussen können.
Er wolle nicht ausschließen, dass die Auftraggeber heutzutage bei kritischen Infrastrukturen darauf achteten. In der Praxis höre man jedoch häufig von Softwarekomponenten und Komponenten irgendwelcher Infrastrukturen, die von den Systemadministratoren nicht verändert werden dürften, da anderenfalls die Gewährleistung ausgeschlossen werde. Er glaube, dass die Betreiber von kritischen Infrastrukturen, die von einem Zulieferer Softwarekomponenten einkauften, die Macht hätten auf die vertraglichen Grundlagen dieses Softwareproduktes hinsichtlich der Haftung einzuwirken. Die Frage beziehe sich auf seine Kritik, dass viele Hersteller oder Diensteanbieter per ABG sämtliche Haftung von sich wiesen. Aus seiner Sicht sei

dies für den Enduserbereich noch immer so. In der Industrie ändere sich dies, da Berater konkrete Vorschläge zu Service Level Agreements und Security Level Agreements machten.

SV Dr. Bernhard Rohleder fasst nach, ob **Thorsten Schröder** seine zuvor geäußerte Kritik mit der getroffenen Aussage relativiere.

Thorsten Schröder erwidert, das er dies möglicherweise tue. Er bleibe jedoch bei der Aussage, dass sich für den Endbenutzer, der um seine Privatsphäre bange und primär von Sicherheitsschwankungen betroffen sei, nicht sonderlich viel ändere.

Der **Vorsitzende** dankt den Anhörpersonen, den Mitgliedern der Projektgruppe sowie der interessierten Öffentlichkeit. Er ruft abschließend den Tagesordnungspunkt „Verschiedenes“ auf.

TOP 2 Verschiedenes

Der Vorsitzende erinnert die Mitglieder der Projektgruppe an den bevorstehenden Abgabetermin der Dokumente am 5. Dezember 2011. Da es keine weiteren Wortmeldungen gibt, schließt der Vorsitzende die Sitzung um 18.45 Uhr.