Berliner Gespräch

„Cyber-Security – Neue Services im Spannungsfeld zwischen Regulierung und Selbstverantwortung“

13. Oktober 2016, 17:00-22:00 Uhr

EIT ICT Labs Germany GmbH/EIT Digital Germany ,
Ernst-Reuter-Platz 7, 10587 Berlin

Im Internet der Dinge führen und steuern Maschinen den Menschen anhand einer Vielzahl erhobener Daten und eigenständig getroffener Entscheidungen. Beispiele finden sich in Applikationen wie autonomes Fahren, eHealth, eShopping, Smart Home und Robotik. Hier verliert der Mensch zunehmend die Kontrolle über sein Handeln.
Zusätzlich kann der Mensch nicht mehr kontrollieren, welche personenspezifischen Daten erzeugt werden. Daraus ergeben sich zwei Fragen: Wie kann der Mensch die Selbstbestimmung über sein Handeln und wie die Kontrolle über seine erzeugten Daten behalten?
In einem Kreis von maximal 100 Teilnehmern (Politik, Wirtschaft, Wissenschaft) wollen wir in kurzen Keynotes und Impulsvorträgen (Politik, Anbieter, Anwender, F&E) folgende Aspekte behandeln:
- Welche Anforderungen stellt dies an die staatliche Regulierung?
- Welche Folgen hat dies für die Wirtschaft?
- Welche Technologien für Lösungen kann die Forschung bieten?

Begrüßung und Einführung
Prof. Dr. Claudia Eckert, Fraunhofer-Institut AIESEC, München und TU München

Prof. Eckert:

Meine Damen und Herren, ich begrüße Sie recht herzlich zum heutigen Berliner Gespräch im Namen des MÜNCHNER KREISES. Herr Prof. Dowling lässt sich entschuldigen. Er wäre gern hier gewesen, hat aber andere Verpflichtungen. Wir freuen uns sehr, dass Sie gekommen sind mit uns das spannende Thema „Cyber- Sicherheit – neue Services im Zwiespalt, im Gerangel sozusagen, zwischen Regulierung und Selbstbestimmtheit zu diskutieren mit unseren Keynote Gästen, mit unseren Pannelisten und natürlich mit Ihnen allen, dass wir hier – das wäre mein Wunsch – zu einer regen Diskussion kommen.

Wir starten mit ein paar Worten zum Werdegang dieses Berliner Gesprächs. Das ist herausgekommen aus Aktivitäten eines neu gegründeten Arbeitskreises „Cyber-Sicherheit“ des MÜNCHNER KREISES und hier haben sich verschiedenste Vertreter aus Industrie, Wissenschaft und auch Verbänden zusammengetan, um zu diskutieren, was Handlungsempfehlungen sein könnten, die wir für die Politik erarbeiten wollen, Technologietrends beobachten und darüber zu informieren, mit den Fachleuten zu sprechen

und drittens den gesellschaftlichen Diskurs voranzubringen. Aus diesen Aktivitäten sind der heutige Tag und das heutige Programm entstanden.

Bevor wir beginnen, möchte ich an dieser Stelle Dank sagen zu allen denjenigen, die das im Hintergrund vorbereitet haben. Das ist zum einen Herr Prof. Helmbrecht, der das auch inhaltlich mit vorbereitet hat und mein Kollege Prof. Georg Siegel, die einfach diese Themen im Vorfeld aufbereitet haben. Ich möchte auch meinem Kollegen Herrn Prof. Thielmann danken, der unermüdlich dabei ist, die Dinge voranzutreiben, zu managen. Und last but not least möchte ich Herrn Bub danken, dass wir hier in seinen heiligen Hallen zu Gast sein dürfen. Und ich bin sicher, dass wir uns alle hier sehr wohl fühlen werden.
Wir haben uns mit dem Thema schon einmal in Arbeitsgruppen auseinandergesetzt und wollen das heute vertiefen. Ich freue mich sehr auf unsere ersten drei Keynotes. Wir beginnen mit Klaus Vitt, Staatssekretär des Bundesministeriums des Inneren, CIO des Bundes. Wir freuen uns, Ihre Sicht auf dieses Spannungsfeld Cyber-Sicherheit zwischen Regulierung und Selbstbestimmtheit zu hören. Herr Vitt, bitte !

Keynotes
Prof. Dr. Udo Helmbrecht, ENISA, Heraklion, Griechenland
Arne Schönbohm, Bundesamt für Sicherheit in der Informationstechnik, Bonn
Staatssekretär Klaus Vitt, Bundesministerium des Inneren, Berlin

Staatssekretär Vitt:
Vielen Dank. Ich bin gespannt, ob ich diesem Anspruch, den Sie gerade formuliert haben, auch gerecht werden kann. Ich bedanke mich erst einmal recht herzlich für die Einladung. Wir, das Bundesinnenministerium, haben dem Thema Cyber-Sicherheit von Anfang an eine hohe Priorität eingeräumt und hier auch einen politischen Schwerpunkt gesetzt. Das werden Sie gleich an meinen Ausführungen sehen. Bei der Frage, wieviel Regulierung und wieviel Selbstverantwortung für die Gewährleistung von Cyber-Sicherheit erforderlich sind, haben wir mit dem kompatiblen Ansatz, auf den ich gleich etwas näher eingehen, mit dem Sicherheitsgesetz einen neuen Weg eingeschlagen, den wir auch zukünftig weiter ausbauen werden. Ich werde noch einen kleinen Ausblick geben, was wir uns da alles vorstellen können.

Es hat einen Grund: wir glauben, dass wir die Herausforderungen, die auf uns zukommen, nicht allein meistern können, sondern wir müssen unsere Kompetenzen bündeln und immer mehr und immer engere Kooperationen eingehen. Bevor ich das mache, würde ich gern noch

ein wenig auf die Digitalisierung eingehen, weil die Digitalisierung erhebliche Auswirkungen auf die Cyber-Sicherheit hat. Denn je mehr wir digitalisieren, werden wir sehen, werden wir eine höhere Abhängigkeit von der IT bekommen, und damit werden wir anfälliger. Die Digitalisierung betrifft alle Bereiche der Wirtschaft, der Gesellschaft und des Staates. Wir verändern mit ihr die Prozesse und die Abläufe in all diesen Bereichen. Hinzu kommt damit eine weitgehende Vernetzung weiterer Bereiche. Das ist sowohl bei den Unternehmen, aber auch im privaten Umfeld – Sie wissen, wie abhängig man vom Smartphone oder anderen IT mäßigen Unterstützungen wird.

Wenn wir die Freiräume und die Potenziale betrachten – ich nenne das einmal die Chancen –, dann haben wir auf der einen Seite die Chancen aber auf der anderen Seite auch Risiken. Darauf möchte ich gern kurz eingehen, denn wir haben eine zunehmende Abhängigkeit von IT gestützten Systemen und Prozessen. Damit bekommt die Verfügbarkeit und die Sicherheit der IT-Systeme eine immer höheren Bedeutung. Wir nennen das ein bisschen anders. Es ist bereits jetzt absehbar, dass die digitale Verwundbarkeit in allen Bereichen unseres Lebens und Handelns zunehmen wird. In den kommenden Jahren wird sich das zu einer der zentralen Herausforderungen unserer Gesellschaft entwickeln.

Zu den Kernaufgaben, wenn man das wieder auf den Staat bezieht, gehört die Gewährleistung von Freiheit und Sicherheit, und das gilt auch für den Cyber-Raum. Für den Staat besteht daher die Pflicht, die laufenden Veränderungsprozesse aktiv zu begleiten auf der einen Seite. Wir müssen aber die Rahmenbedingungen so gestalten, dass unsere Werte und Rechte auch in der digitalisierten Welt beachtet werden.
Der letzte Bericht des BSI zur Lage der IT-Sicherheit hat eindeutig gezeigt, dass die Anzahl der Schwachstellen und die Verwundbarkeiten in IT-Systemen nach wie vor auf einem sehr hohen Niveau liegen. Einige dieser Schwachstellen offenbaren schwerwiegende Sicherheitslücken. Das eine oder andere haben wir in der jüngsten Presse lesen können. Das bedeutet, dass der Schutz der IT-Systeme durch die Anwender häufig mit den hoch entwickelten Werkzeugen zur Ausnutzung von solchen Sicherheitslücken nicht immer Schritt halten kann. Auch der aktuelle Lagebericht, der gerade vom BSI vorbereitet und demnächst veröffentlicht wird, wird dies noch einmal bestätigen. Gravierend hat sich das nicht verändert.
Was wollen wir erreichen? Wir wollen Deutschland digitalisieren, aber die damit verbundenen Risiken deutlich minimieren. Einen wesentlichen Beitrag hierzu leistet das IT-Sicherheitsgesetz, das letztes Jahr im Juli verabschiedet wurde. Es folgt der grundsätzlichen

Überzeugung, dass Cyber-Sicherheit nur in einer sicheren Umgebung entsteht. Oder anders gesagt, der Cyberraum ist nur so sicher, wie es die dort angeschlossenen Systeme und Infrastrukturen sind.

Mit dem IT-Sicherheitsgesetz wurde in Deutschland ein Mindeststandard für die IT-Sicherheit bei den Betreibern von kritischen Infrastrukturen eingeführt. Wenn man die betrachtet, sind diese kritischen Infrastrukturen für das Wohl unserer Gesellschaft von enormer Bedeutung Adressaten und Unternehmer aus den unterschiedlichsten Bereichen sind für die Bereiche Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie aus dem Finanz- und Versicherungswesen. Das IT-Sicherheitsniveau in diesem Bereich ist allerdings sehr unterschiedlich. Sie kennen die Vorfälle, die in diesem Jahr bei den Krankenhäusern passiert sind. Das war ein deutliches Beispiel für solche Situationen. Wenn man dann noch Ausfälle der IT-Systeme in dieser kritischen Infrastruktur betrachten, können die weitreichende teilweise dramatische Folgen für unsere Gesellschaft haben.

Es leuchtet daher unmittelbar ein, dass hier eine höhere Anforderung an IT-Sicherheit gelten muss im Vergleich zu anderen Bereichen oder zu dem normalen privaten Umfeld. Auf freiwilliger Basis – und das ist das, was hier in der Vergangenheit versucht wurde – bestehende Angebote und Initiativen in Anspruch zu nehmen, reicht hier nicht mehr aus. Dafür ist die Bedrohungslage zu kritisch. Das heißt aber nicht, dass der Kooperationsgedanke beim IT-Sicherheitsgesetz keine Rolle gespielt hat. Im Gegenteil, die Expertise der Wirtschaft ist bei den Arbeiten an der Anfang Mai in Kraft getretenen Rechtsverordnung zur Bestimmung kritischer Infrastrukturen umfassend berücksichtig worden. Betreiber kritischer Infrastrukturen sollen anhand von messbaren und nachvollziehbaren Kriterien überprüfen können, ob sie in diesen Regelungsbereich des IT-Sicherheitsgesetzes fallen oder nicht. Damit wir Bedrohungen im Cyberraum frühzeitig erkennen und wirksam Vorsorge und Gegenmaßnahmen erkennen können, brauchen wir ein umfassendes Bild über die Gefahrensituation. Mit dem IT-Sicherheitsgesetz wurde deshalb für die Betreiber der kritischen Infrastrukturen die Meldepflicht für kritische IT-Sicherheitsvorfälle eingeführt. Dem Bedürfnis der Unternehmen nach einem größtmöglichen Schutz ihrer Interessen wurde dabei soweit wie irgend möglich Rechnung getragen. So sollen die entsprechenden Meldungen an das BSI auch möglich sein und zwar ohne namentliche Nennung des Unternehmens, aber nur dann, wenn es nicht zu einem gravierenden Ausfall oder einer

gravierenden Beeinträchtigung der kritischen Infrastrukturen gekommen ist. Um den Aufwand bei den betroffenen Unternehmen möglichst gering zu halten, ist außerdem geplant, dass bereits etablierte Meldewege oder Meldeverfahren so weit wie möglich erhalten bleiben. Diesen kooperativen Ansatz möchten wir auch auf andere Bereiche, andere Wirtschaftsbereiche, andere Unternehmensbereiche übertragen. Die größte Herausforderung wird dabei der Mittelstand sein. Rein quantitativ wird es eine Herausforderung sein. Das eine ist sozusagen die Menge und das andere ist die Qualität, d.h. wie hoch die IT-Sicherheit bei den Mittelständlern ist. Wenn die in Richtung Digitalisierung gehen, kann das eine richtige Herausforderung werden. Da müssen uns Konzepte und Wege einfallen. Wir werden so etwas Ähnliches machen wie das IT-Sicherheitsgesetz. Ob wir es gesetzlich regeln, wissen wir noch nicht. Wir werden aber sozusagen Punkte haben müssen, wo Meldungen verdichtet werden, weil das BSI ansonsten von der Anzahl der Meldungen erschlagen würde. Das werden wir nicht machen können. Das war das Thema kooperativer Ansatz bezogen auf das IT-Sicherheitsgesetz.

Wie geht es weiter? Wir würden natürlich ein ähnliches Konstrukt auf die Zusammenarbeit zwischen Bund und Ländern übertragen – da sind wir gerade dabei und haben heute Planungsphasensitzung, wo wir das formal beschlossen haben, wo wir jetzt einheitliche Meldewege etablieren werden.

Ich möchte noch auf ein weiteres Thema eingehen, was uns im Zusammenhang mit der IT-Sicherheit intensiv beschäftigen wird. Das ist der Datenschutz. Mit der ab Mai 2018 anwendbaren EU-Datenschutzgrundverordnung werden die Aspekte des technologischen Datenschutzes deutlich ausgeweitet und gestärkt. Außerdem bietet die EU-Datenschutzgrundverordnung die einmalige Möglichkeit, ein einheitliches Datenschutzniveau in Europa zu etablieren. Das würde für die Unternehmen eine deutliche Verbesserung und auch eine deutliche Erleichterung sein. Natürlich kommt auch dazu, dass bei Verstößen Strafen prozentual vom Umsatz verhängt werden können, was natürlich eine richtige Dimension sein kann. Nehmen wir an, dass uns das nicht gelingt, dann kann folgendes passieren bei digitalen Dienstleistungen, dass sie lange spezifisch geprägt werden müssen. Bei Grenzübertritt gelten auf einmal andere Regelungen und das müsste berücksichtigt werden, was ungemein kompliziert ist.

IT-Sicherheit ist ein zentraler Bestandteil der Gewährleistung des Datenschutzes. Man kann auch sagen, es gibt keinen effektiven Datenschutz ohne IT-Sicherheit. Um auf Augenhöhe mit den Angreifern agieren und Angriffe erfolgreich abwehren zu können, benötigt man heutzutage Echtzeitdaten und sichere Analysemöglichkeiten zur Missbrauchsbekämpfung. Gerade an dieser Stelle jedoch bewegen wir uns mit Mastern zur Gewährleistung der IT-Sicherheit teilweise an datenschutzrechtlichen Gründen. Ich würde dafür ein Beispiel machen. Um Schutzlücken zu erkennen und Angriffe abzuwehren, müssen z.B. Telemedien Anbieter, die bei ihren Diensten anfallenden Daten über einen gewissen Zeitraum für einen ganz konkreten Zweck vorhalten, also speichern. Kritiker sagen, dass das so nicht geht, weil die Speicherung durch den Anbieter ohne einen konkreten Anlass erfolgt. Was wird das bedeuten? Solange es noch nicht zu einem erfolgreichen Angriff auf den Server gekommen ist, dürften diese Daten also nicht gespeichert werden. Die Frage, die wir uns stellen, lautet: kann es richtig sein, dass der Anbieter eines Telemediendienstes erst dann tätig werden darf, wenn seine Systeme bereits erfolgreich kompromittiert wurden? Schadet ein solches Datenschutzverständnis nicht am Ende sogar dem Schutz der Daten? Wir sehen, dass Datenschutz und IT-Sicherheit ein gemeinsames Ziel haben, nämlich die Bürger, die Wirtschaft und die Behörden vor einem unbefugten Eindringen in Systeme und einen Missbrauch von Daten zu schützen. Wir werden uns aus diesem Grund dafür einsetzen, dass künftig mehr Daten gespeichert und ausgewertet werden dürfen, um einen Cyberangriff frühzeitig zu erkennen und abwehren zu können. Wir werden aber auch dafür sorgen, dass diese Daten allein nur zu diesem Zweck verwendet werden dürfen und nicht für andere Interessen des Betreibers oder Dritter.

Auch auf europäischer Ebene tut sich sehr viel. Die Rechtssetzung schreitet voran. Ende letzten Jahres haben das europäische Parlament und der Rat der europäischen Union ihre Verhandlungen zu einer Richtlinie zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, kurz: die NIST-Richtlinie, abgeschlossen. Die NIST-Richtlinie ist im August d.J. in Kraft getreten. Derzeit laufen bei uns die Arbeiten zur Umsetzung der NIST-Richtlinien. Was sind so die wesentlichen Elemente und Aufgaben, die da zu erfüllen sind? Das sind drei Stück. Der erste Part ist der EU-weite Aufbau nationaler Kapazitäten für Cyber-Sicherheit, der zweite Part ist eine stärkere Zusammenarbeit der der Mitgliedsstaaten. Und der dritte Part wird Ihnen bekannt vorkommen; Mindestanforderung an IT-Sicherheit und Meldepflichten bei erheblichen und gravierenden IT-Sicherheitsvorfällen. Also, vergleichbar zu unserem IT-Sicherheitsgesetz.

Sie sehen, dass wir als Bundesregierung uns aktiv in diese Verhandlungen eingebracht haben und erfolgreich entsprechende Ideen dort platzieren haben können. Die Annahme der NIST-Richtlinie ist ein entscheidender Schritt für mehr Cyber-Sicherheit in Europa und ein zentraler Baustein in der gemeinsamen Cyber-Sicherheitsarchitektur. Ich gehe noch kurz auf unsere Cyber-Sicherheitsstrategie ein, die aus dem Jahr 2011 stammt. Da wurde ein wesentlicher Grundstein für eine Vielzahl von Maßnahmen gelegt, die bereits heute einen signifikanten Beitrag zur Erhöhung der Cyber-Sicherheit geführt haben. Die dort verankerten strategischen Ziele werden über die digitale Agenda der Bundesrepublik entsprechend getrackt, gemonitort und weiter verfolgt.
Aufgrund der Situation, die ich eben geschildet habe, zunehmende Digitalisierung auf der einen Seite, Professionalisierung der Angreifer, war eine Überarbeitung der Cyber-Sicherheitsstrategie erforderlich geworden. Wir erarbeiten zurzeit die Cyber-Sicherheitsstrategie 2016. Diese Arbeiten sind weitgehend abgeschlossen. Die Abstimmung ist weitgehend abgeschlossen. Die Cyber-Sicherheitsstrategie wird dem Kabinett zur Entscheidung vorgelegt und danach kommuniziert.

Ich will nicht zu viel verraten, kann aber ein paar Elemente daraus darstellen. Es handelt sich um vier Handlungsfelder, auf die wir uns konzentrieren, die wir weiterentwickeln und weiter ausbauen. Das ist einmal sicheres und selbstbestimmtes Handeln. Das heißt, auch in einer digitalisierten Umgebung müssen wir sicheres und selbstbestimmtes Handeln ermöglichen und gewährleisten. Und das gilt für alle, für Bürger, für Unternehmen und für den Staat. Was dazu kommt, ist, dass es dabei auch um den Erhalt und die Steigerung der Beurteilungsfähigkeit zu Cyber-Bedrohung geht, was eine immer wichtigere Aufgabe wird.

Das zweite Element, IT-Sicherheit und Sicherheit im Cyberraum sind als gemeinsame Aufgabe und Auftrag von Staat und Wirtschaft zu verstehen. Hier brauchen wir mehr Kooperationen und intensivere Kooperationen. Erste Gespräche dazu laufen schon, z.B. mit der DCSO.

Dritter Punkt: wir benötigen eine noch leistungsfähigere gesamtstaatliche Cyber-Sicherheitsarchitektur. Das bedeutet nichts anderes, als wie welche Organisationen auf welcher rechtlichen Grundlage zusammenarbeiten. Organisation sind dabei die Ministerien untereinander. Organisationen sind sozusagen das Innenministerium mit der Wirtschaft, mit

den unterschiedlichen Unternehmen. Was wir dafür brauchen, ist eine rechtliche Grundlage. Denn die Frage ist, warum tauschen wir Informationen mit dem einen Unternehmen aus und mit dem anderen nicht? Dafür brauchen wir klare Kriterien. Das ist ein wesentliches Element. Vierter Punkt: wir müssen weiterhin eine aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik einnehmen.

Wie Sie sehen, meine Damen und Herren, werden die Digitalisierung und die Cyber-Sicherheit die großen Herausforderungen für die Zukunft sein. Nur gemeinsam werden wir diese Herausforderungen meistern können. Daher werden wir bestehenden Kooperationen weiter ausbauen und neue Kooperationen vereinbaren. Nur wenn wir unsere Kompetenzen bündeln, werden wir hier erfolgreich sein und die Herausforderungen der Zukunft meistern können. Bei all diesen Herausforderungen geht es immer auch um die optimale Balance – jetzt komme ich zu unserem Thema – zwischen Regulierung und Selbstverantwortung, dem Thema dieser Veranstaltung. Ich bedanke mich für die Aufmerksamkeit. Vielen Dank.

Prof. Eckert:
Ganz herzlichen Dank für die Ausführungen. Wir haben ein bisschen Zeit, Fragen aus dem Publikum entgegenzunehmen. Herr Vitt wird sie gern beantworten. Meinen Studenten sage ich immer, wenn ihr nicht fragt, frage ich. Vielleicht kann ich das Eis brechen mit der ersten Frage .Wir haben gerade nochmal abgeschlossen mit der Balance zwischen Regulierung, Selbstbestimmung und Selbstbestimmtheit. Was denken Sie denn, was die Menschen draußen denken? Oder frage ich anders herum. Es gibt die Studie, über die wir nachher noch etwas hören werden, wo über 70% der Befragten sagen, dass das unsicher ist und der Staat muss sich eigentlich …Sagen Sie, man muss selbstbestimmt sein. Und diese Leute sagen, dass sie das gar nicht wollen.

Staatsekretär Vitt:
Ich glaube, dass der Staat damit überfordert wäre, um das ganz einfach und ganz nüchtern zu betrachten. Das werden wir als Regierung nicht allein hinbekommen. Das andere Extrem ist die Freiwilligkeit. Da sehen wir, dass das auch nicht funktioniert. Das IT-Sicherheitsgesetz ist ein guter Kompromiss für die. Ich nenne das hier eine Win-Win-Situation, und will beschreiben, warum das so ist. Einmal Mindeststandards an IT-Sicherheit. Bei den Betreibern kritischer Infrastrukturen würde jeder sagen, dass das eine Selbstverständlichkeit ist. Bei den Krankenhäusern haben wir gesehen, dass es keine Selbstverständlichkeit ist. Da geht es um

Menschenleben, um das ganz konkret zu formulieren. Ich könnte noch andere Infrastrukturen nennen. Also, wenn man erkennt, ist diese Freiwilligkeit nicht ausreichend ist, dann ist es so, dass man gesetzliche Regelungen braucht.

Das zweite Thema ist die Meldepflicht. Da ist es so, dass das eine Win-Win-Situation ist. Wenn ein Betreiber einer kritischen Infrastruktur dem BSI einen kritischen Sicherheitsvorfall meldet, hat das BSI eine Verantwortung entgegenzunehmen, analysieren, bewerten und die anderen so schnell wie möglich zu informieren, damit die sich rechtzeitig schützen können. Diese Win-Win-Situation würde ich gern übertragen auf andere Unternehmen. Und Mittelstand, finde ich, ist die größte Herausforderung. Jetzt gehe ich auf die andere Seite, natürlich auch auf die öffentliche Verwaltung, um das auch klar zu sagen. Die Zusammenarbeit zwischen Bund und Ländern auf dem Gebiet kann verbessert werden. Die Zusammenarbeit heute ist sozusagen nicht verbindlich geregelt. Das ist sozusagen eine Kannvorschrift und was man darauf ableiten kann, ist eine Kannvorschrift bei so einem Thema nicht ausreichend.

NN:
Ich hätte noch eine Frage. Sie sprachen zwei europäische Regulierungen an. Wie sehen Sie all das.

Staatssekretär Vitt:
All das finde ich eine sehr wichtige, eine sehr gute Verordnung. Die Herausforderung, die sich daraus ergibt, müssen wir klar in Deutschland machen und ich glaube, dass wir das hinkriegen. Da haben wir unsere elektronische ID vom Personalausweis als unkritisch. Die Herausforderung dahinter ist, dass jemand anders aus einem anderen europäischen Land mit seiner ID kommt, die sozusagen für sein Land entsprechend akzeptiert wurde und bei uns damit arbeiten möchte. Ich habe Kontakte zu dem einem oder anderen Land. Wenn wir einmal so weit sind, dass wir das für uns dekliniert haben, dann würden wir so einen gegenseitigen partnerschaftlichen Test machen. Das ist Dänemark, um es gleich zu verraten, und Österreich, die sich anbieten, weil die bezogen auf die Digitalisierung ziemlich weit sind. Und das wollen wir einmal ausprobieren. Aber, das kann ich heute schon sagen, wird eine ziemliche Herausforderung. Aber Altersverordnung ist gut, gar keine Frage.

NN:

Ich möchte ein bisschen einhaken an dieser Stelle. Es geht manchmal nicht nur um eine Verordnung. Wir haben ein Beispiel dafür. Wir haben mit schmerzhaften Wehen jahrelang das Gesetz der Digitalisierung der Energiewende bekommen. Das Problem an der Sache war, dass im Grunde genommen eine Freiwilligkeit völlig ausgeschlossen war, weil die Einsicht in die Notwendigkeit und Sicherheit völlig fehl . Über Jahre hat man die Entwicklung eines Schutzprofils im Grunde genommen zunächst blockiert und dann lamentiert. Wie lange wollen wir das machen? Die letzte Digitalisierung der Energiewende ist ein Fundament für das Internet of Things und für Smart Metering und Smart Processing bis rein in das Gesundheitswesen. Wenn wir das nicht konsequent anwenden und übertragen auf beispielsweise den gesamten , dann haben wir nur ein Fundament für ein brüchiges Gebäude. Das kann nicht sein. Ich hoffe, dass Ihre Nachricht auch im Innenministerium bedeuten, dass besonders stark für , denn wir sind nicht in einer schwierigen Situation. Wir sind in einem Notstand. Die IT-Security ist im Tagesgeschehen bei allen Innovationsprozessen praktisch zu kurz gekommen. Die Frage ist, wie ist die Situation, das voranzubringen. Dann ist noch das Wirtschaftsministerium, dann das Verkehrsministerium. Da ist die gleiche Frage. Und bei der gesamten Industrie. Wann und wie wollen wir das alles machen, wenn wir keine IT-Security haben? Dann wird das nicht ein digitales Debakel, dann wird das ein digitales Desaster.

Staatssekretär Vitt:.

Ich interpretiere einmal die Frage daraus. Klar ist, wenn sich irgendjemand Gedanken macht über Digitalisierung, muss er in der Konzeption die IT-Sicherheit mitdenken. Macht er das nicht, kann es passieren, dass ich danach noch einmal ein Redesign machen muss. Wenn ich das nicht mitberücksichtig habe, werde ich gravierende Lücken haben. Das Risiko ist ungemein groß. Wie gehen wir auf die einzelnen Ministerien zu? Ich nehme jetzt ein Beispiel. Wir gehen auf die einzelnen Ministerien zu. Da gibt es ganz konkrete Digitalisierungsvorhaben. Smart Metering war so ein Thema. Da wird das BSI frühzeitig eingebunden. Das läuft wirklich gut. Ich glaube, dass das Bewusstsein immer mehr vorangeschritten ist. Dass wenn man in Richtung Digitalisierung geht, sich ganz konkrete Digitalisierungsprojekte vornimmt und dann frühzeitig die Sicherheit das BSI mit einbezieht. Wir können uns zurzeit nicht beklagen. Das kann man sagen. Ich will nicht ausschließen, dass irgendetwas an uns vorbeiläuft. Aber zu einem gewissen Punkt werden wir die wieder einfangen, wenn ich das einmal so locker formulieren darf.

Vielleicht habe ich mich da missverständlich ausgedrückt. Bei den Telemediendiensten ist es so, dass die Dienstanbieter, die Daten speichern, nicht wir speichern, sondern die speichern die. Wir haben nur eine gesetzliche Grundlage. Wir würden für die gesetzliche Grundlage sorgen. Ich habe eine große Hoffnung in die EU-Datenschutzgrundverordnung. Da gibt es nämlich konkret bezogen auf Datenspeicherung Rahmenbedingungen. Unter den Rahmenbedingungen kann man Daten speichern. Und wir kriegten sozusagen ein einheitliches Verständnis und Niveau auf europäischer Ebene. Das ist, glaube ich, die einzige Chance, die wir haben.
Wenn ich noch eines ergänzen darf. Es wäre gut, wenn wir bei uns in Deutschland nicht zu viel Änderungen und Anpassungen an dieser Grundverordnung zu mindestens im Bereich der Unternehmen vornehmen würden, denn ansonsten kriegt wieder jede Ausprägung. Das wiederum ist ein Nachteil für die Unternehmen. Wir haben jetzt eine einmalige Chance, eine einheitliche Datenschutzgrundverordnungen in Europa zu haben.

Prof. Eckert:
Herzlichen Dank soweit erst einmal. Ich möchte die nächste Keynote ankündigen. Ich freue mich sehr, dass wir mit Herrn Arne Schönbohm den Präsidenten des Bundesamtes für Sicherheit und Informationstechnik hier begrüßen können und auch Sie haben die Challenge bekommen, zum Titel unserer heutigen Veranstaltung Ihre Gedanken, Ihre Überlegungen uns mitzuteilen.

Herr Schönbohm:
Liebe Frau Prof. Eckert, lieber Herr Prof. Thielmann. Haben Sie herzlichen Dank, dass ich hier heute dabei sein darf. Ich glaube, es ist schon einmal ganz wichtig, dass man zwei Dinge macht. Auf der einen Seite, dass man miteinander und nicht übereinander spricht. Und eines meiner Herzensanliegen ist, dass wir natürlich die Entscheider irgendwo erreichen im Bereich der Cyber-Sicherheit. Gerade hier auch im MÜNCHNER KREIS, glaube ich, ist es ein ganz wichtiger Punkt, dass wir hier die Entscheider schön erreichen können. Sie haben vorhin die Frage gestellt, was denn das Thema eigentlich ist im Bereich automatisiertes Fahren oder Gesundheit oder Smart Metering. All diese Themen sind das, was wir versuchen im Bundesamt für Sicherheit und Informationstechnik, was wir tun, womit wir die Sicherheitskonzepte mit erarbeiten wollen. Gerade auf der CeBIT im März, Sie haben es auch gezeigt, Herr Staatssekretär, wie wir das Thema Car to X dargestellt haben, also wie das

Sicherheitskonzept einer sicheren Infrastruktur mit einem Baustellenfahrzeug, mit Fahrzeugen ist. Wie funktioniert dann dort eigentlich die Übertragung von Daten? Wie ist dort die Sicherheitsfunktionalität, die Sicherheitsarchitektur letzten Endes aufgebaut? Das ist eine der zentralen Aufgaben, die das Bundesamt für Sicherheit in der Informationstechnik hat. Wir sind halt nicht nur das Bundesamt für Sicherheit im Bundesinnenministerium sondern gesamtheitlich. Und ich glaube, dass das eine ganz wichtige Aufgabe ist, gerade wenn man sich das Thema der Digitalisierung intensiv anschaut. Und wir vergessen immer, wie schnell das alles eigentlich geht. Heutzutage ist für jeden von uns dieses Thema hochattraktiv.

Vorhin wurde über die mittelständischen Unternehmer gesprochen. Neulich war ich bei einer Mitgliederversammlung des Bundesverbandes der mittelständischen Wirtschaft und sah auch die ganzen Geschäftsführer. Die können ganz toll Produkte entwickeln, herstellen, verkaufen usw. Wenn man die nachts um 3 Uhr weckt und sagt, dass etwas zum Thema Digitalisierung erzählen sollen, dann beten die Ihnen das alles runter. Und dann sagen Sie, dass Sie jetzt über das Thema der Informationssicherheit reden wollen, worauf die Ihnen sagen, dass sie doch einen IT Beauftragten haben, der das macht.

Das ist einer der zentralen Punkte, dass wir da auch hinkommen müssen, dort die Entscheider zu bekommen und die auch in dieser sich schnell verändernden Welt entsprechend mitzunehmen. Es ist ja nicht alles so ganz trivial, wie sich das weiterentwickelt. Hier wurden mir Zahlen aufgeschrieben. ARD/ZDF online Studien aus dem Jahr 2015 belegen, das 79,5% der Bevölkerung in Deutschland das Internet gelegentlich benutzen. Ich habe gedacht, dass das ein bisschen mehr wäre, aber die tägliche Nutzungsdauer beträgt 108 Minuten. Wenn Sie sich im Vergleich dazu 2000 angucken, da waren es nur 28%. Wenn Sie dann überlegen, wie lange Sie Skala und alle anderen Themen teilweise im Einsatz haben, dann haben wir natürlich desruptive Technologien oder wie man das letzten Endes bezeichnen mag. Damit müssen wir auch einhergehen und ich glaube, dass das auch wichtig ist, um zu verstehen, wie das Spannungsfeld zwischen Regulierung und Selbstverantwortung aussieht. Je mehr wir uns digitalisieren – und das ist eigentlich eines meiner Schwerpunktthemen – umso mehr Angriffsvektoren haben wir natürlich, umso mehr Möglichkeiten hineinzukommen. Staatssekretär Vitt hat das Thema Krankenhaus schön dargestellt. Glauben Sie, so ein befall wäre vor 15 Jahren möglich gewesen? Natürlich nicht. Je intensiver die darauf basieren und wechselhafte Prozesse zusammenhängen, umso gravierender wird es natürlich auch. Wir können ganz plakativ sagen, so wie Sie sich alle digitalisieren und damit auch eine Menge

Geld verdienen – hier gibt es auch ein paar Server Sicherheitsunternehmer die stark unterwegs sind. Das ist natürlich das, was die organisierte Kriminalität (?) und all die anderen dementsprechend genauso machen. Genau das machen die, und die sind meistens auch sehr findig in dem Thema, damit vernünftig umzugehen.

Der Lagebericht 2016 vom BSI ist gerade in der Phase der Fertigstellung. Da werden wir die Zahlen dann genauer darstellen. Aber wir haben jeden Tag Hunderttausende neue Startprogrammvarianten. Wir haben allein für Android rund 50 Millionen verschiedene Startprogramme, nur um Zahlen zu nennen. Da wir das schon veröffentlicht hatten, im April das Thema Ransomware, das Thema Verschlüsselung und Erpressung, haben wir im Rahmen der Allianz für Cyber-Sicherheit eine Umfrage gemacht, und danach ist der Anstieg im Bereich Ransomware bis Mai um Faktor 70 gewesen, nicht nur 70%. Allein laut unserer Umfrage vom April haben rund 32% aller Antwortunternehmen gesagt, dass sie in den letzten sechs Monaten davon betroffen waren.

Es gibt noch eine Vielzahl von weiteren Zahlen, auf die ich nicht näher eingehen will. Es ist natürlich so, dass diese Zahlen einfach zeigen, dass die Gefährdungslage nicht nur eine Gefährdung ist, sondern dass es real ist, dass dort oben realer Schaden entsteht. Jetzt kann man sagen, dass mit einem Gesetz alles gut wird. Wir haben auch ein Gesetz gegen Einbrüche in Berlin und ich weiß nicht, ob das dadurch besser geworden ist, wenn ich mir die Einbruchszahlen hier im Land Berlin angucke. Von daher muss man noch ein bisschen fordern und fördern. Genau das, was Herr Staatsekretär Vitt dargestellt hat. Es geht natürlich auch darum, dass man die Aufgabe des BSI hinterfragt. Seit bin ich seit acht Monaten Präsident vom BSI und eines der ersten Themen, was mich bewegt hat, war, gemeinsam eine Art Leitbild zu machen. Was machen wir eigentlich? Wofür stehen wir? Wofür stehen die 660 Mitarbeiter? Wofür arbeiten die? Da haben wir gesagt, dass das BSI als die nationale Cyber-Sicherheitsbehörde die Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft gestaltet, Prävention, Detektion, Reaktion.

Das Entscheidende ist, dass Staat praktisch das Brot- und Buttergeschäft der Bundes. Das ist die Sicherheit der Netze des Bundes und all der Themen, die wir dort tun. Wir machen da eine Menge und ich bin auch dankbar dafür, dass wir diese Aufgaben und die notwendigen Ressourcen haben. Staat ist natürlich mehr als genau das, was Staatssekretär Vitt gesagt hat. Aber was machen wir in der Wirtschaft, wenn wir die Informationssicherheit in der

Digitalisierung gestalten wollen? Jetzt gehe ich zu Herrn Reinemann von Siemens und sage ihm, wie sie die Skala genau machen müssen. Da wird es sich bedanken und sagen, dass er das auch weiß. Da müssen wir natürlich gemeinsam einen kooperativen Ansatz überlegen, was wir hier bei. Cybersicherheit by Design von vorneherein mit einplanen kann. Sie haben bestimmte Themen gesetzt wie Datensparsamkeit und andere Themen. Wie kann man das machen? Und wie kann man das auch so machen, dass es etwas sicherer ist? Da gibt es hervorragende Beispiele wie im Bereich Smart Metering. Das dauert manchmal etwas lange, wie das ist, aber darüber kann man nachdenken und diskutieren. Immerhin muss man ein Rollout anders wie in England nicht stoppen und wieder neu aufsetzen, weil die Informationssicherheitsarchitektur von vornherein richtig war. Hier ist es wichtig, dass wir die Sachen, die wir machen, auch richtig machen.

Dann haben wir das Thema der Gesellschaft. Ich weiß nicht, wie oft Sie bei Informationsveranstaltungen sind. Dort sprechen Sie mit den normalen Menschen. Wenn Sie fragen, wer ein Smartphone nutzt, gehen viele Hände hoch. Wenn Sie fragen, wer irgendein Schutzprogramm beim Smartphone nutzt, gehen ganz wenige Hände hoch. Wenn Sie sich dann die Zugangsdaten derjenigen anschauen, welche Smartphones sie haben und was sie darüber machen. Wenn Sie denen dann eine Phishing Mail auflegen nach dem Motto „Der Prinz aus ZamundaI möchte gern 30 Mio. $ bei Ihnen anlegen, gibt es normalerweise genug Kandidaten im Raum, wo die Hand immer noch hochgeht. Da besteht vielleicht Handlungsbedarf, auch die normalen Menschen aufzuklären, zu sensibilisieren. Das ist das, was sich hier in dem Leitspruch wiederspiegelt.

Herr Vitt hat über das Thema des Informationsaustausches gesprochen. Wir bekommen eine Vielzahl von Daten von den kritischen Infrastrukturen. Ich glaube, dass es ganz wichtig ist und wir arbeiten auch vertrauensvoller mit denen zusammen, nicht weil sie müssen, sondern weil man einfach die Erfahrung gemacht hat, dass melden gar nicht weh tut. Das muss man manchmal lernen, und auch den Vorstand, die Aufsichtsräte überzeugen. Wenn man Themen gemeldet hat, ist es noch besser, dass man nicht nur sagt “Fire and Forget“, sondern dass man etwas zurückbekommt. Das ist ganz toll, dass es eben nicht eine Einbahnstraße ist. Wir haben vor drei Wochen die Dax und die MDax Unternehmen in separaten Meetings eingeladen und haben das Lagebild etwas ausführlicher dargestellt. Dann habe ich einmal reihum gefragt, was bei ihnen der Fall ist. Die sind ja nicht verpflichtet zu melden Der Vorstand eines Dax Unternehmens sagte z.B., dass sie in den ersten sechs Monaten 36mal CEO-Fraud gehabt

haben, 36mal, ein Unternehmen. Sie wissen das ja selbst. Die haben nicht jedes Mal jeweils 40 Millionen gezahlt, so wie LEONI, was durch die Presse ging, sondern sie haben das erfolgreich detektiert, anerkannt, abgewehrt usw. Natürlich ist das dann für die anderen Dax Unternehmen, die mit am Tisch sitzen, hochinteressant zum Austausch ähnlicher Themen. Liebes BSI, was kann man da machen? Wie kann man da vielleicht mit dem BKA zusammenarbeiten? Wir haben gleichzeitig ein Cyber-Abwehrzentrum, wie Sie wissen, wo die Informationen gebündelt werden und wo man auch überlegt, welche Institutionen des Bundes wo und wie dementsprechend dagegen vorgehen können. Das sind Themen, die man machen kann. Wo man keine Regulierung braucht, weil man sagen kann, dass Melden und Austauschen einen Mehrwert bringt.

All dieses hilft uns nicht wirklich weiter bei den kleinen und mittelständischen Unternehmen. Das ist in der Tat so, wo wir intensiv an verschiedenen Konzepten arbeiten, wo wir Multiplikatoren brauchen. Wir können nicht alle auf einmal beglücken. Also, muss ich Multiplikatoren suchen. Das ist natürlich ein Thema, wo wir die geeigneten Multiplikatoren suchen. Jetzt haben wir eine Allianz für Cyber-Sicherheit gemeinsam mit der Bitcom, wo Herr Holz und zahlreiche andere mitarbeiten, Herr Reinemann von BMA, Siemens. Das sind mittlerweile 2000 Unternehmen und bisher waren wir sehr stark ausgerichtet auf das Themenfeld IT Hard- und Softwareindustrie, die Sicherheitsunternehmen. In den letzten Jahren seit Gründung haben wir festgestellt, dass es da viele hervorragende Lösungen gibt. Das Entscheidende ist doch, dass wir jetzt diese Sicherheitslösungen, die wir haben, teilweise Made in Germany, auch in die Anwendung reinbringen. Seit April, wo auch Dr. Mittelbach dort den Vorsitz übernommen hat, wollen wir von den Anwender wie Volkswagen, Continental und all den anderen, dass die ihren Bedarf definieren und sich dann austauschen, wie man dementsprechend damit umgeht. Volkswagen und Conti ist nur ein Beispiel. Es gibt viele andere auch, die wir dort dementsprechend machen. Und damit kriegen wir auf einmal eine andere Sensibilisierung hin, andere Informationen und somit wird dieser gesamte Netzwerkgedanke, den wir haben, wo wir Informationssicherheit gestalten wollen, als Informationsamt, als BSI, als Bundesamt für Sie alle letzten Endes und einen erheblichen Mehrwert für alle bringen. Das ist das, was wir dort tun und woran wir hier natürlich intensiv arbeiten.

Bei den Bürgern, die ich zu Beginn geschildert habe, glaube ich nicht, dass wir die so regulieren können oder beglücken können, dass wir sagen können, es gibt einen

Internetführerschein. Ich glaube, dass ich es nicht machen könnte und es auch politisch schwierig durchsetzbar ist. Von daher, ich bin kein Politiker, ist das ganz gut. Ich glaube, dass das nur über Freiwilligkeit und Selbstverantwortung geht. Das heißt, Training, vielleicht einen siebten Sinn zu machen, wie es früher einmal mit dem Thema Verkehrsschulung war. So etwas kann man mit dem Thema Informationssicherheit gemeinsam mit den Multiplikatoren machen. Dann soll man auch an die Schüler und an die anderen rangehen. Meine Tochter ist jetzt neun und hat kein Handy. Also, ist sie sicher. Aber dementsprechend sollten die aber da schon vorbereitet werden. Darum haben wir z.B. gemeinsam mit der Polizei, polizeiliche Prävention und versuchen auch den Schulen Materialien zur Verfügung zu stellen, wie man sich sensibel im Internet verhält, Informationssicherheit. Das Entscheidende ist dabei, dass man das gemeinsam mit den Polizeien, den Multiplikatoren macht, die dieses kontinuierlich mit hineinbekommen in die dementsprechenden Einzelteilthemen. Wir denken über neue Konzepte nach und haben eine Denkwerkstatt mit einem Chaos Computerclub und einigen anderen Partnern, wo wir über die anderen Modelle wie Natching usw. und andere Themen, passende Themen, die die Gesellschaft vorantreiben, informieren, damit sie von sich dieses handeln und den Mehrwert ihres Handelns auch erkennen – Denkwerkstattmodelle. Das sind natürlich Punkte, wo wir auf neue Themen kommen, um dann da voranzukommen.

Ich möchte noch auf ein letztes Thema kommen: Standardisierung, Zertifizierung und Verschlüsselung. Standardisierung und Zertifizierung ist eines der ganz wichtigen Themen, woran wir auch arbeiten. Ich habe vorhin Smart Metering genannt, autonomes Fahren und diese ganzen einzelnen Teilthemen. Es ist ganz wichtig, dass hier die Qualitätsanforderungen für die IT-Produkte festgelegt werden, dass die transparent sind und dass wir hier noch schneller werden und noch mehr zertifizieren. Das BSI, als Beispiel, ist der Weltmarktführer im Ausstellen von Sicherheitszertifikaten, High End. Es gibt keine Institution, die mehr ausstellt als wir. Aber wir können da noch schneller und besser werden, indem wir vielleicht gemeinsam mit unseren europäischen Partner, unsere Schwesterbehörde ist die ANSSI in Frankreich, grenzüberschreitend gemeinsam Zertifizierungen entwickeln, und daran arbeiten wir gerade, damit dieses schneller geht. Nicht im High-End-Bereich, aber im Low-End-Bereich, weil uns damit schon ungemein geholfen wäre. Wenn man dieses dann noch stärker gemeinsam auch mit der ENISA (?) und anderen Partner vorantreiben kann. Aber fangen wir erst einmal bilateral an und dann kann man das weiter aufbauen. Das ist ein ganz wichtiges Thema.

Das andere wichtige Thema ist die Verschlüsselung. Im Rahmen des nationalen IT-Gipfels im letzten Jahr wurde die Initiative vom BMI unterschrieben und vorgestellt, die Charta zur Stärkung der vertrauenswürdigen Kommunikation. Darüber gibt es viele Diskussionen teilweise in interessierten Kreisen. Da sind wir einer der sehr starken Verfechter. Zurzeit sind die Code Maker (?), die den Wettlauf gegenüber den Code Breakern aufgrund der technischen Verfahren gewonnen haben. Wir als BSI verstehen uns als Code Maker Unterstützer, um diesen Wettlauf weiterhin vorne zu haben. Im Rahmen der gesetzlichen Vorhaben wird es einfach von der Klarheit her eine CITES Organisation geben, die sehr stark mit einem Thema forscht, wie man den Code entsprechender der gesetzlicher Regularien breaken kann. Wir verstehen uns da eher wie die Verteidiger, die versuchen, das vorher sauber zu halten und die anderen können gerne die Tore schießen entsprechend der gesetzlichen Themen. Aber dieses Thema der Verschlüsselungsthematik weiter voranzubringen und auch in Einheit zu bringen innerhalb Deutschlands, ist von herausragender Bedeutung.

Die Themen, die ich jetzt bewusst genannt habe, basieren im Wesentlichen auf dem Thema der Freiwilligkeit im Sinne von Fördern. Vor neun Monaten war ich auch noch Unternehmer. Es ist immer gut, wenn man da nett versucht Themen rüber zu bringen und zu erklären nach dem Motto „machen Sie doch mal“ usw. Jeder Unternehmer macht dann etwas, wenn er irgendwo einen Mehrwert bekommt. Ich kann mich gut an den Cyber-Security Summit mit der Telekom erinnern, als wir mit Herrn diskutiert haben und er sagte, dass wir das ein bisschen fördern müssen und ob wir gesetzliche Initiativen haben müssen oder nicht. Ich sagte damals zu ihm, dass ich genau sagen kann, wie viele Feuerlöscher bei ihm in der Telekomzentrale sind. Er schaute mich an und fragte: wie viele? So viele, wie die gesetzlichen Vorgaben es vorschreiben, keiner mehr, keiner weniger.

Ich glaube, dass wir schon in bestimmten Teilbereichen, wo wir eine kritische Infrastruktur haben, Vorgaben machen, so wie es IT-Sicherheitsgesetz ist. Man kann überlegen, wie Sie es dargestellt haben und darauf eingehen, ob man das noch weiter nach unten ausbauen kann in anderen Bereichen, die von elementarer Bedeutung ist. Und ich glaube, wir werden insgesamt – und das wird die Diskussion zeigen – darüber nachdenken müssen, was denn eine Kette von hintereinander fahrenden LKWs im Bereich der Logistik ist, die autonom fahren. Sind die zu werten wie ein Zug, also Logistik, oder nicht? Je weiter diese Digitalisierung voranschreitet, umso mehr werden wir überlegen, was eigentlich unsere kritischen Infrastrukturen sind und wie sich das verändert.

Von daher, glaube ich, müssen wir schon intensiv darüber nachdenken. Ich habe jetzt keine Lösung dafür. Wir arbeiten ja an Lösungen, aber für alles hat man nicht sofort etwas, was man vorstellen kann. Aber das sind Themen, worüber wir nachdenken müssen, weil die Digitalisierung weitergeht. Und da werden wir wahrscheinlich irgendwo ein Regulativ brauchen in zukünftiger Art und Weise, weil die Bedrohungslage zunimmt. Die Digitalisierung, Vernetzung, Verknüpfung nimmt zu und dementsprechend müssen die Sicherheitsbehörden handlungsfähig sein. Die sind handlungsfähig, weil wir Informationen haben, Ihnen etwas anbieten können. Von daher, glaube ich, sind wir ein fairer Gesprächspartner. Wir sind Vertriebsleute teilweise, vielleicht auch Geschäftspartner, um da zu einem vernünftigen Tun zu kommen. Gemeinsam können wir die Informationssicherheit für Deutschland in der Digitalisierung gestalten und das ist das, wofür wir antreten. Haben Sie herzlichen Dank für die Aufmerksamkeit.

Prof. Eckert:
Ganz herzlichen Dank für Ihre Ausführungen. The door is open. Stellen Sie Fragen! Wenn Sie kurz sagen, wer Sie sind.

NN:
Bundesverband der Energie- und Wasserwirtschaft. Wir vertreten die zahlreichen Betreiber kritischer Infrastrukturen im Sektor Energie, Wasser, Abwasser und arbeiten immer noch sehr gut mit dem BSI und Innenministerium zusammen. An der Stelle auch Danke. Am 3. November endet jetzt die Frist zur Benennung der Kontaktstellen beim BSI. Haben Sie einen Überblick wie weit der Stand in den sieben Sektoren ist? Und im Hinblick auf die Meldepflicht, über die ja auch schon gesprochen wurde, die gilt ja für den Sektor Energie schon seit Inkrafttreten der Verordnung. Das BSI hatte früher einmal die Zahlen von sieben Meldungen pro Betreiber genannt, haben Sie da vielleicht auch schon, jetzt wo die Meldepflicht ein paar Monate läuft, einen Erfahrungswert, ob das mehr oder weniger ist? Danke.

Herr Schönbohm:
Vielen Dank. Ich habe neulich die Zahl gesehen. Ich will jetzt – es ist auch Presse da - ungern die Zahl nennen. Ich habe aber neulich die Zahl gesehen, wie viele sich dar bei uns akkreditiert haben. Das ist ein Thema, wo die Kriterien draußen sind und dann kann man sich

dort bewerben. also Einschreiben praktisch und dann wird man dort akkreditiert. Aufgrund der Zahl, die ich dort gelesen habe, ist es, glaube ich, noch einmal gut, wenn wir noch einmal sensibilisieren und die Verbände und andere Partner ansprechen - das ist geschehen -, um dann dort noch einmal auf die Mitglieder einzuwirken, das vielleicht auch äußere Bestandteile der kritischen Infrastruktur sind und sich vielleicht dann da doch bewegen. Was wir erleben, ist so das klassische Thema nach dem Motto: Das ist so wie früher in der Schule, man macht das einen Tag bevor die Arbeit geschrieben wird, fängt man an zu lernen. Da sehen wir hier genauso. Und von daher sind wir vorbereitet. Wir halten die Ressourcen vor. Wir haben es geübt und wir sind erprobt. Aber da ist noch Luft nach oben. Die Anzahl der Meldungen, da war ich ganz überrascht, ist auch positiv nach oben gegangen. Dazu werden wir im Lagebericht auch ein bisschen was sagen. Das entscheidende ist aber, dass wir auch zunehmend freiwillige Meldungen bekommen. Das ist das, wo ich glaube, dass es einfach ein Erfahrungshorizont ist. Wenn RWE etwas gesagt hat und gesagt hat, ich hab gemeldet, hat es gar nicht wehgetan, dann macht der andere es vielleicht auch freiwillig. Das erleben wir gerade. Von daher haben Sie schon eine ganz gute Sache genannt.

Prof. Thielmann:

Herr Schönbohm, Sie haben neben dem BSI auch das ANSI genannt. Die Digitalisierung und damit auch die Sicherheitsthemen sind ja global. Was halten Sie davon, wenn man darüber nachdenkt, ein europäisches BSI zu kreieren? Sie haben auch über Standardisierung gesprochen, was auch ein Thema ist, was nicht nur national ist.

Herr Schönbohm:

Also, hier sitzt ein guter deutscher Kandidat für so etwas. Vielleicht liegt die Herausforderung beim BSI. Wenn wir einmal die Bandbreite angucken, die wir haben, von der Sicherheit der Netze des Bundes über das Thema Beratung, Wirtschaft und Gesellschaft, über das Thema Zertifizierung, über das Thema Digitalisierungsthemen, autonomes Fahren usw. Das ist so eine Bandbreite, die wir da haben, die auf der europäischen Ebene schwer darstellbar ist. Ich glaube, wir waren gerade bei der Evaluierung, das darf ich sagen Prof. Helmbrecht, am Dienstag gemeinsam in Brüssel zum Thema CERT EU. Ich will es einmal so formulieren: wenn wir ein gutes CERT haben, das so funktioniert wie das Bundes-CERT, wäre ich schon einmal ganz zufrieden, wenn wir da diesen Weg entsprechend weiterkommen. Und wenn dann vielleicht, das geht politisch strategisch rechtlich gesehen nicht, ENISA und CERT noch intensiver zusammenarbeiten, sind wir auch schon einen großen Schritt weiter. Aber wir

werden immer die Diskussion haben zwischen der Rolle der Mitgliedsstaaten und der Kommission natürlich.

Dr. Sturm:

Mein Name ist Jürgen Sturm, ZF Friedrichshafen AG, in der IT Verantwortung. Das ist eine Frage und kein Widerspruch, sondern vielleicht können Sie es noch etwas weiter ausführen. Sie haben vom ökonomischen Prinzip gesprochen, also unternehmerisches Handeln. Und wir müssen ja für das Ganze eigentlich immer Digitalisierungschancen ergreifen. Das ist ganz wichtig. Und dabei Risiken Management. Ich glaube, wir müssen alle miteinander noch stärker herausarbeiten, dass diese ganzen regulatorischen Dinge dann, wenn man sie zu Ende denkt, ob man wirtschaftlich besser an das Ziel kommt, diese Gefahren abzuwehren. Weil wenn ich das Wissen teile. Diese Herausforderung ist für jedes Unternehmen egal, welcher Größenordnung, so groß, dass es für jeden zu groß ist. Wenn das richtig ist, dann ist über diese Vernetzung und entsprechende Trusted Partners, wo ich sehr schnell dieses Best Practices in kürzester Zeit generieren kann, ist das eine Ratio. Und die arbeiten wir meines Erachtens nicht genügend raus. Vielleicht können Sie da irgendwie darauf achten, dass man solche Fallbeispiele, die wir immer wieder haben, dann auch als Business Case durchdeklinieren und sagen, bevor da jeder in seinem Schrebergarten versucht, das selber zu lösen. Was bedeutet das, wenn wir dann einmal in der Laubenkolonie, dass wir alle gemeinsam die Best Practices austauschen? Vielleicht können Sie darauf eingehen.

Herr Schönbohm:

Herr Dr. Sturm, haben Sie herzlichen Dank. Ich glaube in der Tat, wenn wir sagen, freiwillig, dann geht es natürlich am Ende darum, was der Return vom Investment ist. Am Ende ist es eine Frage des Risikomanagements, das man da eingeht. Und da glaube ich, muss man schon noch intensiver darüber nachdenken, wie man den Staat bewertet. In der Regel werden Daten kopiert. Das war beim Thema Sabotage relativ einfach. Wenn die Bänder stillstehen, ist das wie Betriebsunterbrechung. Da gibt es zahlreiche wirtschaftliche Modelle. Das können Sie aber darstellen. Wenn ich jetzt die Daten kopiert habe von einem neuen Kraftwerkstyp, eine Turbine von mir aus von Siemens, was ist dann der Schaden? Ist es die Arbeitsleistung, der entgangene Gewinn, der entgangene Umsatz? Ist es gar kein Schaden, weil sie es eh nicht nachbauen können? Es ist ja die Frage, wie wir was bewerten? Das ist einer der zentralen Punkte im Bereich des Risikomanagements. Da, glaube ich, ist in den letzten Jahren schon eine Menge passiert, wenn ich mir anschaue, wie das in Amerika bewertet wird. Wenn ich mir

anschaue, dass Grundlage dafür, dass ich eine Cyber-Versicherung abschließe, ist ja genau das, dass man sagt, welchen Minimum Standard man hat, z.B. BSI Grundschutz, den ich jedem empfehlen würde, der gerade in der Phase der Überarbeitung ist mit 77 Bausteinen. Und dass man dann sagt, dafür, dass ich das mache, wie stark sich eigentlich das Thema meines Risikos reduziert. Wie stark brauche ich das mit dem Risiko. Und da spielen inzwischen auch Wirtschaftsprüfer eine wichtige Rolle, nicht im Sinne von Dienstleister sondern im Sinne von Bewertung der Risiken genau wie Versicherungsunternehmen. Das wird ein konträrer Prozess sein, den wir auch weiter entwickeln wollen und darum habe ich den Leitspruch vom BSI gesagt: wir wollen Informationssicherheit gestalten. Das heißt eben genau, dass wir hier natürlich auch gern mit Ihnen gemeinsam überlegen, wie denn das richtige Risikomanagement eigentlich aussieht. Das ist bei jedem irgendwie individuell unterschiedlich, aber dazu wird es mit Sicherheit Clusterthemen geben.

Prof. Eckert:
Sie wollen gestalten, Herr Schönbohm. Was wäre denn aus Sicht vom BSI Schlüsseltechnologie, die unbedingt gestaltet werden muss, die auch hier durch deutsche Industrie gestaltet werden muss, damit wir diese Kompetenz einfach haben und uns nicht abhängig machen? Dann sind sie gleich dran.

Herr Schönbohm:
Dann können wir gerade die andere Frage noch nehmen, dann kann ich darüber nachdenken. Das ist ein Thema, Frau Prof. Eckert, zum einen vielen Dank für die Frage, die, glaube ich, sehr schwierig auf der einen Seite zu beantworten und sehr weitgreifend ist. Da gibt es auch gemeinsame Anstrengungen, Überlegungen, auch gemeinsam mit anderen Partnern aus anderen Ministerien und dazu gibt es, glaube ich, auch Überlegungen im Rahmen des Cyber Sicherheitsstrategie.

Prof. Eckert:
Das war mir schon klar, dass das ein bisschen auf dem Stein ins Wasser zu schmeißen. Ich hab Sie ein bisschen überrannt. Jetzt sind Sie dran.

NN:
NN von Roland Berger. Stichwort Talente. Wenn Sie als Unternehmen jetzt zehn IT-Sicherheitsexperten in Deutschland einstellen wollen, dann ist es gar nicht so einfach, die zu

finden. Deswegen zwei Fragen, erst einmal astrakt. Können Sie oder auch Klaus Vitt noch einmal darauf eingehen, wie Sie die Situation, das Angebot am Markt einschätzen, auch was die Rolle BSI und Bundesregierung ist, vielleicht auch in anderen Häusern, da auf Ausbildung und Verfügbarkeit einzuwirken. Zweitens haben Sie für Ihr Haus, das BSI, gesagt, 600 Mitarbeiter, Leitbild, viele neue Aufgaben. Fühlen Sie sich ausreichend gerüstet? Wie sieht das BSI nach drei Jahren aus bei den ganzen neuen Aufgaben, die Sie sich vornehmen? -

Herr Schönbohm:

Vielleicht, Herr Vitt, darf ich anfangen und dann können Sie für die Bundesregierung darstellen. Erst einmal, ausgelastet bin ich genug. Wenn Sie mich fragen, wie das BSI in drei Jahren aussieht, glaube ich, wird es – wenn ich mir jetzt die verschiedenen Parteiprogramme einmal durchlese und die verschiedenen Strategien durchlese – als nationale Cyber Sicherheitsbehörde eine der zentralen Rollen spielen, d.h. nicht alles selber machen sondern eher wie ein Dirigent mit einem guten großen Orchester. Natürlich können wir auch die Pauke spielen und haben dort im Bereich des Bundes eigene Zuständigkeiten und Fähigkeiten. Aber wir werden natürlich viel intensiver auch kooperativ mit den anderen zusammenarbeiten und auch lernen. Das heißt nicht nur sprechen sondern auch zuhören und fristgerecht liefern und all diese ganzen Teilthemen. Intern, wir sind ja hier unter uns, ist es so, dass ich sehr stark das Thema Thought Leadership ausgeb. Ich möchte gern, dass das BSI als Juwel, als Kompetenzzentrum in Deutschland eine Thought Leadership hat, nicht in allen Bereichen, aber in bestimmten ausgewählten Kernbereichen. Das halte ich für elementar wichtig. Und das halte ich deshalb auch für wichtig, weil wir darüber natürlich auch die Talente bekommen. Wir haben z.B. im Bereich der Kryptografie einen der fähigsten Professoren in Deutschland oder weltweit, eine der weltweiten Koryphäen. Wir haben so etwas auch im Bereich autonomes Fahren. Und diese ausgesuchten Leuchttürme in dem Umfeld, Kryptografie ist schwierig mit den Veröffentlichungen, aber die weiß es natürlich, ist es dann so, dass die wiederum auch andere Talente anziehen. Es gibt ja diesen Spruch: First Class People Hire First Class People. Second Class People Hire Third Class People. Dann ist natürlich auch ganz wichtig, dass wir bei dem, was wir anbieten, eine vernünftige Work Live Balance. Wir haben also eine gute Nachfrage im Bereich des höheren Dienstes, auch worauf sich viele Personen bewerben. Im Bereich des gehobenen Dienstes ist es nicht ganz so einfach. Da ist vielleicht auch das Thema Beamtenrecht eine Herausforderung in dem Zusammenhang. Mittlerer Dienst ist gut. Wir decken das, aber wir sind auch einer der beliebtesten Arbeitgeber in dem Umfeld in Deutschland, Platz 15 laut einer EU Studie. Wir

sind diejenigen, die auch gern frühzeitig Diplomarbeiten und anderes machen, um frühzeitig die Personen zu binden, Praktika und anderes anbieten. Wir bieten Stipendien an, in Bonn zum Beispiel. Wir sind aber auch draußen auf den ganzen, so wie Sie hier auch, in Darmstadt und wo das alles ist, auf den verschiedenen Jobmessen.
Aber mir ist natürlich auch wichtig, dass wir mit der Wirtschaft intensiver zusammenarbeiten. Da überlegen wir gerade, inwiefern man eigentlich auch ein Austauschprogramm machen kann für eine bestimmte Zeit mit Partnern aus der Wirtschaft, nicht im Sinne von, dass die da sind, weil die Leute von uns rausziehen oder rausbewerben, sondern im Sinne von, dass wir wechselseitig voneinander lernen. Dass wir wissen, was vielleicht eine BASF oder jemand anders dort macht in dem Umfeld, und zwar nicht nur der sondern auch die anderen. Wie die vielleicht auch Personalmarketing machen. Wie die vielleicht auch so eine große Bandbreite haben. Das ist eigentlich das mit den Zertifizierungsstellen, mit den anderen Partnern, mit dem TÜV IT z.B. auch zusammenarbeiten. Das sind so die Themen, wo ich sage, dass wir dadurch innovativ und auch ein attraktiver Arbeitgeber sind.

Last but not least in all den Umfragen, die ich bisher gelesen habe, ist das Thema Work Live Balance, dass man etwas Sinnvolles tun will, wichtiger als allein Geld zu verdienen. Das ist eines der Themen, die uns natürlich in die Karten spielen im positiven Sinne. Daran bin ich unschuldig. Das ist die Generation, die sich gerade jetzt in diese Richtung entwickelt hat. Und das spricht für das BSI, weil Sie da tolle Sachen machen können, und es ist international vernetzt und verdrahtet, weil wir auch diesen internationalen Charakter haben in Richtung EU, aber auch Richtung USA und anderen Partner. Das ist, glaube ich, ist ein Alleinstellungsmerkmal, wo es uns in dem Umfeld noch gut geht. Aber wir müssen gemeinsam auch daran weiter arbeiten.

Prof. Eckert:
Ich würde noch zwei Fragen zulassen, weil Herr Schönbohm früher weg muss.

NN:
Das passt in der Reihenfolge ganz gut, weil ich noch mal in die Kerbe schlagen will. Wir haben jetzt auch die Bundeswehr, die sich sehr intensiv um das Thema kümmert. Elf neue Professuren in der Thematik, d.h. der Kampf um die Köpfe wird nicht nur zwischen Wirtschaft und Behörden sondern auch zwischen Behörden und Behörden stattfinden. Jetzt stelle ich einmal ein provokantes Schreckensszenario auf. Die Bundeswehr bekommt die

ganzen Leute und wir haben Cyber Vorfälle, zu sagen was Cyber War ist, ist immer schwer. Es war früher immer einfach. Wenn der russische Panzer auf dem Platz steht, wusste man, er ist da. Heute ist es ein bisschen schwieriger. Wie verhindern wir die Situation Bundeswehr Einsatz im Innenland etc., die Schwierigkeiten, dass wir Cyber Vorfälle im Umfeld haben. Und dann haben wir auf der einen Seite, ich nenn es jetzt einmal Krieger bei der Bundeswehr, die nichts tun dürfen. Und wir auf der andren Seite haben zu wenige Leute. Also, wie wollen Sie das Thema Cyber Strategie, von daher die Frage in beide Richtungen, dafür sorgen, dass wir diese Kräfte dann auch vereint nutzen können? Auch in der Defense, wenn unklar ist, ob es der russische Student oder der russische Offizier ist.

Herr Schönbohm:

Teilweise wird der Student dann zum Offizier. Vielleicht relativ einfach. Wir haben zunächst einmal ein Cyber-Abwehrzentrum. Das Cyber-Abwehrzentrum funktioniert, wo die Behörden sich untereinander abstimmen wo auch eine Bundeswehr daran beteiligt ist. Einsatz der Bundeswehr im Innern ist eine politische Frage, die würde ich mich nicht trauen zu kommentieren. Oder würde ich für unschicklich halten zurzeit. Das ist im April, Mai schon durch die Presse gegangen, als der Minister im Rahmen der Kabinettsklausur in Meseberg gesagt hat, dass z.B. auch beim BSI stärker mobile Teams aufbauen werden. Das sind genau die Themen, wo wir helfen. Es ging durch die Presse. Es gab diesen Vorfall im Krankenhaus in Neuss. Natürlich war da ein BSI Kollege und hat geholfen, dem Patienten in eine stabile Seitenlage zu bringen. Jetzt kann man sagen, dass es nicht ein oder zwei Fälle sondern Tausend Fälle sind. Wenn es Tausend Fälle sind, 2000 Energieversorger oder so sind, sind wir lucky und haben auch kein Internet mehr, weil wir keinen Strom haben. Jetzt aber eben nicht, wenn Energie und alles andere noch funktioniert und andere Sachen ausfallen, haben wir Konzepte. Das ist ein normales Katastrophenschutzkonzept, wie man dann darauf reagieren kann. Das BKA hat auch Quick Direction (?) Forces, die 24/7 einsatzbereit sind. Der Verfassungsschutz hat es, um dann auch aufzuklären, wie es dazu gekommen ist. Wir haben es und das wird koordiniert über das Cyber-Abwehrzentrum. Und natürlich kann man davon ausgehen, der General Schell heißt. Der war es bis Oktober. Der ist auf der Hardthöhe. Das ist nicht so weit weg von der Bundesberger Allee. Natürlich tauschen wir uns aus, wie man das macht und überlegen auch, wie man mit den einzelnen Themen zusammenarbeitet. Aber das geht natürlich weit darüber hinaus, wie man das im Einzelnen macht. Aber ich glaube, da gibt es gute Lösungen.

Herr Raab:

Ich wollte quasi auch noch mal in dieselbe Richtung gehen. Ich glaube nicht nur, dass wir zu wenige Talente haben sondern teilweise auch die falschen. Wir reden von den IT-Experten, die wir haben. Wenn wir über IT und Industrie 4.0 sprechen, brauchen wir auch die ganzen Leute, die sogenannten OTI (?) unterwegs sind. Auch die gibt es, wahrscheinlich auch zu wenig. Aber das wächst auch immer mehr zusammen, d.h. wir brauchen immer mehr Leute, die auch in beiden Welten denken können. Sehen Sie sich da in der Aufgabe, Sie haben auch vorhin von der Thought Leadership gesprochen, da auch in Richtung des Bildungssystems, in Richtung Universitäten einzuwirken, Ideen zu geben, dass entsprechender Ausbildungsgänge entstehen, weil da auch noch einmal ein ganz anderer Bedarf an ausgebildeten Fachkräften entstehen wird, den es heute so noch gar nicht gibt.

Herr Schönbohm:

Herr Raab, vielen Dank. Kurze Antwort: ja. Relativ einfach, ja natürlich. Jetzt muss man gucken, ob es meine Priorität Nummer 1 ist. Nein, ist es nicht. Es ist aber ein gesellschaftliches Thema, was wir natürlich mittelfristig lösen müssen. Dafür brauche ich die Koryphäen. Dafür brauche ich die Themen, von denen wir sagen, dass das die drei, vier Kernpunkte sind, wo wir auch die zukünftigen guten ausgebildeten Leute brauchen. Das müssen nicht alles die Cyber-Sicherheit Spezialisten und die super Cracks sein. Es langen auch normale andere Ausbildungslehrgänge, die man vielleicht auch machen kann. Vor einigen Jahren gab es mal den Spruch – das habe ich noch gelernt, als ich vor 27 Jahren Student war –, der hieß: Lebenslanges Lernen. Wenn ich mir die Halbwertszeit von Wissen angucke, ist es schon wichtig, dass ich in den ersten 23 Jahren meines Lebens einmal im Crack war, nicht wahr Herr Sturm, und dann sagen wir nicht, jetzt hören wir auf zu lernen. Mir geht es darum, die Leute stärker dort ran zu führen und weiter auszubilden. Das gemeinsam vielleicht auch mit den Universitäten zusammen.

Prof. Eckert:

Gut, genau. Gemeinsam mit den Universitäten, Forschungseinrichtungen. Letzte Frage für diese Runde.

NN:

NN von der Bosch Engineering. Ich bin Anwender Ihrer Lehre. Mit welchem Risikobegriff wollen Sie als BSI zukünftig arbeiten? Der bestehende Risikobegriff ist als taktische

Entscheidungshilfe für Verfolgen von Prospects jetzt nur bedingt geeignet. Wir benutzen die ganze Zeit diesen Risikobegriff und es kommt in der Art und Weise, wie Sie das benutzen oder wie wir das bei Security benutzen, die Aussicht auf den Gewinn. Man ist ja auch bereit, Risiken einzugehen für den Gewinn. Ich möchte hinweisen, wie schwer sich die DIN getan hat, die ISO 31000 praktisch zu einer DIN Norm zu machen. Können Sie als BSI dort noch unterstützen?

Herr Schönbohm:

Wir können mit Sicherheit unterstützen. Ob wir das bisher adäquat gemacht haben, sage ich ganz ehrlich, weiß ich nicht. Wenn ich mir anschaue – wo ist Herr Jacumeit von DIN? – da arbeiten wir gut zusammen miteinander und auch im Rahmen der Überarbeitung des BSI Grundschutzes. Ich glaube, in dem Zusammenhang werden wir schon andere Risikobegriffe bekommen. Aber es ist auch eine sehr operative Frage und das ist am Ende eine Frage der Unternehmensführung. Welche unternehmerischen Risiken bin ich bereit einzugehen und welche nicht mehr. Da können wir mit Methodiken versuchen zu unterstützen. Aber da sehe ich eigentlich sehr stark auch die Wirtschaftsprüfer und die anderen in der Pflicht. Was wir machen können, ist hervorragend darstellen, wie das Klagebild, wie die Bedrohungslage ist und wie man damit umgehen kann. Aber dieses dann umzusetzen in das operative Handeln und Tun des Unternehmers oder der staatlichen Institution, ist Sache des Managements. Also, wir werden nicht in die Rolle des Managements reingehen können. Da bin ich bei Ihnen, aber das machen wir ja im Wesentlichen hier. Das sollten wir noch offensiver kommunizieren, vielleicht auch gemeinsam kommunizieren. Also, bringen Sie es auch rüber bei Ihren Leuten. Jetzt haben das die anderen hier auch gehört. Herr Dr. Sturm, Herr Holz, Herr Reinema – implementieren!

Prof. Eckert:

Ich denke, das ist Konsens. Herr Schönbohm, ganz herzlichen Dank, dass Sie sich auch den Fragen so ausführlich gestellt haben. Ich freue mich sehr, dass wir jetzt den Blick öffnen in die europäische Dimension und dass Herr Prof. Udo Helmbrecht hier ist. Er ist Präsident der Europäischen Netzwerksicherheitsarchitektur, kurz ENISA. Wir freuen uns, auf den Einblick, Ausblick, vielleicht gute Practices aus europäischen Nachbarländern.

Prof. Dr. Udo Helmbrecht, ENISA, Heraklion, Griechenland:
Es freut mich, dass ich hier sein darf. Nachdem ich jetzt der dritte in der Runde bin, möchte ich ein bisschen reflektieren, was gesagt wurde und mache das vielleicht auch ein bisschen sarkastisch. Zunächst einmal finde ich es toll, wieder in Deutschland zu sein, weil man hier noch mit Titel angeredet wird. Ich habe lange dafür gearbeitet. In Europa benutzt man nur Vornamen, kann auch einen Kommissar duzen. Das Problem ist, einen deutsche Kommissar duzt man nicht, denn dann ist man wieder Deutscher und sagt wieder Sie. Die Krawatte habe ich übrigens umgetan, als ich vorhin hier reingekommen bin.

Ein paar Punkte: 660 Mitarbeiter, Herr Schönbohm. 2003 waren es 380, als ich damals da war. Ein EU BSI – eine interessante Frage. Was ist die ENISA? Die ENISA ist eine europäische IT-Sicherheitsbehörde, die alle die das BSI kennen, die Dinge umfasst, die dort die Struktur kennen. Ein Dr. Isselhorst macht ein bisschen was Herr Kowalski macht im Bereich Standardisierung. Was wir nicht machen ist Kryptografie. Und wir haben auch nicht die Befugnisse des BSI, die es bei der Novellierung 2009 bekommen hat, über das IT-Sicherheitsgesetz. Was aber interessant ist, es ist ein ähnliches Muster. Wenn Sie in Europa, auch in Deutschland, wir nennen das Secondary Legislation, durch andere Gesetze, Befugnisse bekommen. Das heißt, ENISA bekommen über das Telekommunikationsgesetz, über die ENISA (?) Direktive, das Europäische IT-Sicherheitsgesetz, über die Direktive.
Wenn man sich das anschaut, dann, sag ich mal, befinden Sie sich hier im deutschen Elfenbeinturm.

Es ist gut, was gemacht wird, und wir sind sicherlich in Deutschland Jahre voraus, wenn wir es mit anderen Staaten vergleichen. Ich vergleiche das Innenministerium, in der Abteilung dort ist zuständig Strategie, Umsetzungsplan Bund. Als ich damals anfing, war es noch im Wirtschaftsministerium der Staatssekretär Tacke, der mit dem Signaturbündnis angefangen hat. Viele gute Initiativen, nur wenn man sich das dann anguckt, der Personalausweis kommt nicht zum Fliegen, die Gesundheitskarte kommt nicht zum Fliegen. Die Frage ist dann, wer sie benutzt und wenn sie nur die gesetzlich Versicherten benutzen und wenn sie europäisch nicht funktionieren, ist es auch wieder halbherzig.

Ich will ein paar europäische Beispiele nennen. Sie haben in Deutschland einen Verband Bitkom und Teletrust. Wenn Teletrust sagt, IT-Security made in Germany, habe ich sie als BSI Präsident auch vertreten. Wenn Sie sich das europäisch angucken, dann haben Sie einen

Staat Estland mit einem Präsidenten Ilves. Die haben da eine grottenschlechte Signaturimplementierung, aber flächendeckend in einem Staat Estland mit weniger Einwohnern als die Stadt München. Der Präsident Ilves versteht etwas von IT, weil er einmal Programmierer war. Wenn der in Brüssel ist, lobbyiert er für die estnische Signatur. Da ist keiner von Ihnen dann dabei. Österreich hat eine Bürgerkarte. Wenn ich ein PDF Dokument unterschreibe, mache ich das, Entschuldigung, mit einer österreichischen qualifizierten Signatur, die ich bekommen habe, weil die täglich funktioniert. Alles andere habe ich probiert. Aber ich laufe hier nicht mit einem Lesegerät für 70 € herum. Wenn Sie weiterschauen, dann ist Estland auch ein Land, das keine Industrie hat und die Technologie nimmt, die vorhanden ist, am besten amerikanische. Wenn es um Irland geht, dann nehmen die auch am besten amerikanische Technologie. Sie haben die Firmen extra angelockt und wollen nicht, dass man sie stört.

Eine polnische Regierung sagt auch, dass sie die Amerikaner nehmen. Wenn ich jetzt die Sache wirklich einmal sarkastisch anschaue, Oettinger ist Kommissar für die digitale Agenda, Schulz Parlamentspräsident und Schäuble tritt dann auf, wenn es in der Finanzkrise ist. Das sind für manche in Brüssel verdammt viele Deutsche. Das darf man nicht vergessen. Wir haben auf der anderen Seite Einfluss, aber wir werden manchmal auch anders gesehen, als wir das hier glauben. Das ein bisschen zur Einstimmung.

Jetzt etwas technischer. Wir hatten die Datenschutzgrundverordnung, die Altersverordnung erwähnt. Die Frage ist, ob das so kommt, wie wir uns das vorstellen. Wir haben zwei Dinge in unserem Metier. Das ist Verschlüsselung und qualifizierte Signaturen. Das sind die Dinge, wie ich vorhin sagte, wir gar nicht zum Fliegen bekommen. Ich möchte gleich noch etwas zu dem Thema sagen, was wir mit Herrn Siegel vorbereitet hatten zum Thema „Internet of Things“ und was auch hier in Regulierung hineinpasst. Aber zuvor noch etwas zum Thema Fortschritt und Technik. Ich hatte die Gelegenheit zum Googeln, Herr Schönbohm, weil Sie hier die Fragen zur Schlüsseltechnologie gestellt bekommen haben. Wenn man das liest, ist das ein Witz, ich sage es ganz offen. Auf der Seite vom Wirtschaftsministerium steht als Schlüsseltechnologie Biotechnologie, Elektromobilität, Forschung, IKT, Luftfahrttechnologie und am Ende steht sogar noch so etwas wie Raumfahrt. Eine Raumfahrtnation werden wir bestimmt nicht. Und IKT als Antwort wird hier bestimmt nicht erwartet. Auf dem Level sind Schlüsseltechnologien der Regierung definiert. Das ist nicht das, worüber wir hier reden wollen. Wir reden über andere Dinge.

Aber wenn wir von Fortschritt reden. Ich habe vor kurzem einen Spiegelartikel gelesen, der darüber berichtet hat, wie Technologien jetzt bei Industrie 4.0 Menschen arbeitslos machen. In einem Vortrag habe ich einmal gesehen, dass der gleiche Spiegelartikel mit dem gleichen Thema – nur das Roboterbild war anders – aus dem Jahre 1978 stammte. 40 Jahre – damals von der Spiegel Computerredaktion. Dann fiel mir ein, dass ich 1977 gelernt habe, also auch fast 40 Jahre im Geschäft bin. Wir müssen uns zwischendurch auch einmal fragen wie wir mit solchen Technologien umgehen und welche Risiken wir da haben. Wenn wir Internet of Things nehmen, reden wir z.B. über Hausautomation. Wenn Sie sich das seit einem Jahr anschauen, dann gibt es Firmen, angefangen von Telekom, RWE oder anderen, die das anbieten, Bosch auch. Alles, was dort angeboten wird, sind Cloud Lösungen. Ich habe ein Haus in München, ein Büro auf Kreta, ein Büro in Athen, eine Wohnung auf Kreta und pendle hin und her. Ich habe gedacht, mich einmal damit zu beschäftigen. Das ist ein Nightmare, wenn man da über IT-Sicherheit redet. Wenn man sich anguckt, was da gemacht wird, dann haben wir Messgeräte, Türöffner. Die Frage ist, ob diese Firmen IT-Sicherheit machen.

Ich möchte jetzt nicht tiefer in IT-Sicherheit gehen, weil ich auch in das Thema Privatsphäre gehen möchte. Was passiert denn heute in anderen Bereichen? Wenn wir heute Car to go oder Carsharing nehmen, werden unsere Daten aufgezeichnet. Die dürfen nicht verknüpft, nicht benutzt werden, aber es hat einen Fall gegeben, wo jemand in einen schweren Verkehrsunfall verwickelt war und die Polizei dann von dem Betreiber die Daten bekommen hat. Das heißt, die Daten sind da. Dann besteht die Frage, wer sie langfristig kontrolliert, nicht die nächsten drei Jahre sondern die nächsten 50 oder 100 Jahre. Sie werden ja heute erhoben. Wenn Sie darüber reden, dass Sie im Auto Sensoren haben, die Ihr Fahrverhalten verfolgen, dann ist es einfach, ein Versicherungsmodell zu haben und zu sagen, dass Sie die Versicherungsprämie halbieren, wenn Sie Ihnen die Daten geben. Das werden die Leute machen.

Im Gesundheitswesen gibt es genügend Dinge – wir waren letzte Woche auf der Ausstellung - , wo man sieht, was heute möglich ist, welche Geschäftsmodelle entstehen. Das ist purer Kapitalismus dahinter, und dann werden die Geschäftsmodelle implementiert. Und wir reden über die Prämierung einer Datenschutzgrundverordnung. Zwischen Wunsch der vielleicht manchmal fundamentalistischen Datenschützer und dem, was betriebswirtschaftlich dann am Ende doch jemand macht, liegen Welten. Die Frage ist jetzt, ob es überhaupt möglich ist, bei dem, was da an Daten erhoben wird, das langfristig zu verfolgen und zu sichern. Wenn Sie

sich das angucken, dann gibt es, hier ein kleines Beispiel, ganz gute Geschäftsmodelle. Es gibt eine App, die Visitenkarten fotografiert. Das ist ein einfaches Ding. Wenn sich die AGBs diese App anschauen, dann steht da drin: Sie haben die Einwilligung desjenigen, dessen Visitenkarte Sie gerade fotografiert haben. Sie haben eingewilligt, dass diese Daten beliebig weiter verwertet werden können. Dann wundern Sie sich, wenn Sie den Verkehr nachverfolgen, dass die Server, wo die Daten abgelegt werden, überall in der Welt stehen. In China, Europa, Russland und den USA. Sie haben keine Kontrolle mehr darüber, wenn Sie Ihre Visitenkarte geben, was derjenige damit macht. Das gilt für alle Beispiele, die kommen. Wenn wir uns in dieser schönen neuen Welt bewegen, werden Daten von uns freiwillig gesammelt, weil wir einen Vorteil davon haben. Sie werden weiter verwertet. Die Frage ist dann, ob es Möglichkeiten gibt, wie man sie technologisch schützen kann, dass ich noch ein Selbstbestimmungsrecht habe. Darüber kann man auch lange philosophisch reden. Aber die Frage ist, ob das überhaupt möglich und gewollt ist.

Ich gebe Ihnen ein anderes Bild, was ich glaube, was heute geschieht. Sie alle, wenn Sie zuhause Erdbeeren oder Tomaten anbauen, pflegen Ihre Pflanzen und ernten Tomaten und Erdbeeren. Was machen die Googels, Amazonas, Tencents und Alibaba? Die pflegen uns, ernten unsere Daten und machen mit den Daten selber noch Geld. Farming Data ist eigentlich ein englischer Begriff dafür, den man dafür einführen sollte, d.h. wir werden zum Gut dieser Konzerne. Wenn Sie sich das weltweit anschauen, erwähnte Cloud Lösung, sitzen diese Firmen außerhalb Europas. Wir haben dem in Europa in dem Sinne auf der globalen Ebene kaum etwas entgegenzusetzen.

Jetzt ist die Frage, was wir dort machen. Was kann man mit Gesetzen machen? Was kann man freiwillig machen? Wir haben die NIS Direktive (?), Herr Staatssekretär hat sie erwähnt. Wir haben die Datenstromverordnung. Aber die Frage ist schon, wie war das in der Diskussion mit Google, dem Recht auf Vergessen. Wie weit das umsetzbar oder durchsetzbar ist oder umgangen wird? Damit haben wir alle unsere Erfahrungen. In der Regulierung beschäftigen wir uns mit der Frage, wo wir sie brauchen. Dann gibt es für mich eine interessante Parallele. Wir haben Regulierung in vielen anderen Bereichen und nehmen die auch historisch hin. Wenn Sie das zeitlich sehen, haben wir Förderglobalisierung und Förderprivatisierung. Autos, Züge, Flugzeuge – alles ist reguliert. Wenn wir Dinge importieren haben wir das CE Siegel. Wir haben Prüfung, Audit – alles reguliert. Wenn wir in

unseren Bereich gucken, beginnen wir gerade erst mit der Regulierung. Und wir haben schon die Diskussion, ob das zu viel oder zu wenig ist.

Die jetzige Kommission ist im Amt bis Ende 2019. Bis dahin hat sich der zuständige Kommissar Herr Oettinger auch noch etwas vorgenommen. Das ist noch mehr als die halbe Legislaturperiode, und wir wollen richtig etwas tun. Was wird auf der Ebene gerade gemacht? Das Telekommunikationsgesetz wird novelliert. Sie werden es der Presse entnehmen: Netzneutralität, Copyright. Wir machen ein Telemediengesetz. Das sind Dinge, die gerade in dem Brüsseler Prozess, in den parlamentarischen Ratsprozess gehen. Und das sind Dinge, die auf europäischer Ebene zwischen zwei und drei Jahren brauchen. Aber wir sitzen auch genauso fleißig wie Sie hier in Deutschland und überlegen, was wir noch machen sollen. Warum haben wir z.B. keine Haftungsregelung im Softwarebereich? Warum kann jede Garage Software auf den Markt bringen? Aber wenn Sie irgendein Bauteil bei ZF bauen und einbringen, haben Sie einen Qualitätsprozess. Sie haben Supply Chain, alles Mögliche. Wir haben keine Supply Chain für Software. Das ist ein Thema, was angefangen wird zu diskutieren.

Eine andere Frage ist und da komme zurück auf die Frage von Heinz Thielmann, was europäisch mit ENISA geschehen soll. Wir starten gerade die Diskussion, wie das Gesetz novelliert werden soll. Die Kommission wird nächstes Jahr im Herbst mit einem Vorschlag herauskommen. Die Frage ist dann, wie es weiterentwickelt werden soll, welche Aufgaben ENISA bekommen soll und in welchem Spannungsfeld es mit den anderen Mitgliedsstaaten bestehen soll. Das heißt, dass wir auf dieser Ebene wir über ein allgemeines Gesetzesvorhaben nachdenken. Europäisch gibt es immer zwei Möglichkeiten, entweder eine Regulierung wie die Datenschutzgrundverordnung, die dann 1:1 in allen Mitgliedsstatten umgesetzt wird, damit es harmonisiert wird, oder die NIS-Direktive, die den Rahmen gibt und in jedem Land in nationales Gesetz umgesetzt wird. Bei der NIS-Direktive kann es beispielsweise passieren, wenn es schlecht läuft, dass wir verschiedene Schwellwerte für Gerichtswesen haben. Das versuchen wir zu verhindern, aber das ist etwas, wo dann diese einzelnen Schwellwerte schon bei den Unternehmen mit dabei sind, die das IT-Sicherheitsgesetz haben. Da ist die Frage europäisch.

Ich mache einen Schwenk, weil hier jemand aus der Wasserwirtschaft und Energiewirtschaft ist. Wir hatten am vergangenen Dienstag unsere Verwaltungsrat Sitzung, wo Vertreter aus

allen Mitgliedsländern sitzen, für Deutschland ist das der Präsident Schönbohm. Die Sektoren kennen Sie. Man hat dann gesagt, wir priorisieren. Wasser ist kein Thema auf europäischer Ebene für uns. Es steht zwar in dem Gesetz drin, aber wir beschäftigen uns nicht damit. Dafür haben wir keine Ressourcen bekommen und machen es deshalb nicht. Das ist eine politische Entscheidung und ich will den Bogen zu dem Thema Risikomanagement spannen. In dem Sinne ist es eine politische Entscheidung, welches Risiko man eingehen will. Ich vergleiche das immer sehr gern mit den Kollegen vom BKA, wo Sie sagen, wie viele Polizisten Sie am Flughafen brauchen. Wenn nichts passiert, sind es zu viele, wenn etwas passiert, sind es zu wenige. Sie müssen eine politische Entscheidungen treffen und sagen, was Sie da investieren. Sie können sarkastisch sagen, Europa leistet sich 11 Million für IT-Sicherheit. Das ist genau unser Budget, das Risikobudget, was die Politik investiert. Wir haben ein europäisches CERT, was Herr Schönbohm erwähnte. Das ist vor vier Jahren installiert worden, weil einige Mitgliedsstaaten den Kommissaren gesagt haben, dass es ohne europäisches CERT Probleme gibt, wenn was passiert und sie seien Kommissare. Dann gab es ein europäisches CERT. Das ist europäisches Risikomanagement, politisches Risikomanagement. Das heißt, Gesetze oder Handlungen sind politisch definiert.

Ich will Ihnen noch ein Beispiel geben, weil das wahrscheinlich zu wenig bekannt ist. Es lohnt sich manchmal, Gesetze zu lesen. Es lohnt sich auch manchmal, den Lissabon-Vertrag zu lesen. Der Lissabon-Vertrag hat nur noch eine Handvoll Themen nationaler Souveränität hat. Das ist z.B. Finanzpolitik, Verteidigungspolitik, Geheimdienste. Finanzpolitik, weil es auch aus deutschem Interesse ein Instrument ist, was sich die deutsche Regierung nicht aus der Hand nehmen lassen will. Wir machen Politik über Finanzpolitik. Wir machen Förderung, Abschreibungen, was auch immer. Geheimdienste – nach Snowdon wissen wir, dass wir uns alle gegenseitig bespitzeln -, also wird es niemals einen europäischen Geheimdienst auf absehbare Zeit geben. In unserem Geschäft wissen wir, ob das Cyber War, Cyber Espionage, Cyber Sabotage, Cyber Crime ist, dass das alles der gleiche Faktor sein kann. Wir trennen das aber fein säuberlich.

Zur Verteidigung haben wir die NATO. Wir haben eine kleine European Defence Agency, die aber nur Studien macht. Einer kleiner Schlenker, weil ich noch eine Honorarprofessur an der Bundeswehruniversität habe. Für uns ist das ein Traum, elf neue Professuren, 70 neue Stellen, 70 Millionen kriegen wir. Wir bekommen ein schönes Gebäude hingesetzt. Wir kämpfen gerade im Großraum München mit allen möglichen anderen Instituten. Der Verfassungsschutz

baut auf. Das heißt, überall wird aufgebaut mit den Stellen, und wir kämpfen alle um die gleichen Leute. Aber es zeigt auch, dass die Bundeswehr da anders denkt, weil es zunächst einmal ein anderer Strang ist als der zivile Strang.

Vielleicht noch etwas. Wenn ich dort in meiner Eigenschaft als Honorarprofessor Studenten ausbilde, Soldaten ausbilde und wir haben jetzt einen Cyberstrang bei der Bundeswehr – ich erwähne das nur deshalb, weil wir es gerade angesprochen haben – worin bilde ich dann die Soldaten aus? Wer war bei der Bundeswehr? Wenn Sie Verteidigung machen, werden Sie auch angegriffen, vielleicht auch mit der Waffe zu schießen. Soll ich das meine Studenten auch lehren?

Ich weiß nicht, wieweit Leute manchmal denken. Aber, ich glaube, viele haben noch nicht darüber nachgedacht, was das zukünftig für die Ausbildung unserer Soldaten bedeutet. Wenn ich noch einmal zu dem eigentlichen Thema zurückkomme, was ich Ihnen so als Bogen sagen wollte, auch aufgrund dessen, was gesagt wurde, haben wir auf der einen Seite das Thema Internet of Things. Das Thema Internet of Things, wie auch immer Sie das Andocken, ob Sie das mit Cyber Physical Systems in Industrie 4.0 reinbringen, ob Sie das in Home Automation bringen, ob Sie das in Gesundheitssensoren bringen, egal wo, werden Sie überall Chips haben, die Daten sammeln, Daten verteilen, in Cloud Lösungen haben. Und Sie werden diese Daten nach heutigem Ermessen kurzfristig nicht schützen und verfolgen können. Es gibt Ansätze, wo wir investieren müssen, wo man so etwas über den Lebenszyklus der Daten vielleicht doch schützen kann.

Die Frage ist dann, was man durch Regulierung erreichen kann. Was ich mit diesen kurzen Schnappschüssen sagen wollte, ist: Denken Sie daran, dass Vieles in Brüssel diskutiert wird, dass wir als Deutsche da nicht gut vertreten sind im logistischen System und dass eine ganze Reihe von Dingen sich in dem Umfeld abspielt, zu sagen, was ich tun will, um meiner staatlichen Verantwortung, dem Schutz der Bürger, gerecht zu werden. Oder was will ich tun, weil es vorher in der Selbstverpflichtung nicht funktioniert hat? Oder was ist auch Lobbyismus, wenn manchmal auch Lobbyisten bestimmte Gesetze haben wollen? Und das vielleicht einfach nur als Food for Thought für die nächsten Diskussionen. Dankeschön.

Prof. Eckert:
Ganz herzlichen Dank, Udo Helmbrecht auch für die Gedanken im Vergleich mit Estland, durchaus interessant. Haben Sie direkte Fragen!

NN:
Herr Helmbrecht, wir kennen Sie gut. Aber ich bin sehr enttäuscht. Außer Sarkasmen haben wir eigentlich nicht viel gehört. Und ein bisschen etwas Positives oder Vorschläge, was man tun sollte. Denn wenn ich jetzt ein Bürger wäre, würde ich sagen, der Einrichtung, der Sie vorstehen, brauchen wir wahrscheinlich gar nicht, denn es ist eh sinnlos. Sie haben selber angefangen mit ein bisschen Provozieren. Deswegen musste ich das jetzt sagen. Frage habe ich keine.

Prof. Helmbrecht:
Sie haben da durchaus Recht, weil die Frage ist, dass wir gute viele Ideen haben. Das Problem ist nur, wenn ich jetzt hier 20 Folien vorlege und sage: das ist das, was die ENISA tut und welche Empfehlung wir machen, dann lebe ich auch in sieben Jahren auf europäischer Bühne. Wer von Ihnen liest unsere Empfehlungen? Wer von Ihnen liest die BSI Empfehlungen? Da gehen aber nicht alle Hände hoch. Ich erinnere mich noch, als ich 2013 zum BSI ging – meine Stammtischfreunde kannten das BSI nicht bis auf einen der bei Eurocopter arbeitete und sagte, jetzt wisse er endlich, wer immer der Verhinderer bei Abstrahlmessungen ist.

Und wenn Sie auf europäischer Ebene sind und feststellen, dass es vier Jahre für die Datenschutzverordnung braucht, drei Jahre lang die ANES (?) Direktive braucht, dann habe ich Ihnen heute ein bisschen diesen Frustvortrag gehalten, wo ich Ihnen einfach sagen wollte: denken Sie darüber nach, dass die Musik in Brüssel spielt und wir nicht gut vertreten sind. Und das andere ist etwas, wo ich ehrlich gesagt, nicht wiederholen wollte, was Herr Staatssekretär und Herr Schönbohm gesagt haben. Das Problem, was wir heute haben und das man einmal zugeben muss, ist, wenn wir an vielen Stellen Vorträge halten, stellen wir vieles positiv dar, wo wir wissen, dass die Dinge auch nicht funktionieren.

Der Personalausweis funktioniert nicht. Ich sage das hier ganz ehrlich. Wir machen hier gerade ein Projekt über eHealth europäisch. Das ist wirklich abenteuerlich. Es ist wunderbar, den Geschäftsvorteil zu haben, zu sagen, Sie sind im Krankenhaus in Nizza im Urlaub und wollen Ihre Arztrechnung bezahlen. Das funktioniert auch in den nächsten drei Jahren nicht.

Es ist nicht die Technologie. Es sind nicht die Produkte. Das ist so, wie der politische Betrieb funktioniert. Es ist auch nicht das Geld. Wir haben anderthalb Milliarden im Horizon 2020 und machen da IT-Sicherheitsforschung. Wir haben hier PET (?). Ich wusste erst nicht, was das war, was hier drin ist. Es ist das Gleiche. Es ist die Behörde in Budapest, die Geld ausgibt. Das ist auch Geld in Europa. Wir nehmen gerade 500 Millionen Euro in die Hand für eine Public Private Partnership. Wir können uns vorstellen, dass wir noch einmal anderthalb Milliarden von der Industrie einsammeln, um Projekte zu machen. Das sind alles Projekte mit unverhältnismäßig viel Geld auf europäischer Ebene. Wenn wir heute Abend hier sitzen und diskutieren, glaube ich, dass wir mal über so etwas diskutieren und uns fragen, was wir da besser tun können.

Nur ist das Problem, wenn wir heute Abend hier rausgehen, glaube ich nicht, dass wir viele Ideen haben, wie es morgen besser wird. Ich will das jetzt nicht falsch verstanden wissen. Wenn man sich anguckt, was Staatssekretär Vitt vorgetragen hat, sind das alles Erfolgsprojekte und Dinge, die wichtig sind. Ich finde es sehr gut, wenn ich zurückdenke, weil vor fünf Jahren hat auf europäischer Ebene keiner über die IT-Sicherheit gesprochen. Und heute kann man auch mit Herrn Oettinger darüber reden. Vor zehn Jahren hat von unseren Ministern auch kaum jemand über IT-Sicherheit gesprochen. Und wenn Sie gucken, wie oft ein Präsident Schönbohm in Berlin ist und auch mit den Leuten reden kann, war das vor 15 Jahren nicht so. Also, das ist alles positiv. Nur der Weg vor uns, wenn Sie diese tagtäglichen Zahlen im BSI Lagebericht lesen, dann ist die Frage, ob wir uns manchmal nicht ein bisschen zu viel im Kreise drehen. Wir müssten die Ärmel hochkrempeln, um in die richtige Richtung zu laufen.

Prof. Eckert:
Gut, wir gehen jetzt in die richtige Richtung und machen noch eine Frage und gehen dann zum nächsten Tagesordnungspunkt. Und wir machen eine kurze Frage mit einer ganz kurzen Antwort.

NN:
Als Vertreter aus der Finanzwirtschaft kritische Infrastruktur erleben wir jetzt gerade, dass wir sowohl mal das Sicherheitsgesetz, wir haben verschiedene Regulierungsbehörden, sind stark durchreguliert. Ich will mich darüber nicht beschweren. Jetzt kommt auch noch die EU dazu, macht Sonderprüfungen mit dem Stichwort Cyber-Security. Jetzt einmal eine kurze Frage.

Werden Sie da konsultiert beispielsweise durch die EWA EZB (?)? Wird die Fachexpertise, die trotz allem bei Ihnen vorhanden ist – ich war vorher auch woanders unterwegs und kenne deswegen ein bisschen Ihre Einrichtung – in Anspruch genommen? Gibt es da einen Austausch oder muss ich den Eindruck weiter mit mir tragen, dass die sich das von Wirtschaftsprüfern auf diktieren lassen? Und ich kenne die Fragebögen eigentlich schon, und da wird ohne Sachverstand reguliert.

Prof. Helmbrecht:

Das kommt darauf an. Wir haben Sektoren, wo der Austausch gut funktioniert. Das ist im Telekommunikationsbereich. Das ist im Finanzbereich. Das ist ein bisschen im Energiebereich, aber meistens im Telekom- und Finanzbereich. Wenn Sie das in Brüssel auch anschauen. Da, wo wir oft involviert sind, gibt es einen Ausschuss, der SiTra Ausschuss, der im Wesentlichen ein Telekommunikationsausschuss ist. Und es gibt im Rat eine Arbeitsgruppe. Das ist der Telekommunikationsausschuss. Das heißt, wenn Sie sich europäisch IT-Sicherheit anschauen, wird das historisch in erster Linie aus dem Thema Telekom betrachtet. Das ist auch in unserem Namen drin, dass wir eben Infrastruktursicherheit heißen, Network and Information Security. Über die, wie ich sagte, Secondary Legislation, und über die Gesetze, wie ANES Direktive kommen dann andere Sektoren dazu. Aber es ist eben mehr oder weniger ausgeprägt, wie ich sagte, manche Teile sind nicht dabei und andere intensiver. Wenn wir dann Legislative implementieren, heißt das, dass wir dann mit diesen europäischen oder mitgliedsstaatlichen Behörden zusammenarbeiten. Aber ganz konkret, neben dem BSI ist das in Deutschland die Bundesnetzagentur, einfach aus dem Stichwort, aber dann erst in nächster Linie mit dem Finanzsektor. Das ist nicht sehr intensiv, aber das gibt es vielleicht nicht so, wie Sie es wünschen würden. Aber es ist auch nicht null.

Prof. Eckert:

Gut, Vertiefung gleich nach einer Pause. Ganz herzlichen Dank, Udo Helmbrecht.

Panel
Mit den Keynote-Referenten und Impuls-Referenten
Michael Barth, genua GmbH, Berlin
Dr. Alexander Duisberg, Bird & Bird LLP, München
Prof. Dr. Claudia Eckert, Fraunhofer-Institut AIESEC, München und TU München
Matthias Kammer, DIVSI, Hamburg
Dr. Jürgen Sturm, ZF Friedrichshafen AG, Friedrichshafen

Prof. Eckert:

Wir wollen einen Teil des nächsten Panels noch anstoßen, und zwar haben wir jetzt schon unterschiedliche Sichten gesehen. Was wir noch nicht ganz im Fokus hatten, war die gesellschaftliche Sicht, die von Matthias Kammer vertreten wird und der als Geschäftsführer des DIVSI ein paar andere Aspekte hineinbringen und uns seine Perspektiven darstellen wird. Ich hätte dann gern noch die juristische Sicht dargelegt. Das ergibt ein schönes Portfolio. Nach der Pause werden wir dann mit den technischen Fragestellungen aus Anbieter- und Anwendersicht weiterzumachen. Matthias, darf ich Dich bitten, ein paar Gedanken, ich nehme an, zur DIVSI Studie zu äußern?

Herr Kammer:

Liebe Claudia Eckert. Ich bedanke mich ganz herzlich für die Einladung. DIVSI ist das Deutsche Institut für Vertrauen und Sicherheit im Internet, eine Gründung der Deutschen Post. Uns gibt es seit 2011. Im Kern ist unser Interesse die Frage, wie es den Menschen in Deutschland in der digitalen Zeit geht. Über die Erkenntnisse, die wir da gewonnen haben, stellen sich dann alle möglichen Überbaufragen. Ich will aber erst einmal über einige Daten berichten aus einer aktuellen Studie, die wir im Frühjahr veröffentlicht haben. Die zweite DIVSI Internet Milieustudie, die die deutsche Gesellschaft ab 14 betrachtet und in sieben Perspektiven, in sieben Milieus differenziert untersucht. Nicht alle Menschen sind gleich, nur weil sie an der digitalen Welt teilnehmen, sondern da gibt es sehr viele Unterschiede. Heute will ich mich konzentrieren auf die Kernüberschriften, die auch die meisten gemeinsam haben.

Nach unserer Studie haben wir es in diesem Land noch mit Offlinern zu tun. Das ist jeder sechste. Das war vor vier Jahren noch viel, viel mehr. In dem Sinne hat sich sehr viel verändert. Generelle Beobachtungen sind, dass das Internet in der Mitte der Gesellschaft

angekommen ist. 61% können sich ein Leben ohne Internet nicht mehr vorstellen. Das ist um 10% gestiegen in vier Jahren.
Die große Mehrheit sieht mehr Chancen als Risiken. 7^2% sehen Chancen vorn und Risiken kommen dann. Wenn man so will, ist doch ein sehr ausgeprägter Internetoptimismus festzustellen. Warum? Es macht das Leben im Alltag einfach leichter, und das wissen wir alle auch. Es ist nicht so, dass das nur eine Erfindung oder Wahrnehmung der Menschen da draußen wäre, sondern wir nutzen es auch, weil es uns das Leben erleichtert. Daher erkläre ich mir auch sehr deutlich, warum die Chancen so weit vorne stehen. Was Sicherheit angeht, gibt es nach unserer Beobachtung mittlerweile eher eine pragmatisch fatalistische Haltung, weil Sicherheit eben nicht erreichbar ist. Das Leben geht aber weiter und deshalb sind die Chancen vorne. Da sehe ich in der Tat eine große Herausforderung, damit umzugehen, wenn man sich fachlich mit diesen Fragen beschäftigt. Das kann man von der Bevölkerung im weitesten Sinne nicht verlangen. Was sind für Konsequenzen festzustellen, wenn es um Gefahrenwahrnehmung geht? 64% sind der Meinung, dass man sich wohl an einen freieren Umgang mit Daten gewöhnen muss. 36% sehen das eher zurückhaltend, aus Sorge Fehler zu machen, und versuchen sich danach zu organisieren.

Claudia Eckert hat vorhin einen Ausschnitt aus einem zentralen Punkt genannt, nämlich die Frage, was für eine Verantwortungsphilosophie wir in solchen Untersuchungen in der Bevölkerung feststellen können. Du hattest den Ausschnitt Staat, zu dem ich gleich komme. Vorn steht eine für mich überraschende Veränderung gegenüber dem, was wir vor vier Jahren hatten. 82% der Befragten haben gesagt, dass Sie zunächst sich selbst in der Verantwortung sehen. Das ist ein Absprungpunkt für Diskussionen über eine aufgeklärte Frage, wie man mit Sicherheitsfragen umgeht, den ich so nicht erwartet hatte. Also, die meisten sehen sich zunächst einmal selbst in der Verantwortung. Aber gleichzeitig wissen sie natürlich auch, dass sie mit dieser Verantwortung allein völlig in der Wüste verloren sind. Deswegen gibt es eine Erwartung an den Staat, für Sicherheit zu sorgen, 66% sagen das, trauen es ihm aber nicht zu. Das ist, wie ich finde, eine zentrale Vertrauenskrise, die man an diesem Punkt festmachen kann. Ich will ein Beispiel nennen, was pars pro toto stehen mag. Warum, haben wir in den qualifizierenden Teilen, die wir vorweg befragt hatten, als ein Beispiel gefunden. Wenn das eigentlich für die Bevölkerung oberste Organ, der Deutsche Bundestag, so gehackt werden konnte, wie das geschehen ist, dann mögen die Fachleute sagen, dass das kein typisches Beispiel für den Staat ist. Aber für die Bevölkerung ist es das oberste Organ. Und wenn sie

das schon nicht hinkriegen, wieso sollen sie eigentlich für Sicherheit sorgen können? Ich finde das plausibel als einen Befund, mit dem man umgehen muss.
88% verlangen von der Wirtschaft mehr Datenschutz. Aber auch hier, allein es fehlt der Glaube. Ein ganz symptomatischer Satz: Ich erwarte, wenn ich irgendwo in irgendeiner Form registrierter Kunde bin, dass mit meinen Daten vertraulich umgegangen wird. Aber ich bin sicher, dass es nicht so ist.

Ein weiterer Teil, der etwas mit diesem Punkt zu tun hat, ist, ob es das Leben leichter macht. Das ist eine schwierige Frage im Kontext von Sicherheit. Schneller, leichter, einfacher sind eigentlich die Grunderwartungen an die Dienstleistungen, die in der digitalen Zeit geboten werden und die, die sich in diesem Kontext bewegen, sind auch erfolgreich am Markt. Schneller, leichter, einfacher. Alles, was kompliziert ist und deswegen nach Sicherheit riecht, wird weggeschaltet. Convenience gewinnt immer über Sicherheit. Das ist, wie ich finde, eine Riesenherausforderung für technische Gestaltung, wie man Convenience und Sicherheit zusammenkriegen kann. An ein paar Ecken wird es wahrscheinlich auch einer harten Regulierung bedürfen, wenn man an dieser Stelle durchsetzen will, dass ein bestimmter Sicherheitslevel in der IT Welt irgendwann Platz hält und sich auch alle daran gewöhnen, so wie wir das auch vom Autofahren und sonst woher kennen. Im Moment ist das eher noch freie Wildbahn.

Die Lebenswirklichkeit von Menschen verzieht sich dann an vielen Ecken in Paradoxien. In der Snowden Geschichte haben wir in mehreren Befragungen festgestellt, dass die Bevölkerung überwiegend, also diejenigen, die es richtig finden, dass Geheimdienste den Terroristen auf der Spur sind, fanden das in Ordnung. Das waren ca. 30 bis 35%, wenn ich das so richtig im Kopf habe. Andere haben deutlich gesagt, dass es ein Angriff auf die Verfassung ist und unerhört ist, dass wir abgehört werden. Wo kommt das hin und wo soll das enden? Wenn man fragt, was das für dein persönliches Verhalten für Konsequenzen hat? Keine, kein Telefonierverhalten geändert und nichts. Das heißt, eine klare Haltung gegenüber einem bestimmten Vorgang führt nicht dazu, dass ich in meinem Leben Alltagsverhalten so ändere und es mir dadurch auch noch unbequemer mache.

Freierer Umgang mit Daten hatte ich vorhin genannt. 64% sagen, dass wir uns daran gewöhnen müssen, bemerken aber gleichzeitig: bitte, nicht mit meinen Daten. 80% ist das Ranking der Daten, die nicht frei zur Verfügung stehen dürfen. Das liegt zwischen 70 und

80%. Da geht es um Bankdaten, Fotos, Familieninformationen. Das bitte alles nicht frei verfügbar. Aus der individuellen Sicht derjenigen, die gleichzeitig die Erkenntnis haben, dass wir uns wohl an diesen freieren Umgang gewöhnen müssen. Ein Widerspruch, der typisch ist für die Paradoxien in der digitalen Zeit. 80% wissen - das hat mich überrascht, dass es so hoch ist -, dass sie bei kostenloser Nutzung eines Dienstes mit ihren Daten zahlen. Gleichzeitig fordern aber noch mehr, dass der Staat solche Geschäftsmodelle verbieten möge. Was bedeutet das? Es sind schon einige Sachen hier angeklungen. Dazu will ich kommentierend gar nichts sagen, glaube aber, dass wir in einer Ramp-up Phase eines großen Umbruchs leben, den wir in vielerlei Hinsicht beobachten können. Wir haben in einer unserer zentralen Thesen, unserer Mission wenn man so will, stehen, dass das Internet eine herausragende Kulturleistung der Menschheit ist, weil es um vielmehr geht als nur um Techi- Fragen, sondern es verändert unser Zusammenleben, es verändert Wertesysteme. Wir haben in einer Jugendstudie festgestellt, dass junge Leute, wenn sie in einem Laden eine CD mitnehmen, an der Kasse sehr wohl wissen, dass das Diebstahl ist. Aber vergleichbares Verhalten in der digitalen Welt macht man ja so und da gibt es nichts. Und da funktionieren im Moment auch unsere gesamten staatlichen Infrastrukturen, die wir haben, die sich eigentlich in der Strafverfolgung tummeln, nicht so gut wie in der analogen Welt. Da haben wir noch riesige Herausforderungen und Wertevorstellungen, die wir bisher hatten, durchzusetzen.

Ich glaube, dass wir einen breiten gesellschaftlichen Diskurs brauchen, an dem viele teilnehmen sollten und auch Leadership zeigen sollte, und wo es um die Frage geht, wie wir in der digitalen Zeit zusammenleben wollen. Was sollen eigentlich die Kernelemente unserer Werteordnung sein? Vielleicht müssen wir einen neunen Gesellschaftsvertrag aushandeln im Rousseauschen Sinne. Das kann sehr wohl sein.

Unser Schirmherr ist Altbundespräsident Roman Herzog, der zu diesem Punkt immer herausarbeitet, dass selbst die in unserem Grundgesetz vorn stehenden 20 Artikel, die unsere Werteordnung wiedergeben, müssen nicht unbedingt in Stein gemeißelt sein. Es sind Verfassungsrechtler und wir alle leben mit diesem Ewigkeitsgedanken, der an vielen Stellen darin steckt. Aber es können da sehr wohl Werte verändern. Eine Leitplanke sollte dabei gelten, und zwar, dass die Würde des Menschen im Kern unantastbar bleibt. Das zu untersuchen im Kontext von Geschäftsmodellen, die wir heute schon kennen und wenn es darum geht, was mit meinen Daten geschieht, welche Bedeutung haben eigentlich Daten für die Einzelnen haben? Das scheint transparent zu sein, und hier wünschte ich mir sehr, dass

wir eine Diskussion darüber führen, wem die Daten gehören, was in dem Kontext Privatheit ist, wenn sich Menschen so völlig widersprüchlich verhalten, wie ich es beschrieben habe. Welche Regeln wollen wir da haben? Was nützt uns der Grundsatz der Datensparsamkeit, wenn es keinen Menschen interessiert? Ist das eigentlich ein richtiges Steuerungsinstrument und für was?

Solche Diskussionen führen wir nicht ausreichend, sondern das sind unterschiedliche Abteilungen, die mit sich diskutieren. Ich wünsche mir sehr, dass Datenschutz nicht ein Privileg in Diskussionskreisen der Datenschutzbeauftragten bleibt. Das bringt uns überhaupt nicht weiter. Wir brauchen einen viel breiteren Diskurs und eine Auseinandersetzung darüber, was Privatheit ist, was meine digitale Identität ist. Wer will ich eigentlich sein in dieser digitalen Welt? Da wünschte ich mir schon, dass so ein Zusammenwachsen von technischer Gestaltung. gesellschaftlicher Entwicklung hier deutlicher wird, als wir es bisher haben. Das steht mir zu sehr nebeneinander. Deswegen wollte ich gern mit diesen Zahlen, die ich aus einer Studie mitgebracht habe, meinen Eindruck von dem mitbringen, in was für einem Status die deutsche Bevölkerung in Gänze zurzeit ist. Wir haben in zwei Studien die jüngere Generation untersucht, die 9- bis 24jährigen und die Kinder von drei bis acht. Jedes zehnte dreijährige Kind ist online. Die Diskussion, ob das gesund oder krank ist, ist eigentlich vorbei. Das findet alles längst statt. 55% der achtjährigen Kinder sind im Internet unterwegs. Ab dem 12., 13. Lebensjahr ist ‘always online‘ ein Lebensgefühl, das umgekehrt so beschrieben kann, wenn es einmal ausfällt, ist das eine Notsituation, in der man sich dann wiederfindet.

Wir werden Ende Oktober eine Studie vorstellen über die Generation Ü60 und Ihnen darin auch zeigen, dass in der Tat auch in dieser Generation längst nicht nur verschlafene alte Menschen wären sondern hoch digitale Performer. Aber dort konzentriert sich der Teil derjenigen, die offline sind und wahrscheinlich abgehängt werden. Vielen Dank für die Aufmerksamkeit.

Prof. Eckert:
Danke. Wir werden nachher gleich weiterdiskutieren, aber vielleicht ganz spontane Wortmeldungen zu den Ausführungen?

NN:

Ich bin eigentlich systemfremd hier, weil ich aus der Energiewirtschaft komme. Ich bin Anwältin im Energierecht, wo die Sicherheit auch eine Rolle spielt. Ich habe jetzt eher eine andere Frage an Sie, weil Sie das mit der Menschenwürde angesprochen haben. Die Frage, die ich mir stelle ist, unabhängig von dem Datensammeln, eher in die Richtung, was mit den Daten gemacht wird. Wie ändert das unser Menschenbild? Stichwort: welche Rolle räumen wir Algorithmen ein, die wiederum so künstliche Identitäten schaffen, die wiederum Entscheidungsgrundlagen in vielerlei Hinsicht schaffen? Ist das auch Gegenstand Ihrer Untersuchungen? Beschäftigen Sie sich auch vertieft damit? Können Sie etwas dazu sagen oder?

Herr Kammer:

Der erste spannende Punkt, der mich beschäftigt, wenn Sie eine solche Frage stellen, ist, dass ich ganz sicher bin, dass die breite Mehrheit der Bevölkerung keine Vorstellung von Algorithmenwirkungen hat, aber den Nutzen genießt. Das ist erst einmal der Punkt und darum bin ich dafür, dass wir auch so eine Diskussion führen, denn Algorithmen leben davon, dass man ihnen Daten gibt. Sonst können sie nichts machen. Die liefern wir alle und damit lassen sich dann eine Menge schöne Sachen herstellen und wahrscheinlich auch vieles, was der Mensch, der seine Daten abgibt, im Ergebnis selbst gar nicht will. Die Diskussion darüber zu führen in einem Land wie unserem, das eine freiheitliche Geschichte hat, wo sich die Frage stellt, ob uns künftig Algorithmen regieren im wahrsten Sinne des Wortes, finde ich eine Diskussion, die man konsequent führen muss, weil sich dann auch die Frage stellt, wer noch wofür Verantwortung hat. Wen wähle ich eigentlich?

Wir werden zu Weihnachten ein Buch herausbringen, in dem wir die Frage gestellt haben, ob das Grundgesetz noch tauglich ist für die digitale Zeit. Wir haben uns in zwei Büchern mit den Grundrechten und der Funktion der Schutzwirkung der Grundrechte beschäftigt. Im dritten Buch geht es jetzt um das Demokratieprinzip, also repräsentative Demokratie. Wir wählen und was bedeutet das eigentlich in der digitalen Zeit, wenn sich auch die Frage, wer ein Abgeordneter ist, in diesem Bild verändert? Hat der eigentlich für irgendetwas noch Verantwortung? Was ist eigentlich die ministerielle Verantwortung im Verhältnis zu all dem, was in der digitalen Welt wo läuft und wo man gar nicht weiß, wie es genau funktioniert, wenn man eine Spitzenverantwortung trägt. Das ist eine immense Herausforderung, die da vor uns liegt.

Mit Blockchain wird es noch spannender, weil wir uns nun endgültig verabschiedet haben von der Möglichkeit, das zu verstehen und als normaler Mensch erst recht. Da brauchen wir wirklich Plattformen, wo wir uns richtig als Bürger und Bürgerinnen dieses Landes einmischen und sagen, was wir wollen. Damit, wer auch immer sich dann hinterher damit auseinandersetzen muss, erst einmal hört, dass es Menschen gibt, die dazu wenigstens eine Frage, Anmerkung oder Sichtweise haben.

NN:

Ich bin Ihnen unheimlich dankbar für diesen Vortrag und für diese Gedanken, weil die ganze technische Diskussion um die Vernetzung sich eigentlich immer wieder um Details dreht, die gar nicht relevant sind. Relevant ist wirklich, wie wir die Gesellschaft im Rahmen einer Neuvernetzung transformieren. Das betrifft jeden Bereich der Gesellschaft. Wir versuchen im Moment mit der Pyramidenbetriebsordnung von Ramses II. die neue Welt zu gestalten. Die Frage nach der Verfassung ist wirklich berechtigt. Es ist lustig; ich habe gerade in diesem Punkt der Ministerin Hendricks vorgeschlagen, wenn sie schon einmal dabei ist, die Verfassung zu ändern, um sozialen Wohnraum zu schaffen, dann sollte sie sich doch um den Artikel 10 kümmern. Darin steht, dass das Brief-, Post- und Fernmeldegeheimnis gilt. Ich habe vorgeschlagen, sie möge ergänzen, dass das Schalt- und Zustandsgeheimnis gilt, weil alle Leute der Internettechnik glauben, dass für sie das Fernmeldegeheimnis nicht gilt. Das Gleiche gilt für Eigentum. Wir sind nicht Eigentümer des Smartphones. Eigentümer ist der, der den Betrieb bestimmt. Das Gleiche gilt für die Wohnung. Sie ist ein besonders verfassungsrechtlich geschützter Raum nach Artikel 13. Aber wir haben ein Google Open Home und die Gewaltenteilung ist neu gegeben, denn die Schließgewalt ist nicht mehr beim Bewohner sondern bei dem Cyberorganisator.

Herr Kammer.

Etwas karikierend zugespitzt. In diesen Welten, die Sie eben beschrieben haben, finde ich, begeben wir uns zunehmend in eine amerikanische Kolonie.

Prof. Eckert:

Danke erst einmal. Wir werden nachher weiter diskutieren. Ich möchte vor der Pause diesen ersten Bereich noch abrunden mit Herrn Duisberg, Partner Birds & Birds. Er beleuchtet für uns dieses spannende Thema aus einem ganz anderen Blickwinkel, aus der juristischen

Sichtweise, die sicherlich auch sehr spannende und auch sicherlich nicht ganz eindeutige Antworten und vielleicht noch weitere Fragen für uns bereithält.

Dr. Duisberg:
Ganz herzlichen Dank, liebe Frau Eckert. Als Jurist werde ich versuchen, mich kurz, knapp und klar auszudrücken und werde gucken, ob es gelingt. Ich wollte mir eigentlich nur drei Aspekte rausgreifen, die vielleicht hier noch nicht so intensiv beleuchtet worden sind, zum Teil vielleicht schon. Und ich knüpfe an das an, was Herr Schönbohm sagte, dass wir den Mittelstand, die KMUs mitnehmen müssen. Ich möchte Sie jetzt sozusagen auf die Ebene der Sicherheit führen. Wir haben gerade sehr eindrucksvoll das Thema Datenschutz, Privatsphäre und Menschenschutz gehört. Ich ziehe erst einmal einen Bogen zur Sicherheit und komme zum Schluss auch noch einmal auf den Datenschutz.

Zur Mitnahme der KMUs möchte ich Sie auf einen Punkt hinweisen, der, glaube ich, ganz wichtig ist, der die Stellschrauben betrifft, die man sich näher anschauen müsste. Das ist die Frage der Verantwortung der Geschäftsführung in diesen Unternehmen. Es gibt da eine ganz schöne Vorschrift – diejenigen, die juristisch tiefer sind kennen vielleicht den 91 Abs. 2 Aktiengesetz -, die besagt, dass der Vorstand eine Verpflichtung hat, Überwachungssysteme einzurichten, die den Fortbestand der Gesellschaft oder des Unternehmens gefährdende Entwicklungen abwehrt. Das sind sozusagen Frühwarnsysteme. Das kennt man dann in gewissen Ausformungen. Es gibt natürlich Dienstleister, die auch da sehr gut ansetzen. Das könnte vielleicht zu wenig sein. Das könnte vielleicht, wenn wir überlegen, Fortbestand des Unternehmens gefährdend. Das ist die ganz große Nummer. Es geht eigentlich auch in den operativen Betrieb.

Diese aktiengesetzliche Bestimmung regelt die Haftung des Vorstands, aber auch der Geschäftsführer. Das gilt gleichermaßen und ist praktisch ein allgemeiner Leitsatz, der diese Verpflichtung begründet. Ich glaube, man könnte, und das ist jetzt wirklich nur die kleine Feinarbeit des Juristen, diese Stellschraube näher beleuchten, ob das nicht auch ausgedehnt werden muss auf Cyberrisiken, die den operativen Betrieb gefährden. Denn das ist das, was auch Herr Schönbohm sagte über den Geschäftsführer, der meint, dass er seinen IT-Verantwortlichen hat und der muss zusehen, wo er bleibt. Das ändert sich, wenn Sie stärker an die persönliche Haftung des Geschäftsführers anknüpfen. Das ist typischerweise in Organisationsstrukturen das Moment, wo Sie ein Umdenken auslösen.

Das haben wir auch beim Datenschutz gesehen. Wenn Sie die Entwicklung über die vergangenen Jahre beobachten, ein Jahrzehnt zurück, war Datenschutz und Datenschutzbeauftragter jemand, mit dem man nicht so richtig etwas anfangen konnte, aber einer muss es machen. Sie haben über die Jahre gesehen, wie diese Rolle ganz signifikant angestiegen ist in der organisatorischen Verankerung im Unternehmen. Wenn Sie das durch den Mittelstand durchleuchtend betrachten, dann sehen Sie so etwas Top down beginnt. Das hat angefangen mit den Skandalen bei Daimler, Deutsche Bank, dass plötzlich der Vorstand im Fokus stand. Das wissen Sie besser als ich, die Dax Unternehmen reden permanent miteinander und gucken, wo jeder steht und was jeder macht. Und wir die anderen müssen uns bewegen.

Dann haben Sie diesen Effekt, der runtergeht bis in den Mittelstand. Das ist ein Phänomen, das man, wie wir es im Datenschutz gesehen haben, auch diese sehr starke Bewusstseinsgefährdung, versuchen muss, das auch auf der Sicherheitsebene zu intensivieren. Das könnte eine Stellschraube sein, die nützlich ist und bei der man auch überlegen sollte, ob man etwas stärker akzentuiert. Das ist vielleicht nur eine kleine Stellschraube, über die es sich lohnt nachzudenken.

Der zweite Punkt ist, was Sie auch ansprachen, cyberphysische Systeme, Produktsicherheit, Vernetzung der Dinge. Da stehen wir momentan mit dem Produkthaftungsgesetz in einer Diskussion, die gerade erst beginnt, ob es eigentlich eine Verpflichtung desjenigen gibt, der als Hersteller ein Produkt in den Markt bringt, dieses Produkt auch cybersicher auszustatten. Sie können das z.B. in allen Diskussionspapieren beobachten, die die Arbeitsgruppe Recht der Plattform Industrie 4.0 entwickelt. Ich darf da an anderer Stelle auch dazugehören, und wir reden da auch mit. Da ist der konservative Betrachtungsstand, dass der Hersteller ein Produkt auf den Markt bringt und dass das angegriffen wird, ist erst einmal nicht das Risiko des Herstellers, sondern das ist im Grunde genommen das natürliche Risiko desjenigen, der ein Produkt kauft. Er weiß, wie es beschaffen ist, und da muss er sich gegen den wehren, der das Produkt angreift.

Wenn Sie aber natürlich Angriffssektoren in der Cyberwelt haben, die eigentlich gar nicht zu erkennen und zu identifizieren sind, dann hilft Ihnen das in der Praxis relativ wenig. Die Frage ist, ob es zumindest überlegt werden muss, dass hier auch eine gewisse Verlagerung der Verantwortung erfolgt. Das können Sie im Rahmen der Produkthaftung zum Teil dadurch

erzielen, dass Sie Produkte auf den Markt bringen, die ungefährlich sind oder jedenfalls nach dem Stand der Technik soweit ausgerüstet sind, dass sie keine Gefahren begründen. Wenn Sie natürlich an Beispiele denken, die bereits genannt wurden – denken Sie an das Connected Car – das Fahrzeug, das Sie in den Verkehr bringen, dann können Sie an der Stelle einen Ansatz sehen, dass der Hersteller des Fahrzeugs sich überlegen müsste, wie cybersicher er sein Fahrzeug ausstatten muss oder ob er diese Diskussion den Gerichten überlässt, die dann acht Jahre später darüber urteilen, ob im damaligen Zeitpunkt der Inverkehrsbringung der Stand der Technik es erforderte, dieses Fahrzeug in bestimmter Weise auszurüsten.

Es ist die Frage von der Regelungsmechanik, ob Sie abstellen auf selbstregulierende Kräfte des Marktes unter dem gegebenen Rahmen der Produkthaftung, wo man dann acht Jahre später sieht, wenn die Gerichte entschieden haben, was erforderlich gewesen wäre oder ob man da eigentlich ein förderndes und sozusagen unterstützendes, die Verbesserung der Cybersicherheit regulierendes Element mit einflicht, ob durch Auslegung mit bestimmten gesetzgeberischen Mechanismen ist dann eine Frage der Umsetzung.

Nehmen Sie – das ist der dritte Teil – das Beispiel der Connected Cars. Es gibt nicht mehr nur den Hersteller, und es gibt nicht nur dieses traditionelle Haftungsverhältnis: ich bin ein Fahrzeughersteller oder ich bin ein Fahrer oder ein Fahrzeughalter und es geschieht etwas und ich kann mich an denjenigen wenden, der geschädigt hat. Also, mein Fahrzeug wird gehackt und ich wende mich an den Fahrzeughersteller, weil möglicherweise das Fahrzeug eben nicht auf der Sicherheit beruht, die sie erforderlicher Weise haben muss. Und Sie haben im Bereich der vernetzten Fahrzeuge, und denken Sie an alle anderen Beispiele, die daraus folgen, natürlich auch Dritte. Sie haben Betreiber von Systemen. Das sind nicht notwendigerweise die Hersteller der Produkte. Das sind Plattformbetreiber. Und ich glaube, und es ist einfach nur der Anlass, dieses Beispiel hervorzuheben, dass wir überlegen sollten und müsen, auch unterhalb des Radars der Betreiber kritischer Infrastrukturen – da gibt es die, die adressiert werden - ob wir sagen müssen, dass Plattformbetreiber, diejenigen, die eigentlich dieses Internet der Dinge ermöglichen, die also praktisch dazu führen, dass sich diese Datenökonomie aufbaut, dass die Mehrwerte aus der Nutzung, Zusammenführung, Neubewertung von Daten das eigentlich ermöglichen. Das ist sozusagen das Getriebeöl, das dieses Ganze funktional machen wird. Bei den Smart Grids sehen wir, dass nicht nur die Energiehersteller nicht nur die Erzeuger, nicht nur die Prosumer sein, die irgendein Solarpanel

auf dem Dach haben, sondern es gibt dazwischen Mittler, die eine ganz wichtige Rolle einnehmen werden.

Die Frage ist, ob diese jetzt unterhalb der Ebene der Kritik des Betreibers diese Intermediäre vor allem eines sicherstellen müssen im Rahmen ihres Geschäftsmodells, dass die Absicherung der Daten, also Integrität der Daten, gewahrt ist. Dass der Eingriff von außen, der unberechtigte Eingriff von außen, robust abgesichert wird. Da ist es eben die Frage, ob so etwas nur durch Selbstregulierung, Selbsthandlungskräfte des Marktes funktionieren kann, bei dem man nachher sieht, wo es gutgegangen ist, wo sozusagen der Wettbewerb und die beste Sicherheit vorhanden ist oder ob es das Wesen der Sicherheit ist, das sich im Grunde genommen schwer nach außen verkaufen lässt; ich bin noch sicherer als der andere. Das sieht man erst, wenn es eigentlich schiefgeht, ob man an der Stelle auch möglicherweise zu Regulierungsmaßnahmen greifen müsste.

Oder ist es so, dass man sagt, BSI Grundschutz ist einfach sozusagen ein Standard und jeder, der Erfolg haben will, hält sich daran. Das ist eine offene Frage und um Ihnen da den Bogen zum Datenschutz zu erleichtern – viele von Ihnen kennen das Projekt der Trusted Cloud des Bundeswirtschaftsministerium, das sich sehr erfolgreich über die letzten drei bis vier Jahren mit der Frage befasst hat, wie man einen Rechtsrahmen zur Zertifizierung von Cloud Dienstleistern entwickelt, um das Ziel zu erreichen, dass die Akzeptanz von Cloud Technologie im deutschen Mittelstand, gerade damit die deutsche Wirtschaft diese Transformation schafft an dieser wichtigen Stellschraube Erfolg haben kann. Das Rahmenregelwerk, das erschaffen worden ist, sehen Sie auch in der Datenschutzgrundverordnung Artikel 42/43. Gerade letzte Woche wurde im Bundeswirtschaftsministerium das Pilotzertifizierungsprojekt, das sozusagen ein Vorläufer der praktischen Umsetzung ist, umgesetzt. Sie sehen, was damit erreicht wurde, ist dass man gesagt hat: Zertifizierer, Zertifikate, dienste sind die gesetzliche Anerkennung der Compliance. Das ist das Ziel, das damit umgesetzt wurde, d.h. es ist nicht nur ein selbstmarktorientierter Ansatz, sondern zu sagen, dass es die rechtliche Anerkennung von Zertifikaten gibt auf der Ebene von Compliance.

Ich würde anregen zu überlegen, ob man so etwas Ähnliches im Sinne eines Transfers auch auf den Bereich der Sicherheit überträgt. Das könnte ein nützlicher Ansatz sein, um auch dieses Momentum voranzutreiben. Vielen Dank.

Prof. Eckert:
Ganz herzlichen Dank. Wie immer wunderbare Impulse, spontane Fragen?

NN:
Vielen Dank für diesen Punkt, dass man versucht, in diese Systeme, die kritisch sind oder wie kritisch, muss Gesellschaft entscheiden, inwieweit man die regulieren muss oder sich das selbst ergibt. Vielleicht als Beispiel dazu. Das Bezahlfernsehen ist genauso ein Beispiel - das ist eine kommerzielle Geschichte –, aber da geht es im Prinzip auch darum, dass der Betreiber ein finanzielles Interesse hat, dass die Leute nicht umsonst bei Sky und den Digitalprogrammen einfach kostenlos zuschauen. Aus meiner Erfahrung ist es so, was hier in der Industrie passiert, dass man in den Millionen von Geräten, die in den Haushalten bestellt werden, jeden Cent einspart. Da ist Sicherheit so definiert, dass man sagt, wir akzeptieren, dass die Leute vielleicht mal eine Stunde, fünf Stunden, wie auch immer, kostenlos Fernsehen schauen können, wenn es jemand gehackt hat. Wir bereiten uns aber als Industrie darauf vor, diese Geräte ganz schnell mit einem Softwareupdate zu versehen, so dass diese Hacker unmöglich gemacht werden. Als Gesellschaft müssen wir ja entscheiden, ob wir bereit sind, fünf Stunden mit einer falschen Stromrechnung, mit Stromausfall, mit Waschmaschinen, die sich automatisch stark nach oben zu leben oder sind wir es nicht. Wenn wir aber dann nicht bereit sind, heißt das, dass es Kosten, Regulierung, viel Arbeit für TÜVs und andere Zertifizierer gibt. Es gibt Chancen für Hersteller.

Vielleicht als Anregung von mir: Man hat beim Sicherheitsgurt gesagt, dass es die Menschen krank macht. Die Autos werden zu teuer und lassen sich international nicht mehr verkaufen, weil wir den Sicherheitsgurt einbauen müssen. Wir haben Warnschutzregelungen und alle möglichen Dinge, die uns vor Gefahren von außen schützen. Meine persönliche Meinung ist, dass die Gesellschaft und die deutsche Wirtschaft nicht deswegen den Bach runtergehen wird, wenn wir ein bisschen mehr Regulierung einführen; ein CE Zeichen, ein VDE Zeichen und was es in diesem Bereich gibt. Wir sollten das machen und das wäre im Prinzip auch eine Anregung, vielleicht dieses Spannungsfeld direkt mal zu diskutieren. Ich habe viel gelernt heute Abend, aber von keinem der Redner eigentlich eine Meinung gehört wie: ich finde, wir sollten so weit gehen. Und das ist die Rolle des Staates, weil hier die Feuerwehr noch eingreift und beim Rest muss individuell Vorsorge getragen werden.

Die Frage ist jetzt an Sie: Was ist denn Ihre Meinung dazu? Sollten wir Smart Grid oder andere Bereiche noch stärker reglementieren und dem Bürger, die Industrie und die kritische Infrastruktur vor dem Bösen schützen oder sind wir schon zu weit gegangen an der Stelle?

Dr. Duisberg:
Vielen Dank. Sie haben einen sehr weiten Bogen gespannt, aber völlig treffende Frage. Natürlich ist Smart Grid ein beschränktes Beispiel, weil das Teil der kritischen Infrastruktur ist. Da haben Sie im Grunde genommen auch eine Regulierung, die jetzt sozusagen der Umsetzung harrt und bei der Sie ansetzen an den Betreibern der kritischen Infrastrukturen und dann so eine Art Trickle-Down Effekt haben, weil die Sicherheitsanforderungen an die kritischen Betreiber natürlich die Auswirkung auf die Zulieferer hat. Dieses Ökosystem wird an der Stelle auch abgesichert. Wenn Sie fragen, ob alles und jedes zertifiziert werden sollte und das Kraft Regulierung, dann würde ich nein sagen.

Was Sie natürlich machen können, ist, dass Sie sagen, dass es bestimmte Sicherheitsstandards gibt, die möglicherweise an bestimmten Stellen sektoriell für bestimmte Branchen oder auch aus der Verbrauchersicht möglicherweise auch. Das macht einen Unterschied, ob Sie Probleme bei Ihrem Pay TV haben oder das Auto gegen die Wand fährt. Das sind sicher unterschiedliche Gefährdungssituationen, ob es eine Anforderung gibt, bestimmte Zertifizierungen tatsächlich auch einzufordern bzw. Compliance Anforderungen zu formulieren, die durch Zertifikate dargelegt werden können. Dass Sie sozusagen durch einen entsprechend akkreditierten Zertifizierer für bestimmte Dienste, die Sie erbringen, zertifiziert sind und damit Ihrer Pflicht und Schuldigkeit im Sinne der Absicherung Genüge getan haben. Der Kunde, der Verbraucher, das Unternehmen, das sich darauf einlassen will, hat diese vertrauensstützende Maßnahme, auf die er tatsächlich auch vertrauen kann, soweit es eben reicht. Das wäre, glaube ich, ein überlegenswerter Ansatz.

Prof. Eckert:
Ich würde vorschlagen, dass wir jetzt einen Cut machen und Sie alle darüber nachdenken, ob Sie dafür auch mehr Geld zahlen würden für diese Dienste, die diese Zertifizierungsprozesse durchlaufen. Dann sind wir bei den Ergebnissen von Herrn Kammer, diese Diskrepanz. Ich danke erst einmal. Draußen wartet eine Stärkung auf uns alle und ich schlage vor, dass wir danach mit den restlichen Impulsen gesammelt weitermachen und dann eine offene

Diskussion, wo Sie alle noch einmal Ihre Fragen stellen können, weil dann Herr Kammer und Herr Duisburg noch einmal mit auf dem Panel sind.

Prof. Eckert:
Meine Damen und Herren, die Veranstaltung ist komprimiert. Ich werde jetzt die Teilnehmer des Podiums nacheinander aufrufen und bitten, Ihr Statement zu dem Thema für heute Abend abzugeben. Bitte machen Sie sich Notizen, was Sie die Herrschaften später fragen wollen. Ich würde auch gern Herrn Kammer und Herrn Duisberg zum Mitdiskutieren nach vorne bitten. Das wäre das Prozedere für den weiteren Verlauf.

Ich fange bei Ihnen an, Herr Sturm, von der ZF Friedrichshafen. Darf ich Sie bitten, aus der Sicht eines Anwenders die Thematik Cybersicherheit, um die es heute geht, zu beleuchten, Zertifizierung oder Selbstbestimmung

Dr. Sturm:
Sehr gerne. Wenn ich jetzt hier bin, habe ich in dem Sinn drei Perspektiven, die ich gern einbringen möchte. Zum einen bin ich seit vielen Jahren ein IT Entscheider auf der Anwenderseite als IT Verantwortlicher im Konzernunternehmen. Als zweites habe ich relativ viel Zeit investiert in den Aufbau von Netzwerken, als Voice e.V. Anwenderverband, der IT-Industrie ist und dann bin ich auch wiederum die dritte Perspektive, Konsument und Bürger. Auf die drei Themen würde ich gern kurz ein kleines Schlaglicht auf jedes Thema setzen.

Das erste ist: ich bin IT-Verantwortlicher seit 1999 und habe in der Form eigentlich immer die Fragestellung, die wir heute diskutieren, mit aus einer IT-Verantwortung mitgestalten müssen. Für mich ist die Frage, und das war vorhin schon mein Statement, dass egal wie groß das Unternehmen ist, diese Bedeutung, das richtige Maß zu finden, chancenorientiert die Chancen der Digitalisierung zu ergreifen und auf der anderen Seite Schutz, Vertrauen und Sicherheit auch für das Unternehmen in Begriffen der Gefahren zu managen, war immer ein Thema für mich.

Wenn ich in dem Kontext mit dem CEO über das Thema seiner Verantwortung gesprochen habe – das war heute Morgen das Aktiengesetz, die Organhaftung -, dann hat der CEO gesagt: „Herr Sturm, ich bin nicht der Weltmeister, ich will Weltmarktführer, z.B. in meiner Rolle BSH Hausgeräte sein, haben Sie ihm das ausgeredet. Da sagt der CEO: wir wollen Weltmarktführer für Hausgeräte sein, aber ich will nicht unbedingt der Weltmarktführer in der

IT-Security sein. Ich weiß aber sehr wohl, dass dieses Thema IT-Security sehr wichtig ist. Ich wüsste auch ganz gern bestimmte Dinge von meinen Konkurrenten. Nach unserem Wertekanon machen wir bestimmte Dinge nicht. Aber ich kann nicht davon ausgehen, dass andere Firmen auch so sind. Ich gehe davon aus, dass wir angegriffen werden und d.h., finden Sie für mich das richtige Maß an entsprechendem Schutz und Sicherheit. Auf der anderen Seite auch nicht völlige Behinderung, weil wenn wir alles so sicher machen, dass es zubetoniert ist, dann haben Sie keine Innovationen mehr und in einem globalen Unternehmen ist diese Offenheit ein Teil dessen, damit Innovation passiert und erst recht in einem Consumer getriebenem Unternehmen, was Business to Business to Consumer, dieses Multichannel zum Thema hat. Mit anderen Worten: diese Offenheit ist Teil unserer Erfolgsstory und umgekehrt der richtige Schutz. Herr Sturm, finden Sie das richtige Maß!“

Wenn ich das in meinem jetzigen Umfeld als CEO der ZF Friedrichshafen AG sehe, so kommen viele Dinge, die wir aus der Consumer Industrie kennen, jetzt in der Automobilindustrie noch mit viel stärkerer Schubkraft und auch Themen, dass Geschäftsmodelle aufbrechen und in den Verkehr bringen, Sie haben das angesprochen Herr Duisberg. Das Thema der in den Verkehrbringer kann nicht für alles haften, weil der OEM hat das nicht mehr alles unter Kontrolle. Und wir als Zulieferer sind auch das Thema. Die Branchen vernetzen sich und dadurch verändern sich alle möglichen Wirtschaftsstrukturen und finden das richtige Maß für das Unternehmen Sicherheit, aber auch für die Produktsicherheit und im Vergleich zur Consumer Industrie wenden wir das autonome Fahren an. Da geht es um Menschenleben. Da geht es um die Absicherung, dass wir dann die Produkte so sicher gestalten, dass wir dann gegenüber fremdem Zugriff…. Auch da haben wir wieder das Thema, ob wir das richtige Maß finden, weil wir das Thema absichern wollen. Und das führt mich zu meinem zweiten Punkt. Kein Unternehmen ist momentan in der Lage, diese Herausforderung für sich allein zu stemmen. Deswegen komme ich zu dem Thema Vernetzung. Und auch solche Plattformen wie die hier. Wir müssen sämtliche Stakeholder miteinander vernetzen. Herr Schönbohm mit dem BSI hat viele Beispiele gegeben. Es gibt Anwendervereinigungen, die juristische Perspektive. Wir müssen die verschiedenen „Häkelrunden“ (?), die wir dazu haben, auf einer höheren Ebene zusammengeführt werden, um mehr Wirksamkeit zu entfalten. Dazu sind solche Themen wie heute wichtig. Und das ist auch mein Engagement bei Voice e.V.

Meine dritte Perspektive als Bürger und als Verbraucher und Konsument. Ich möchte Chancen orientiert die Chancen der Digitalisierung ergreifen. Wenn ich z.B. durch Connected Health mein Leben verlängern kann, länger gesund bleiben kann, dann will ich das nutzen. Und umgekehrt möchte ich aber auch in meiner individuellen Selbstbestimmung sagen können, was und welche Daten ich wem anvertraue. Das heißt, wir brauchen dann auch Architekturen und da müssen wir Forschung und Entwicklung machen, dass wir Architekturen entwickeln, die das Thema 'ich kann selbst bestimmen, wie viele Daten ich wem bereitstelle und ich kann auch sicher darauf vertrauen, dass das dann so ist'. Und das muss auch Rechtsrahmen einklagbar sind, dass ich, wenn meine individuellen Rechte verletzt werden, es auch einklagen kann. Da müssen wir uns hin entwickeln, und ich bin fest davon überzeugt, dass nicht in allen Wirtschaftsräumen, aber in einigen Wirtschaftsräumen, Konsumenten dafür auch mehr Geld bezahlen werden.

Das kann man nicht über einen Kamm scheren, dass man hier in Deutschland/Europa anders unterwegs ist als in Asien, gerade von der Awareness. Das ist dann wieder die Herausforderung für die globalen Companies, die globale Produkte offerieren wollen, und Sie haben das sicher alle verfolgt. Der chinesische Staat will das Thema Elektromobilität ganz klar reglementieren. Wir haben also den regulatorischen Stachel, von dem wir gesprochen haben. Wieviel brauchen wir? Der kann auch in eine ganz andere Richtung gehen. Siehe chinesischer Staat, dass der vorschreibt, dass jedes Elektromobil die Daten bereitstellt und darüber nicht zu diskutieren ist. Das ist natürlich wieder eine Herausforderung für diejenigen, die in globalen Wirtschaftsunternehmen Produkte bereitstellen. So schließt sich der Kreis. Wir sind in einer sehr dynamischen komplexen Situation und diese drei Initiativen lassen sich nur dadurch vereinigen, dass wir alle unser Wissens und auch Technologien miteinander kombinieren und die entsprechenden Grundrechte, wie wir leben wollen. Danke.

Prof. Eckert:
Herr Sturm, Sie haben mich sprachlos gemacht. Wir machen einfach weiter. Nehmen Sie die Anregung mit, was das wichtige Maß ist. Wir werden sicherlich darüber diskutieren. Jetzt kommt Herr Reinema von Siemens.

Dr. Reinema:
Die Aussage von Herrn Sturm, dass es ein komplexes Thema geht ist, kann ich nur unterstreichen. Natürlich ist Digitalisierung auch ein großes Thema für Siemens. Es ist eine

der drei Säulen der Siemensstrategie neben Elektrifizierung und Authentifizierung. Wir sind der Meinung, dass es kaum eine erfolgreiche Digitalisierungsstrategie geben, ohne dass es auch eine Security Strategie gibt. Das Thema Security hat bei Siemens einen sehr hohen Stellenwert. Es ist eines von zehn Technologiefeldern, die die Siemens AG als Technologieunternehmen hat. Wir betrachten dabei mehrere Facetten. Natürlich kümmern wir uns auf der einen Seite um den Schutz unserer Golden Nuggets unserer Infrastrukturen. Das macht mittlerweile jedes größere Unternehmen. Was für uns auch eine wichtige Facette ist, ist, dass das Thema Sicherheit unserer Produkte und nicht einfach, weil Produktsicherheit mittlerweile en vogue ist, sondern insbesondere auch, weil Siemens einer der Weltmarktführer bei Komponenten für kritische Infrastrukturen ist und wir jetzt den Marktdruck nicht erst durch die Regulierung verspüren, dass die Betreiber kritischer Infrastrukturen auf die Lieferanten zugehen und verlangen, dass dem Thema Security Rechnung getragen wird. Das ist etwas, was Siemens schon in der Vergangenheit pro aktiv angegangen ist und nicht erst seit Stuxnet. Also, Stuxsnet war sicherlich noch einmal einen Weckruf für das ganze Thema Product Security, hat dem noch einmal mehr Geschwindigkeit verliehen. Aber es ist ein wichtiges Thema für uns. Was für uns auch wichtig ist, ist das Thema IT-Security in der IT oder in den IT-Infrastrukturen versus IT-Security in sogenannten OT Infrastrukturen, Operational Technologies, weil wir in diesen beiden Infrastrukturen sehr unterschiedliche Charakteristika und sehr unterschiedliche Anforderungen haben. Im OT Bereich haben wir sehr viel Echtzeitanforderungen. Wir haben kleine Foot Prints. Wir haben sehr viel Legacy. Wir haben Produktlebenszyklen, die 10, 20, 30 Jahre in der IT sind. Da kann ich mal ein Security Problem ausschwitzen und mir sagen, dass ich in zwei Jahren die Klamotten sowieso austausche. Dann ist das Problem auch weg. In dem OT Bereich kann ich das nicht.

Wir beschäftigen uns demzufolge auch sehr stark mit dem Thema Security bei Industrial Control Systems Industrie 4.0, Internet of Things, auch so Fragen, wie ich so etwas mache. Wie bringe ich Updates in Patch ?.Natürlich kann ich irgendwann sagen, dass ich eine Weichensteuerung irgendwo in Sibirien verbaut habe. Da müsste mal ein armer Eisenbahner hin müsste und ein Patch einspielen. Wenn ich aber eine Trafostation unter Wasser 2000 Meter tief im Meer versenkt habe, holt die in den nächsten 30 Jahren keiner mehr rauf. Das ist einfach die Herausforderung. Das heißt, wir müssen heute überlegen, was in diesem Zeitraum passieren kann und was wir hier einbauen müssen. Wir sehen, dass wir es mit einer sehr viel stärkeren Komplexität zu tun haben, sehr viel mehr mit Dynamik. Dass wir uns sehr stark mit Sicherheit von komplexen Systemen beschäftigen müssen, nicht mehr nur einzelne

Systeme, die relativ statisch sind, wo man sagen kann, okay, der darf das zu der Zeit mit diesen Daten tun, sondern es ist alles sehr dynamisch und sehr flexibel. Weil gerade durch Internet of Things und Industrie 4.0 das Ganze noch mehr an Geschwindigkeit bekommt und man sich fragen muss, wie man das überhaupt noch in den Griff bekommt bzw. welche Security Architekturen wir denn brauchen. Da sehen wir ein wesentliches Problem. Es gibt heute glücklicherweise mittlerweile mehr Leute, die etwas von Security verstehen und die sich beispielsweise mit Kryptografie auskennen, Publity, Infrastrukturen und Identity Nexus (?) IT Management. Aber es gibt wenige Leute, und das sehe ich auch bei mir im Team, die wirklich durchgängig Security Architekturen aufsetzen können, wirklich von der Artware Ebene, von der Feldebene bis rauf in die Cloud. Wir sehen, dass immer wieder in unserem Team, dass man relativ viel Security Technologien und Building Blocks verbauen kann, aber wenn die Architektur nicht wirklich sauber ist, dann findet der Hacker immer einen Weg, wo er sich schön vorbeimogeln kann. Das ist eine der Herausforderungen, die wir sehen neben Themen wie Internet of Things als neuen Angriffsvektor. Gerade in den letzten Wochen gab es einige der mittlerweile weltweit größten Denial of Service Attacken, die ungeschätzte IoT Devices genutzt haben mit über einem Terabit pro Sekunde. Wenn man wie ich aus dem Telco Bereich kommt, weiß man, was das heißt. Das ist erst der Anfang. Das ist etwas, was uns sehr stark beschäftigt. Jetzt kann man sagen, na gut, das sind alles Consumer Devices und das betrifft uns nicht. Aber wir haben auch im Telco Sektor gesehen, wie schnell Consumer Devices in den Business Bereich migrieren, also eine sehr starke Herausforderung.

Natürlich beschäftigt uns auch das Thema Ausbildung von Security Experten, schon auch in dem Zusammenhang, dass die Berufsschulen mehr tun sollten und uns mehr gute Studenten schicken sollten. Aber das wird das Problem nicht lösen. Wir investieren selber sehr viel in die Ausbildung unserer Ingenieure, unserer Field Service Techniker. Allein im letzten Jahr haben wir 300 Security Engineers im eigenen Haus ausgebildet.

Wir sehen aber auch, dass Security nach wie vor ein Thema für Spezialisten ist. Ich kenne das aus meiner eigenen Studentenzeit. Wir haben einfach ein großes Problem, was das Thema Usability angeht. Wenn ich einem Field Service Engineer, der draußen in der Nordsee eine Windturbine installiert, das Thema Publity Infrastruktur X.509 Zertifikate beibringen muss, hilft das einfach nicht. Wir haben es auch, ich übertreibe jetzt, vielfach mit Menschen zu tun, denen wir grundlegende Dinge im Bereich Security beibringen müssen, die maximal rote von blauen Drähten unterscheiden müssen. Das ist eine der großen Herausforderungen. Viele

Sachen, die wir bauen, müssen sehr viel einfacher werden. Wir müssen sehr viel mehr Wert auf Usability legen. Natürlich brauchen wir mehr gut ausgebildete Leute in diesem Bereich. Aber das ist eben nur ein Teil der Fahnenstange. Das Thema Usability steht hier klar im Vordergrund und wir sehen immer wieder, wenn wir auch Sicherheitsvorfälle, wenn wir Schwachstellen retrospektiv betrachten, dass man mit einfachen Mitteln schon sehr viel erreichen kann.

Das ist durchaus ein Thema. Natürlich muss hier noch einiges in Sachen Forschung und Entwicklung passieren. Gerade im Bereich IoT, wo wir nicht nur Mensch zu Mensch Identifikation, Authentifikation und Autorisation haben sondern auch Mensch zu Maschine bis hin zu Maschine zu Maschine und sehr dynamische Konfigurationen. Siemens investiert hier in nicht unerhebliche Bereiche in dem Bereich. Gerade auch in Technologien, wo jeder sagen würde, dass wir uns mit Identity und Access Management vor 20 Jahren beschäftigt haben. Der Drops ist gelutscht. Da wissen wir, wie das geht. Nein, gerade durch das Thema Internet of Things, die Skalierbarkeit, die Dynamik, die Flexibilität gibt es Anforderungen, die die heutigen Systeme in dem Bereich einfach nicht zu leisten imstande sind.

Oder auch im Bereich Cyber Defence, wo wir einfach noch enorme Herausforderungen sehen. Wir für uns sehen den Dreiklang. Es ist klar, dass wir auf Prävention setzen. Aber wir setzen auch sehr stark auf Detektion und Reaktion, weil wir einfach aus der Erfahrung wissen, dass jedes System noch so gut sein kann, irgendwann wird ein blasierter Angreifer einen Weg irgendwo durch finden. Das heißt, wir müssen in der Lage sein, diese Dinge so schnell wie möglich entdecken zu können, unterbinden zu können bzw. eine entsprechende Widerstandsfähigkeit zu entwickeln, ähnlich wie wir das beim Thema Feuer auch haben. Wir haben unsere Brandschutzeinrichtungen. Wir haben Rauchmelder. Wir haben Sprinkler. Und wenn alles zu spät ist, kommt irgendwann die Feuerwehr. Das ist eben das, was wir im Security Bereich auch sehen.

Wir führen bei uns im Unternehmen auch, wie das vorher in der Diskussion auch schon mal anklang, Regulierung versus Selbstverantwortung. Natürlich haben wir diese Diskussion auf der politischen Ebene, und als Unternehmen sind wir immer sehr stark für Selbstverantwortung und sind mit Regulierung vorsichtig. Wenn jedes Land der Welt so seine eigenen Gesetze und Regeln erfindet und gerade als international operierendes Unternehmen kann das dann beliebig schwierig werden, und es ist auch beliebig schwierig. Ich sehe das,

wie wir in Deutschland und Europa unterwegs sind, wie die Chinesen da unterwegs sind und wie die so ticken. Oder auch die Amerikaner, wo ich sagen würde, dass wir da mal gucken müssen, dass die Sachen noch zusammenpassen. Das ist aber auch im Kleinen bei uns im eigenen Unternehmen. Ich habe die dankbare Aufgabe bekommen zum 1.10., was die Verantwortung für die Security Governance, was Information Security und Product Security angeht. Genau da diskutiere ich genau dieselben Sachen die ich auf der politischen Ebene diskutiere mit den Divisionen, mit den Geschäftseinheiten, die keine Regeln und Vorgaben haben wollen. Sie haben die Verantwortung, machen alles selber und wissen, wie das geht.

Es gibt einfach bestimmte Sachen, wo man sagt, dass einfach ein Mindestniveau rein muss im Sinne einer Governance. Auf der anderen Seite muss die aus meiner Erfahrung auch immer komplementiert werden mit einer guten Guidance, dass ich sagen kann, okay, hier ist ein Mindeststandard und für alles andere gebe ich dir gute Beispiele, die man nehmen kann oder nicht, um Dinge in die Umsetzung zu kriegen. Man muss eben aufpassen, dass so eine Governance sehr schnell zum Papierkrieg verkommt. Es hat etwas von Safe my Escort, wenn wir das Thema Haftungsfragen bei Vorständen haben. Ich kenne das aus dem Unternehmen, wo ich vorher war und viel mit Compliance Themen beschäftigt war und wo man immer gesagt hat, dann machen wir doch eine Policy dazu und dann ist der Vorstand safe. Er hat das ja allen gesagt und wir haben das kommuniziert und auch noch Security Awareness Training gemacht und alles prima dokumentiert. Umgesetzt war am Ende des Tages wenig und das ist hier genau das gleiche Thema. Also, Regulierung versus Selbstverantwortung haben wir im Großen wie auch im Kleinen im Unternehmen. Da gilt es einfach ein gesundes Maß zu finden.

Prof. Eckert:
Gut, Herr Reinema, herzlichen Dank. Herr Raab hat es schwer, das jetzt noch zu toppen, aber wir schaffen das schon.

Herr Raab:
Der worst Case ist eingetreten. Es ist bereits alles gesagt worden, nur nicht von jedem. Aber mit dem IT und IoT sprechen Sie mir wirklich aus dem Herzen. Was Sie aus den Tiefseekarten kennen, kennen wir aus dem Satellitenbereich bei Airbus. Wenn da oben etwas schief geht. Das muss man sich schon gut überlegen. Das Thema kann man durch so viele Prismen brechen. Ich wollte es jetzt einmal durch einen Begriff brechen, den ich Entgrenzung nennen will, und das hat mindestens drei Dimensionen. Bei dem ganzen Thema der Cyber

Entwicklung haben wir zum einen eine Entgrenzung im Tempo. Es wurde auch schon oft gesagt, dass alles immer schneller abläuft. Die Hauptproblematik dahinter ist, dass die Entwicklungen so schnell ablaufen und dass man wichtige gesellschaftliche Fragen, regulatorische bekommt man hin, aber gesellschaftliche Fragen, die dann immer mitlaufen, in dem Zeitrahmen gar nicht mehr wirklich hinbekommt. Bis man die Fragen durch hat, steht eigentlich schon eine völlig neue technologische Frage mit gesellschaftlichen Hintergründen auf der Tagesordnung.

Ich glaube, das ist eine Dimension. Die zweite ist eine Entgrenzung bei staatlicher Souveränität. Auch das wurde schon gesagt. Dass das Internet mit all seinen Dimensionen natürlich Grenzenlosigkeit und Uferlosigkeit hat und damit staatliches Handeln auf eine ganz neue Art herausgefordert hat und vielleicht auch in Frage gestellt hat. Wobei die Phase der ganz großen Panik, wo staatliche Stellen eigentlich nur noch die Schweißperlen auf der Stirn hatten und das Gefühl hatten, dass ihnen alles entgleitet, ich glaube, die ist durch. Wir sehen jetzt eher eine Umkehrung, dass das Internet teilweise wieder viel stärker zu einem Herrschaftsinstrument wird. Auch eine ganz interessante Entwicklung.
Da prallen natürlich jetzt auch mit null Pufferraum Räume mit völlig neuen Traditionen aufeinander mit all den Schwierigkeiten, die das bietet. Gleichzeitig erleben wir aber diese Uferlosigkeit, aber auch wieder ein Gegentrend, die Balkanisierung des Internets. Dass wir hier Staaten haben, die meistens nicht die Vorreiter in Sachen Demokratie sind, die sehr gerne wieder in ihrer Restriction, in ihrem Bereich die Kontrolle herstellen. Was natürlich für wirtschaftliches Handeln wieder das Problem hat, in einer arbeitsteiligen weltweiten globalen Wirtschaft haben Sie vielleicht in ein paar Jahren nicht mehr die Verlässlichkeit und die Verfügbarkeit von Netzen und Zugriffen, wie wir das heute noch gewohnt sind. Das ist eine Entwicklung, auf die man sich vielleicht auch einstellen muss.

Die dritte Dimension von Entgrenzung ist einfach die Connections, die Verbindung. Das ist eine Binsenweisheit, wie die Zahl der schieren Verbindungen durch die Decke gehen wird, IoT und alles, was dahinter steht. Ich komme gleich noch darauf zurück.

Ich habe mich gefragt, warum ich das unmittelbar angesprochen habe. Ich glaube, wir haben alle ein Gefühl, eine gewisse Zwangsläufigkeit, wenn wir diese Themen aufmachen, dass das in diese Richtung geht und die Fragen, die alle aufgemacht sind und im Vorfeld hier vorbereitet wurden und die Sie stellen. Und natürlich laufen diese Megatrends von Internet of

Everything und die Datenmengen, die explodieren und auch dass Angriffsmodelle durch neue Angriffssektoren - Sie haben das so schön beschrieben -, die auch immer komplexer werden und Cybercanal usw. voraussieht.

Es gibt gewisse Megatrends, aber ich möchte einfach einmal etwas provokant in den Raum stellen, dass da auch ein bisschen kreatives Denken gebraucht wird. Das vermisse ich und zwar auch gerade von öffentlichen Stellen. Ich will das einmal an einem schönen Beispiel klar machen. Wir haben uns auch von einer Zwangsläufigkeit getrennt, dass immer mehr Mobilität, Autoverkehr und alles heißen muss, dass wir immer mehr Luftverschmutzung kriegen. Das ist überhaupt keine Zwangsläufigkeit mehr, das ist lächerlich für uns heute. Das war es aber lange. Aber immerhin haben wir uns von Sachen getrennt, wir haben uns entkoppelt. Ich finde, dass wir diese Flexibilität noch nicht haben bei den Herausforderungen im Bereich, die wir mit Cyber verbinden. Da braucht es eine gewisse neue Denke. Ich will ansatzweise, nicht weil ich den Stein der Weisen gefunden habe, zwei Möglichkeiten reinwerfen, damit Sie eine Idee bekommen, was ich meine. Bei der Zahl der Verbindungen, wir connecten also immer mehr und das schafft einen neuen Angriffsvektor. Wie sichere ich das alles und die ganze Problematik? Warum kann man nicht in besonders kritischen Bereichen an Dingen, die einem besonders wesentlich sind, ein anderes Prinzip aufstellen? Wir kennen alle im militärischen Bereich “need to know“. Need to connect. Muss ich wirklich alles connecten? Das einfach mal erfordert vielleicht einen gewissen Mut oder Tollkühnheit – weiß ich nicht. Einfach einmal die Frage aufzuwerfen oder einen anderen Denkansatz. Es wird nicht überall gehen. Das ist schon klar. Das wäre nur ein Beispiel.

Ein zweiter Punkt wäre, wenn – und ich weiß, dass die Diskussion nicht zu Ende geführt worden ist, obwohl mache sagen, dass sie durch ist -, private Daten nicht wirklich mehr privat gehalten werden können. Wenn der Zug abgefahren ist. Warum hören wir dann nicht in der Debatte etwas, okay, das ist so, machen wir ein neues Prinzip auf. Wenn ich meine Daten schon nicht mehr komplett bei mir halten kann, dass viele darauf zugreifen und sie kommerziell nutzen. Warum kann ich nicht – und das sollte nicht so schwer sein – nachverfolgbar machen, wer auf meine Daten zugreift? Ich kann sie nicht bei mir halten, aber dass man technologisch etwas einbaut, was sozusagen immer eine Rückmeldung gibt, wer jetzt auf diese Daten zugegriffen hat. Das wäre ein anderes Prinzip, wie mit Daten umgegangen wird. Das wird neue Herausforderungen haben, neue Schwierigkeiten. Das ist nur zu zeigen, wie ich denke, wie ich meine, dass man vielleicht auch einmal Denke ändern

sollte und gucken sollte, ob sich damit nicht Problematiken aufbrechen und anders angehen lassen.

Zwei weitere kurze Punkte noch. Vertrauen ist auch schon in vielfältigen Dimensionen genannt worden.
Datenaustausch, Austausch von Bedrohungen, von Angriffen – wurde auch schon mehrmals ausgesprochen heute - scheint mir ein ganz einfacher Weg, wie man nicht mit technologischen Lösungen, sondern indem man sein Verhalten ändert und auch nicht unbedingt riesig viel Geld braucht und mehr Sicherheit herstellen kann. Wenn wir sagen, dass der Umgang mit Daten ein kommerzielles Modell ist, dann ist es auch oft der Umgang mit den Angreifern. Ich glaube, es trägt sehr weit, wenn man das oft in ökonomischen Dimensionen versteht. Je mehr ich Daten austausche, umso kürzer wird der Lebenszyklus von irgendwelchen Angriffsmodellen, sprich: der Return an Investment geht runter. Das ist die simpelste Logik, wie wir einfach mehr Sicherheit herstellen können. Aber es braucht dieses Vertrauen, die Plattformen, all das herzustellen. Aber es würde unheimlich weit führen, wenn man das systematisch ausbauen kann. In der Schweiz gibt es etwas, was nicht organisiert ist wie das BSI, MELANI, ein PPP-Modell, was, wenn ich es recht verstehe, lasse mich aber auch gern belehren, gerade deshalb sehr gut als Bedrohungsaustauschplattform funktioniert, weil es eben nicht weiter meldet wie andere staatliche Stellen und darauf setzt, dass Vertrauen da ist. Auch das wäre es wert, einmal in Deutschland weiterzudenken.

Die letzte Dimension klang heute gelegentlich an, eine internationale Dimension. Wenn man Oettinger dazu zitiert, müsste man mindestens europaweit regulieren in diesen Bereichen. Zumindest versuchen wir jetzt ein gleichartigeres Niveau an Cybersicherheit in Europa herzustellen. Ich glaube, dass man da drei Ebenen unterscheiden kann. Ich glaube schon, dass wir auch in Deutschland regulieren sollten, letztlich unter dem Aspekt, es wurde mehrmals genannt, Made in Germany, um sich auszuzeichnen. Ich glaube, dass wir auf europäischer Ebene Regulierung brauchen, um dieses gleichartige Niveau an Sicherheit zu haben, von dem wir auch profitieren. Das wurde heute auch schon angesprochen. Und ich glaube, dass es Dimensionen gibt, wo es wirklich nur international funktioniert oder am meisten Sinn macht. Ich will es mal so sagen. Da könnte gerade der Threat Intelligence Exchange eines sein. Das bewegt sich dann auf so basischen Ebenen wie, welche Protokolle verwende ich? Sind das Sticks oder Taxi(?), damit ich Daten wirklich extrem zeiteffizient für alle gleichartig verwendbar austauschen kann, weil wir letztlich alle im selben Boot sitzen.

Das sind drei Dimensionen, die man auseinanderklamüsern muss. Und Regulieren auf jeder Ebene lohnt sich in gewissem Maß oder hat einen Mehrwert im richtigen Maß. Bis hierher.

Prof. Eckert:
Ganz herzlichen Dank. Auch da wieder viele Aspekte, Entnetzung gegen Entgrenzung, Usage Tracking versus Datensparsamkeit. Also, viele Aspekte. Sie haben sich das alles gemerkt und können gleich die Fragen dazu stellen. Ich leite über zu Herrn Holz von Atos IT Solutions and Services.

Herr Holz:
Atos Deutschland reicht, keine Komplikationen. Ich finde es erst einmal super, dass Sie alle noch hier sind, denn Ihnen geht es genauso wie mir. Ich fand, dass heute ganz tolle Referenten zu ganz tollen Themen, ganz tolle Aspekte von unheimlich wichtigen und guten Perspektiven, die im Grunde genommen schon alles aufgegriffen haben, was nachher für die Diskussion wichtig ist. Ganz tolle Sache! Danke, Herr Thielmann! Danke, liebe Frau Eckert!
Als ich eingeladen wurde, habe ich übrigens gedacht, dass ich mir abends um 9 Uhr eine Veranstaltung nicht vorstellen kann. Doch das Thema ist so spannend und Sie sind auch dabei; insofern toll. Zweitens freue ich mich riesig hier zu sein, weil ich vor 38 Jahren hier an der TU Berlin einen EDV Kurs gehabt habe und die Lochkarten programmiert. Es ist das erste Mal seit diesen 38 Jahren, dass ich wieder hier in diesem Telefunken Hochhaus bin. Ich bin ganz begeistert. Das war der erste Teil.

Ich möchte nur zwei Kommentare zu den Vorrednern machen. Zum einen, Herr Kammer, fand ich ganz toll, was Sie gesagt haben. Ich finde, dass Sie dieses Paradoxon toll herausgearbeitet – wir haben übrigens heute auch eine Pressekonferenz von Bitcom gehabt, ich bin auch der Sprecher für Security von Bitcom - und haben eine Studie über 1000 Interviews bei Internet Nutzern gemacht und können das im Wesentlichen bestätigen. Dieses Paradoxon finde ich ganz wichtig. Mehr möchte ich dazu nicht sagen, weil, ich glaube, dass das ein Thema für unsere Gesellschaft ist, für eine Ethik Kommission, um zu sagen, wie wir mit dem Thema Datenschutz umgehen wollen. Das ist ein Thema, was wirklich ein Witz ist zurzeit. Was ich mit Betriebsräten zu tun habe zum Thema Datenschutz kann ich Ihnen sagen und was gleichzeitig läuft, wie wir mit unserem iPhone - also das Paradoxon ist unglaublich.

Das zweite Thema ist zu Europa. Herr Raab (?), Sie haben mich sehr frustriert in Ihrem Vortrag. Ich hoffe, dass Sie das bewusst gemacht haben, um eine gewisse emotionale Dynamik zu erzeugen. In meinen Augen kann unser Heil nur in Europa liegen, und ich glaube ganz fest daran. Ich schätze Herrn Kommissar Oettinger sehr, weil ich weiß, wie sehr er an einer digitalen Binnenmarktagenda arbeitet, die sowohl technologische, kommerzielle als auch Security Aspekte beinhaltet. Ich kann nur alle Daumen drücken, dass wir hier Erfolg haben. Weil wenn wir das nicht haben, werden wir als Deutschland noch ein paar Jahrzehnte gut dastehen und unseren Wohlstand halten können. Aber dann wird es auch zu Ende gehen. Das nur vorweg.

Ansonsten, ich bin Dienstleister, habe 12.000 Leute in Deutschland und für mich ist dieses Thema Cyber-Security, was wir heute besprechen, eine Maschine zum Gelddrucken. Etwas Besseres kann mir nicht passieren. Es werden Regulierungen kommen. Was brauchen wir da? Ich habe ein Problem. Ich habe 12.000 Leute. 6.000 Jobs werden sich da in drei bis fünf Jahren verändern, d.h. dass ich für die Leute Arbeit finden muss. Und die Arbeit wird bei Security sein. Da werden die alles tun von Fachleuten, und da kann mir keiner erzählen, dass jemand, der 20 Jahre irgendwas in IT gemacht hat, nicht mit einer Umschulung ein Fachmann in Security werden kann. Nicht sofort werden, aber er kann sich dahinarbeiten und bezogen auf Zertifizierung, was wir von BaFin und anderen Reglementierungen kennen – da müssen Sie sich nur eine Krawatte nehmen, zum Kunden gehen und ein bisschen Security buchstabieren können und dann haben wir hier Dienstleistungen. Das wird passieren.

NN:
Vorsicht, es sind auch Anwender im Raum. Das sind auch Kunden

Herr Holz:
Ich habe geguckt, ob jemand von Accenture da ist, weil das Modell meiner amerikanischen Kollegen ist. Das ist nicht das Modell der deutschen und europäischen Unternehmungen. Insofern ist das in meinen Augen das Thema. Und den Aspekt akzeptiere ich. 300 Fachleute haben wir aufgebaut und ich glaube, dass das ein wichtiges Thema ist. Ich habe vor, in den nächsten 18 Monaten über 1.000 aufzubauen und bin auch mit dem BSI im Gespräch, was die Anforderungen sind. Das wird sicherlich ein Thema werden. Das ist mein Kommentar zu dem Thema, was wir hier besprochen haben. Ein tolles Thema, ein wichtiges Thema und das ist die Kehrseite der Medaille und je mehr Digitalisierung umso mehr Security.

Prof. Eckert:
Wunderbar. Fassen wir zusammen, die Paradoxien, die Herr Kammer auf den Punkt gebracht hat, müssen einfach im Diskurs weitergetrieben werden. Vielleicht brauchen wir neue Ethikregeln. Es geht nichts ohne europäische gemeinschaftliche Aktivitäten, war Ihre Aussage. Das hat Herr Reinema auch schon nach oben gehoben, Weiterbildung, Weiterbildung und Weiterbildung. Das brauchen wir. Ich denke, dazu werden wir sicher noch einiges diskutieren können. Last but not least Herr Barth von der genua.

Herr Barth:
Vielen Dank. Herr Holz, die Maschine, die Sie schon gefunden haben, müssen Sie mir unbedingt zeigen. Dann können wir das auch gern zusammen machen. Wir machen das, was Sie nicht können. Ich spreche hier für genua, ein mittelständisches IT-Sicherheitsunternehmen, das viel im Bereich kritischer Infrastrukturen staatlicher Anwender in speziellen Anwendungsfällen oder auch Maschinen- und Anlagenbau unterwegs ist. Wir bekommen unsere Leute übrigens in den meisten Fällen nicht von der Universität, weil die das nicht können, was wir haben wollen, sondern bilden die noch selber weiter aus, wenn die denn kommen. Aber dadurch, dass wir die Leute auch selber ausbilden, kriegen die auch irgendwie den Spirit mit, den wir in der Company brauchen. Wir sind sehr nahe an der Open Source Community aufgestellt und da sind schon spezielle Leute, wie ich festgestellt habe als Nichttechniker.

Letztes Jahr hat die Bundesdruckerei 52% unserer Anteile übernommen. Mich freut das, denn das sind tolle Perspektiven und gute Möglichkeiten zur Zusammenarbeit. Nur, dass Sie ein bisschen Hintergrund zu meiner Einschätzung haben.

Wer die Fragen der Konferenz nicht mehr ganz im Kopf hat: es waren drei Stück. Welche Anforderung stellt dies an die staatliche Regulierung, welche Folgen hat dies für die Wirtschaft und welche Technologien für Lösungen kann die Forschung bieten? Was heißt ‚dies'? Aus meiner Sicht heißt das die fortschreitende Digitalisierung und ihre Auswirkung für Staat, Gesellschaft und Wirtschaft. Ich habe einen Fokus auf die ersten zwei Fragen. Das liegt daran, weil wir einerseits im Umfeld staatlicher Regulierung agieren mit dem, was wir machen und andererseits, weil wir auch bereits jetzt teilweise schon von der Regulierung oder auch in Zukunft selbst davon betroffen sind.

Aus meiner Sicht steht die staatliche Regulierung derzeit vor einer Aussage und schade, dass die Adressaten nicht mehr hier sind. Die steht vor einer Herausforderung, die sie eigentlich nicht mehr bewältigen kann, weil es grundsätzlich verschiedene Prinzipien sind, nach denen Regulierung und nach denen IT-Wirtschaft läuft. Für mich sind in der IT-Wirtschaft drei Prinzipien ziemlich fest geschrieben. Erstens: Expansion durch Skalierung; zweitens: Erschließung neuer Geschäftsmodelle durch Destruktion und drittens als Grundprinzip 'the Winner takes it all'. Das ist etwas, was zumindest in unserem Wirtschaftssystem, in dem wir leben, so einfach nicht hingenommen werden kann von der Regulierung. So habe ich es zumindest kennengelernt.

Also, muss eigentlich die IT Regulierung auch drei Grundprinzipien folgen. Einmal, wenn sie damit klarkommen sollte, technische Weitsicht, das ist schwierig für Regulierung. Flexibilität und auch Konfliktbereitschaft, d.h. sie muss bereit sein, wenn ihr etwas nicht passt, richtig etwas dagegen zu tun. Das wird für die IT Sicherheitsregulierung speziell in unserem Fall bedeuten, dass man für die technische Weitsicht enge Kooperationen mit den Akteuren in diesem Bereich braucht und auch eine Bereitschaft zur Förderung der Adaption neuer Technologien für die technologische Weitsicht. Für die Flexibilität braucht man eine schnelle und adaptive Regulierung, um auf Fehlentwicklungen und neue Technologien flexibel reagieren zu können. Das ist im Moment auch schwierig, denke ich mir.

Zuletzt braucht man auch eine absehbare Reaktion mit klaren und unverhandelbaren Vorgaben und wenn es sein muss, auch Sanktionen, damit man klar macht, dass es eine Konfliktbereitschaft gibt. Auch die sehe ich an aktuellen Regulierungsbeispielen noch nicht eindeutig ausgeprägt, muss ich sagen.

Gerade die Woche hat mich eine Umfrage von Voice erreicht, wo man danach gefragt wurde, was man von den ganzen digitalisierungsrelevanten Programm im Verlauf der Bundesregierung hält. Ich habe die Umfrage pflichtbewusst beantwortet, habe danach aber noch einmal meine Antworten Revue passieren lassen. Das hat mir gezeigt, obwohl ich nicht als negativ denkender Mensch bekannt bin, dass ich noch nicht mit allem so zufrieden bin, zumindest in meiner Einschätzung und in meiner Eigenschaft als Unternehmensvertreter. Deswegen habe ich mich eigentlich mal gefragt, was diese hier vorhandene, jetzt angetretene, noch amtierende Bundesregierung eigentlich erreichen wollte in der Spitze. Ich habe mir dann

einmal zusammenkopiert, was so an IT sicherheitsspezifischen Sachen im Koalitionsvertrag stand.

Das waren zwei Seiten. Das war für uns damals ein Riesenerfolg. So wichtig war IT-Sicherheit noch nie nach Snowden. Ich habe das bewertet und es kamen viele Kreise raus, wie „ja, könnte man so interpretieren, dass da was gemacht wurde“. Da waren einige Plus drauf, wie „wir wollen ein IT-Sicherheitsgesetz machen“, ja, haben sie gemacht. Es waren auch viele Minus drauf in unterschiedlichen Bereichen. Minus heißt für mich, dass man da eigentlich sagen kann, dass da mehr drin sein muss.

Weil das so ist und vor dem Hintergrund habe ich mich auch tierisch gefreut, dass jetzt die beiden großen Volksparteien, so lange man sie noch so nennen kann, wieder um die Ecke kamen und endlich mal etwas einigermaßen Substanzielles zum Thema IT-Sicherheit gesagt haben. Also CDU und SPD haben beide einmal überlegt, was man tun muss, um Deutschland digital und IT-sicherheitsmäßig besser zu machen. Interessanterweise standen in dem Plan viele Sachen drin, die auch schon im Koalitionsvertrag standen.

Ich habe ein paar Punkte, die noch nicht so deutlich im Koalitionsvertrag standen, rausgegriffen, die durchaus diskutierenswert sind, und meine Bewertung hinzugefügt, wie ich die Chancen davon sehe vor dem jetzigen Hintergrund. Einmal Produkthaftung für Software Produkte, was im Moment politisch ein totaler Quick Win ist. Jeder will das machen, aber natürlich weiß keiner wie. Der Linus Neumann hat im Ausschuss zum IT-Sicherheitsgesetz gesagt, dass Softwarehersteller wie Drogenlieferanten sind. Die müssen die gleiche Produkthaftung übernehmen. Ich hätte denen gern einmal eine Stapel EVP Verträge hingelegt, was nicht das gleiche wie ein Produkthaftungsgesetz ist, aber da steht ein bisschen was über Produkthaftung drin. Wahrscheinlich war ihm das zu viel zu lesen.

Meine Angst ist nur, dass man bei Produkthaftung nicht die trifft, die man treffen will, nämlich die großen, die überall sind. Die haben nämlich eine Rechtsabteilung, die ungefähr so groß ist, wie die Bundesdruckerei und wir zusammen. Sondern man trifft die, die man eigentlich nicht treffen will, nämlich die kleinen schnellen, die sich nicht wehren können. Wie das so ist im Universum. Insofern wenn man das schon regulieren willl, dann soll man das gut und auch mit Weitsicht machen, wie ich es am Anfang angesprochen habe. Förderungszertifizierungs- und Zulassungsregimes habe ich hier auch aufgegriffen. Das steht,

glaube ich, bei der SPD drin. Ich bin total für Zertifizierung und Zulassung, und wir machen das lange und oft. Es muss nur auch irgendwann einen Pay off geben. Wenn ich mit einem Produkt zwei Jahre lang vom Markt ferngehalten werde, einfach weil es nicht fertig wird, nicht das Produkt sondern die Zertifizierung, ist das ein Markthindernis. Dafür ist das Pay off, was Mindestzertifizierung im Bereich criteria (?) bietet, nicht hoch genug. Bei allem verständlichen Fokus auf den Anwender, finde ich das richtig und gut. Man kann als Regulierer auch eine Branche kaputt machen, wenn man da zu viel tut. Also, muss es da ein miteinander Sprechen geben. Herr Schönbohm hat auch ein paar Sachen genannt, die da kommen könnten und werden, hoffe ich. Ich glaube, dass man da gemeinsam etwas hinbekommen kann. Aber es muss eine Veränderung geben. Das geht so nicht weiter. Sonst beschäftigen sich nicht mehr nur noch vier Unternehmen in dem Bereich, sondern irgendwann nur noch zwei und dann eins. Das ist der Tod jeder Innovation. Das kann man nicht haben wollen.

Thema 3: Privilegierung von Unternehmen im Vergaberecht zum Erlangen von mehr technologischer Souveränität. Das steht, wen überrascht es, bei der CDU drin. Das war eigentlich ein Thema, was ich in der öffentlichen Beschaffung schon lange abgeschrieben habe. Ich finde es interessant, dass es wieder auf das Tablett kommt. Ich halte es für notwendig. In den meisten Staaten, übrigens auch in den USA, ist das gelebte und gefeuerte Praxis. Aber ist das derzeit hier in Deutschland umsetzbar?

Ich zitiere die Leiterin eines zentralen Vergabebereiches einer großen Beschaffungsbehörde mit einem Riesenbudget, was sie zu einem Staatssekretär in ihrem Bereich gesagt hat: „Meine Bibel ist das Vergaberecht und da werden Sie auch nichts daran ändern.“ Mit der Einstellung kommen wir nicht darüber hinweg, dass wir das so machen.

Insgesamt komme ich mit dem Blick auf das Thema zu folgenden Schluss. Regulierung wird meist als unzumutbare Mehrauflage gesehen, die den Wettbewerb verzerrt aus Sicht der Wirtschaft, die von der Regulierung betroffen ist. Ich sehe bei der Situation, die wir haben, Regulierung eher als Versuch Fehlentwicklung von einem Markt entgegenzuwirken. Das ist aus meiner Sicht bei IT-Sicherheit auch der Fall. Wir haben hier einen Markt, der funktioniert wie ein Markt funktioniert. Das heißt aber nicht, dass der Markt immer Recht hat. Der Markt hat global gesehen, so wie er soll, das gemacht, was er soll, aber der hat nicht immer die Gesellschaft im Blick und das Gesamtstaatsystem. Der Markt hat den Markt im Blick, und

deswegen glaube ich, dass hier Regulierung an der richtigen Stelle richtig gemacht, auch helfen kann, um das in die richtige Richtung zu drücken und das ans Wünschenswerte anpasst.

Prof. Eckert:
Wunderbar. Herr Barth, auch Ihnen ganz herzlichen Dank. Das war eine Lanze doch mal für Regulierung, aber mit stärkerer Flexibilität, mit gewissen Rahmenbedingungen, um Fehlentwicklungen entgegenzuwirken. Das war Ihr Kredo, aber bitteschön mit Maß. Somit schließt sich schön der Kreis zu Ihnen, Herr Sturm. Ich gebe jetzt das Feuer frei und bitte auch noch mal die anderen Referenten mit nach oben. Bitte, lassen Sie Ihre Fragen los.

Prof. Helmbrecht:
Ich habe zwei Fragen, die eine geht an ZF, Siemens. Vielleicht zum Hintergrund, um das auch positiv zu machen. Nicht, dass mein Bild von Herrn Eberspächer bleibt. Ich bin ja in Brüssel, und das sind 95%, wie sagten Sie, Häkelrunden? Ich bin dann auch ein Lobbyist in eigener Sache oder in dem Thema. Ich möchte nur zwei Beispiele geben. Der Berichterstatter für die Datenschutzgrundverordnung war Herr Albrecht von den Grünen, und der Berichterstatter für NIS Direktive war Herr Schwab von der CDU. Das hat auch schon Einfluss auf den Prozess. Das darf man nicht vergessen. Die Wahl des Berichterstatters schon wichtig ist.

Meine Frage ist, was Sie gerade über die Produkthaftung sagten, sehe ich als Konsument anders. Wenn ich ein Auto kaufe und die Bremsen nicht funktionieren, ist der Autozulieferer oder der Autohersteller verantwortlich. Jetzt habe ich, und das sage ich hier ganz ehrlich, auch wenn ich in Brüssel bin, das Bild, zu sagen, dass wir IT-Sicherheit in der Vergangenheit nicht in den Griff bekommen haben. Jetzt haben wir vielleicht das Glück, wenn wir autonomes Fahren haben oder so viel IT im Auto haben, dass wir endlich IT-Sicherheit in den Griff bekommen, wenn wir die Autohersteller und Zulieferer dafür haftbar machen. Also, nicht das Bild, was vorhin war, sondern das ist schon etwas, wo die Frage ist, und jetzt müssten Sie mich überzeugen, dass ich etwas anderes in Brüssel vertrete, weil ich schon die Hoffnung habe, dass wenn wir Sie zwingen, wir auch die Kette dazu zwingen.

NN:

Die Frage, die ich mir bei dieser Diskussion auch immer wieder stelle, was denn eigentlich in dem Wartungssystem fehlt. Ich bin jetzt kein Jurist, aber so wie es heute aussieht, kann ich mir aussuchen, wen ich mir greife. Ich greife mir immer den Solventesten. Ich greife mir entweder den Automobilhersteller oder ich greife mir irgendjemand, der die Komponenten liefert, also der, von dem ich glaube, dass er das meiste Geld hat. Wenn wir das Thema IT-Security betrachten, haben wir dadurch, dass viele Komponenten zusammenkommen und dadurch, dass es eben nicht nur den Hersteller gibt sondern immer auch den Betreiber und den Nutzer, haben wir schon allein dadurch eine Situation, die komplex zu handhaben ist. Die Frage, die wir uns immer stellen, wenn diese Diskussionen hoch kommen, alle Verantwortung, alle Haftung auf den Hersteller. Gibt es denn Dinge, die wir ändern müssen, wo wir in dem Haftungsregime, was wir heute haben, echte Defizite haben?

Dr. Sturm:

Zwei Punkte auf die Frage, Herr ?. Die eine Sache ist, dass wir schon versuchen sollten, diesen Weg zu gehen. Wenn diese schöne Welt so ist, dass ich einen Inverkehrbringer habe, der sozusagen die ganze Kette auch gestaltet und dass ich sage, der OEM und der Zulieferer dahinter und die Software usw. Das Problem ist nur, dass diese klassischen tradierten Muster zerplatzen gerade. Wenn Sie sich ein selbstfahrendes autonomes Fahrzeug vorstellen, dann fährt es auf Basis von Steuerungsinformation, die die wiederum von einem Kartenhersteller hat. Und der Kartenhersteller ist vielleicht nicht unbedingt derjenige, der entsprechend der OEM ist, der Inverkehrbringer. Dann kommen Sie in ganz schwierige Fragestellungen. Ist der Unfall jetzt dadurch passiert, dass das Steuerungssystem in dem autonomen Fahrzeug versagt hat oder hat es externe Information gehabt, die falsch war? Mit anderen Worten, sind diese klassischen Dinge, diese 1:1 Beziehungen und die ganze Kette darunter gibt es nicht mehr. Das ist die Problematik. Ansonsten ja, wo sie ist. Sonst würde ich das Prinzip nicht auflösen wollen. Das ist der eine Punkt.

Der zweite Punkt ist, dass wenn es so ist, müssen wir uns natürlich überlegen – Sie haben das vorhin etwas sarkastisch mit Häkelrunden bezeichnet, ich wollte aber eher selbstkritisch sein - , dass wir dann Gefahr laufen, unter unseren Möglichkeiten zu bleiben, wenn wir nicht diese neue Realität akzeptieren und uns neue Architekturen bilden, wie wir mit dieser gestiegenen Komplexität umgehen. Das wollte ich damit zum Ausdruck bringen und jetzt schließe ich erst einmal ab.

Prof. Eckert:
Ich würde ganz gern Herrn Duisberg dazu fragen.

NN:
Ich wollte nur direkt dazu. Es wurde noch komplizierter. Deswegen, weil wir künftig und heute beginnt das ja schon, eine dynamische Funktionalität in den Geräten haben. Das heißt, die Funktion, die durch Software und durch Apps, und zwar auch nur durch Kombinationen von Softwarekomponenten dargestellt werden, sind ja über der Lebenszeit weitaus schneller veränderlich und von Dritten werden die zugeliefert. Mir ist völlig unklar, wie man hier – und es wurde auch schon in der Presse dargestellt – überhaupt noch a) von Besitz, b) von Haftung usw. reden kann.

Dr. Sturm:
Wenn ich dazu noch eins sagen darf, wir alle wissen von dem tragischen Unfall von dem Tesla Fahrer. Letztendlich hat sich das Unternehmen Tesla, ein Software Hersteller, gesagt, dass sie nie gesagt haben, dass das funktioniert, so ungefähr, sondern wenn du diese Funktionen nutzt, musst du wissen, dass es nicht funktionieren könnte. Das ist so ähnlich, wie wir über Jahrzehnte mit Software Herstellern zusammenarbeiten, die sagen, dass sie nur alles in ihrem Ermessen befindliches getan haben, um die Software so gut wie möglich zu machen. Ich gestehe nur ein Verbesserungsrecht, wenn ein Fehler auftritt, dass das in angemessener Weise den Fehler behebt. Wenn wir jetzt in die Richtung Lebenswelten gehen, wo wir dann nicht mehr über Softwarefehler oder ‚mein Smartphone funktioniert nicht' sondern ‚ich hab mein Kind sozusagen in ein autonomes Fahrzeug gegeben und es soll jetzt für drei Stunden allein zu den Großeltern fahren'. Das ist eine ganz andere Dimension. Da müssen wir auch mit ganz anderen Prinzipien rangehen. Da müssen wir viel mehr Absicherung machen, wie wir sie aus der klassischen Industrie kennen. Ich will Ihnen nicht widersprechen. Ich will das nur als ganz wichtige Frage. Wir müssen die ganzen Wertschöpfungsketten durchgehen.

NN:
Auch wenn das ein bisschen komisch ist, will ich nur einen Punkt dazu sagen, was glaube ich unser Problem ist. Nehmen wir das Gesundheitssystem. Sie dürfen gesundheitsgerecht im Krankenhaus nicht patchen. Also, könnten wir auch ein Patch Verbot für Tesla machen und dann hätten wir eine Regulierung.

Prof. Eckert:
Herr Kammer wollte sich auch noch dazu äußern und dann Herr Duisberg.

Herr Kammer:
Ich habe ja vorhin mit den Paradoxien aufzeigen wollen, dass es einen Handlungsbedarf gibt. Das wird erkennbar, wenn Menschen etwas nutzen wollen und gleichzeitig ein ungutes Gefühl haben und von jemand anderem erwarten, dass er jetzt irgendetwas daran ändert. Was auch immer das ist. Solange sich das in so einem Niedlichkeitsbereich abspielt, indem wir irgendwie darüber lachen können, dass wir solche Widersprüche sehen, ist das ein ganz hübscher und netter Abend. Aber im Kern steckt dahinter eine ganz klare Erwartung nach Verantwortungsverteilung. Mich interessiert, ehrlich gesagt, die ganze Kette überhaupt nicht. In dem Moment, wo ein selbstfahrendes Auto vor der Frage steht, ob es einen Menschen totfahren darf oder nicht und das entscheidet irgendjemand, wird es eine ganz klare Haftungsregelung geben müssen. Wenn die nicht kommt, wird die Bevölkerung die einfordern, und dann wird die Politik das ganz schnell beschließen, weil es irgendwann einmal eine Machtfrage wird, eine Mehrheitsfrage. Dann wird es ein ganz relevantes Thema für eine ganz normale Diskussion, die wir erkennen. Die ganze Regulierung im Straßenverkehr ist gekommen, weils die Verkehrstoten immer mehr waren und immer mehr wurden. Da gibt es viele Geschichten, warum es am Anfang alles nicht ging und mittlerweile haben wir uns alle daran gewöhnt. Das gilt für ganz viele andere Bereiche auch.

Wollen wir wirklich so lange warten, dass jeder sein persönliches Fukushima gehabt haben muss. Bevor es Regulierungen gibt, die ein ordentliches Leben in der digitalen Welt ermöglichen, wie auch immer das aussehen kann. Ich finde, so eine Debatte brauchen wir wirklich viel zugespitzter als uns immer nur die Probleme aufzuschreiben, die es alle gibt. Die müssen wir auch aufschreiben, aber das muss auf den Punkt gebracht werden, damit wir auch an einigen Ecken wirklich weiter kommen.

Sie haben vorhin nach Regulierungsfragen gefragt. Wir haben alle keine Antworten darauf gegeben. Ich gehöre nicht zu den Leuten, die überall wüssten, wie man das machen muss. Aber was ich erlebt habe in meinem Leben, ist, wenn es den nötigen Druck gab, gab es auch Regeln. Warum schaffen wir denn plötzlich Atomkraftwerke ab? Es gibt seit Jahrzehnten eine Diskussion in der Gesellschaft darüber, dass das nicht in Ordnung ist mit der Atomkraft und

gleichzeitig gibt es Leute, die das aus vielen guten Gründen wollten. Und plötzlich ändert sich etwas. Da ist etwas passiert. Nun kann man sich fragen, auf was wir eigentlich warten an all diesen Ecken. Die Kompliziertheit bei Haftungsfragen erschreckt mich immer, wenn ich das höre, denn im Kern, wenn es darauf ankommt, müssen wir da eine Lösung finden. Wenn wir die nicht irgendwo anders finden, muss die sich letztlich irgendein Gericht ausdenken. Die Lösung wird es geben, wie die auch immer aussieht. Und dann wird irgendjemand damit unzufrieden sein, aber er wird sich daran halten müssen. In die Richtung wird es laufen, und ich bin auch sehr dafür. Wir sollten mit Nachdruck daran arbeiten, dass es dahinkommt. Sie haben vorhin Vorschläge gemacht, wie man das auch stimulieren kann und wie man Anreize dahineinpacken kann, damit sich z.B. Unternehmensgeschäftsführer verantwortlicher fühlen als bisher, wenn es denn noch immer so ist. Das sind alles Indizien dafür, dass es auch geht. Man muss es dann nur auch richtig angehen und es sind im Kern immer Machtfragen, um die es da geht.

Prof. Eckert:
Wir hatten erst noch Herrn Duisberg und dann Herrn Klasen, Herrn Arnold. Wir arbeiten es ab.

Dr. Duisberg:
Ich wollte eigentlich nur noch einmal das unterstreichen, was Sie, Herr Sturm, gesagt haben. Wir erleben diese fundamentale Veränderung von linearen Wertschöpfungsketten zu Datenökosystemen oder wie auch immer Sie das mit welchem Parameter beschreiben, aber die Vernetzung bedeutet, dass Sie sich eigentlich in Gemeinschaften, in Konsortien hineinbewegen. Da sind in der Tat die Haftungsfragen zum Teil dann auch schwieriger aufzulösen, weil sie sich auf die Zurechnung und die Zuordnung der Verantwortlichkeit jetzt rein technisch zum Teil nicht mehr hinkriegen bzw. wenn Sie sagen, die Lösung kommt dann möglicherweise erst, wenn Sie sozusagen einen komplexen datenbasierten Fehlverlauf haben acht Jahre später, wenn der BGH gesagt hat, dass der Sachverständige herausgefunden hat, dass es zwei waren. Und dann sind Sie in einer Situation, wo Sie das heute juristisch auflösen nach möglicherwiese Haftungsgemeinschaften, Gesamtschuld usw.

Was heute noch nicht zur Sprache gekommen ist und was aber eine ganz wichtige Komponente ist bei einer Sicht, damit solche Systeme funktionieren können, ist die Frage der Versicherung und der Versicherbarkeit. Also, natürlich der Cyberversicherung. Das ist,

glaube ich, ein ganz wesentlicher Schlüssel, damit diese Systeme einschließlich, die Deutschen lieben das Auto, damit das funktionieren kann. Die Versicherung ist ja eigentlich die Absicherung dafür, dass Sie den Regress beim Verantwortlichen entweder nicht wirtschaftlich hinreichend abgesichert bekommen oder ihn gar nicht finden. Meine Beobachtung ist, dass das eine ganz große Herausforderung für die Versicherungswirtschaft ist, weil die natürlich ihre Geschäftsmodelle erst entwickeln müssen aufgrund von Schadensannahmen, die es bisher gar nicht gibt.

Also, das ist einfach nur ein zusätzlicher Gesichtspunkt, den man vor Augen haben müsste. Das Autobeispiel ist plastisch, aber es gibt natürlich viele andere, wo auch gerade die Versicherbarkeiten eine ganz wesentliche Facette ist und die noch unterentwickelt ist. Da muss man sozusagen auch möglicherweise Anreize schaffen, Mut machen und sozusagen die Versicherungen, die daran interessiert sind, weil Kfz-Haftpflichtler wissen, dass ihre Prämien einbrechen, weil die Autos weniger Unfälle machen und da eigentlich die Risikolatenzen ansteigen.

Prof. Thielmann:
Gibt es heute schon Cyberversicherungen?

Dr. Duisberg:
Ja, gibt es schon. Jede Versicherung kann Ihnen das natürlich in irgendeiner Art und Weise etwas versprechen und auch einlösen. Nur können Sie im Grunde genommen eigentlich nicht die Deckungssummen und auch die Prämien in irgendeiner Weise bisher ins Verhältnis zur Realität setzen, weil Sie die eigentlich noch nicht so richtig greifbar haben. Zusatzpunkt: die echte Herausforderung ist nicht nur, dass Sie den Schaden nicht so richtig messen, sondern der materielle Schaden ist das eine. Der viel höhere Schaden ist oft das Reputationsthema, und das kriegen Sie sowieso nicht versichert oder sehr viel schwieriger.

NN:
Ich habe eine Frage zum Thema Regulierung, national spezifische Regulierung, deswegen an Herrn Barth und an Herrn Raab aufgrund der Vorrede. Wir haben in Deutschland viele Firmen, die sehr stark insbesondere im Industriebereich vom Weltmarkt abhängig sind. Wie können Sie sich eine national spezifische Regulierung vorstellen, die Weltmarkt kompatibel ist? Und dann diese Unternehmen auch im Weltmarkt eher und nicht benachteiligt?

Herr Barth:

Ich kann mir eine Regulierung vorstellen, die auf Qualität aufsetzt. Also, wir nehmen eine Regulierung, beispielsweise mit Zertifizierung, die Zertifizierung davon abhängig macht, wie gut wirklich ist, was man da verbaut. Dann hilft Ihnen das auch in Papua-Neuguinea, weil es gut ist. Also, nicht eine Regulierung, weil ich jetzt sage, das da muss genutzt werden, weil ich sage, das hat meinen Stemple sondern eine Regulierung, die sagt, das darf genutzt werden, weil es gut ist und wir das überprüft haben. Dann hilft es auch international.

Herr Raab:

Als Ergänzung, die ich dazu machen kann. Es wurde ja schon gesagt, dass es mit einem gewissen Augenmaß passieren sollte, ein gewisses Herausragen. Wir wollen die deutsche Wirtschaft nicht kaputtmachen, sondern dann kann man es nutzen. Nur wenn es zu viel ist, dann schlägt es ins Gegenteil. Aber sonst ganz d'accord.

NN:

Ich möchte noch mal darauf hinweisen, dass es zwischen dem Thema der staatlichen Regulierung und der Selbstverwaltung durchaus die Möglichkeit gibt, dass man das Thema der Ko-Regulierung im Prinzip anwendet. Das heißt also, wenn man es auf Grund von regulierten staatlich vorgegebenen Rahmenbedingungen so hinbekommen, dass man es dann im Sinne der Ko-Regulierung, nämlich durch Standardisierung im internationalen Bereich und vor allen Dingen hier aus deutscher Sicht heraus sicherlich auch ganz stark aus dem europäischen Bereich dann schafft, das Thema Cyber-Security so in den Griff zu bekommen, dass das, was technisch umsetzbar ist, praktisch durch die Ko-Regulierung bestimmt wird und nur noch aufgrund von politischen Rahmenbedingungen dann zu geschehen hat. Ich habe immer so ein bisschen den Eindruck, wenn wir von Regulierung reden, dass wir viel zu stark davon reden, dass auch das Thema der technischen Regulierung durch den Staat vorgegeben wird und dass das, was in dem IT Planungsrat passiert, viel zu stark immer in Richtung technologische Umsetzung gedacht wird anstatt sich wirklich an reine Rahmenbedingungen zu halten. Dann passiert auch das, was im Bereich der Ko-Regulierung passieren kann, dass wir technologische Rahmenbedingungen schaffen, die es auch den deutschen Mittelständlern letzten Endes erlauben, auf dem europäischen Markt und auf dem Weltmarkt mit entsprechenden Produkten und Services an den Markt zu gehen.

Prof. Eckert:

War das jetzt eine Frage? Ein Kommentar. Hätte Sie gern jemand gehört zu Ihrem Kommentar?

NN:

Ich finde Ihre Bemerkung sehr wertvoll, weil ich glaube, dass wir in der Tat bei dieser Thematik, was die digitale Welt angeht, keinen Instrumentenkasten vor Augen, wie das funktioniert und werden kann, auch bei der Arbeitsteilung zwischen denen, die Rahmenbedingungen setzen sollten und nicht mehr und denen, die dann auch wirklich fachlich etwas verantwortlich gestalten können. Herr Helmbrecht hat es vorhin benannt. Ich finde z.B. die in Deutschland erfundene und durch Gesetz vorgeschriebene digitale Signatur wunderbar, nur keiner nutzt sie. Das macht einfach keinen Sinn, auf die Weise sich vorzustellen, dass wir die Welt beglücken, wenn wir technisch unterfütterte Gesetze machen, indem man irgendeine Normierung darein schreibt, die dann nach ein paar Jahren auch gar nicht mehr so funktioniert. Dafür ein richtiges Lot zu finden, ist eine echte Herausforderung und da würde ich auch wirklich von Ihnen, die Sie nicht Staat sind oder so, dann immer einfordern, dass Sie auch konkrete Vorschläge machen, wie es gehen kann. Denn es ist so einfach beim Staat abzuladen, er möge das jetzt doch bitte irgendwie richten. Aber wenn er es denn macht, bitte nicht so, wie das, was dabei rauskommen. Das ist mir zu einfach, denn da sitzen auch nur Leute, die nicht viel mehr verstehen als andere, die hier sind. Dafür ein richtig gutes Lot zu finden oder ein gutes Maß, ist echt nicht gelöst bisher. Wir haben eigentlich eher nur Flops gelandet. Die größte Zuspitzung an Unsinn ist aus meiner Sicht das De-Mail-Gesetz. Das rennt ja auch richtig, dieses Produkt. Und trotzdem ist es das einzige, was der Staat gut findet. Wir bräuchten aber eigentlich eine Grundlage, um auf dieser Weise eine andere sichere Kommunikation auch bewerben zu können, so dass die Leute es auch gerne nutzen. Lauter solche Beispiele könnte man finden. Das sollten wir nicht fortsetzen, sondern ein anderes Maß von mir, nennen wir es Ko-Regulierung oder wie Sie es meinen, hinkriegen, damit Rahmenbedingungen da sind, die Freiraum schaffen für Produkte, die dann aber ein bestimmtes Niveau haben, was dann auch wirklich läuft.

Prof. Helmbrecht:

Also, ich glaube, ich muss jetzt mal wirklich fünf Minuten benutzen, damit hier etwas Konstruktives herauskommt. Wenn was rauskommen soll, erzähle ich Ihnen jetzt, wie wir das auch machen können. Wir haben in der NIS Direktive die Triple Service Providers drin. Das

sind die Amazons oder die, die dann Dienste anbieten, nicht dass das jetzt Retailer sind, aber die, die Cloud Services anbieten. Im Gesetz steht drin, dass innerhalb der nächsten 21 Monate die Kommission Implementing Acts macht. Wer das nicht versteht, ist nicht schlimm, ich wusste das vorher auch nicht. Implementing Acts heißt, dass wir und andere die Kommission beraten, wie die Kommission das Gesetz umsetzen soll. Das ist die Macht der Kommission, und das ist etwas, damit die Macht der Mitgliedsstaaten weg ist. Da kommt dann irgendwann in den nächsten 21 Monaten ein Gesetz, was da zu machen ist. Es weiß keiner, was zu machen ist. Das sage ich ganz ehrlich. Und es ist in den Verhandlungen der letzten Monate reingekommen. Aber es wird einen Prozess geben, wo Cloud Services in Europa reguliert werden. Die essentielle Frage ist, wer von Ihnen ist denn dann im Prozess drin? Und der nächste Punkt ist, wir haben in der NIS Direktive….

Herr Holz:

Unter anderem die Firma Atos ist mit drin mit Beratungen für das Thema der potenziellen Binnenmarktvoraussetzungen, wie wir auch drin waren in der deutschen Cloud beim BSI, in vielen Regularien waren. Insofern glaube ich, dass hier sehr viel Gutes und Konstruktives läuft. Man ist sich sehr bewusst, dass die Balance, die man zwischen dem Thema Protektionismus und fairer Wettbewerb finden muss, ist genau die Diskussion, die gerade stattfindet. Ich muss wirklich sagen, dass ich überrascht bin über die defizitären Äußerungen von Ihnen als jemand, der auch in Europa ist. Wir müssen dafür kämpfen, dass wir das immer hinbekommen. Und ich sehe Leute, wie Herrn Oettinger, und ich muss Ihnen sagen, dass der Tag und Nacht damit umgeht, wie wir Chancengleichheit hinbekommen, wie der die Länder reinbekommt. Und da kann man nur sagen, dass wir mitmachen. Ich finde, jetzt sollten Sie auch mal diesen konstruktiven Ansatz nutzen, weil sonst gehe ich hier raus und betrinke mich.

Prof. Helmbrecht:

Ja, aber dann lassen Sie uns alle hier auch vor Augen führen – und wir diskutieren hier darüber -, ob wir dann in der gleichen Anhörung, in der gleichen Runde in Brüssel sitzen. Dann gibt es das Struck’sche Gesetz, von Struck stammt der Satz „kein Gesetz kommt aus dem parlamentarischen Prozess raus wie es reingegangen ist“. Wir sind hier mit dem zweiten Punkt. Ich sage Ihnen nur, dass wir in dem Gesetz drin sind an vielen Stellen, aber in Brüssel weiß keiner, wie der Prozess ist. Das ist meine Aussage. Ich bin ja ehrlich hier.

Prof. Helmbrecht:

Ich hab noch zwei Punkte. Wenn wir heute Abend hier rausgehen, dann will ich Ihnen nur sagen, dass in Brüssel Prozesse laufen und dort Entscheidungen getroffen werden. Sie können hier Tausendmal tolle Dinge sagen. Sie können auch als Atos dabei sein; das ist überhaupt kein Problem. Wenn Sie in diesem Raum diese Prozesse in Brüssel nicht durchschauen, dann haben wir in 21 Monaten Dinge implementiert, worüber man lamentieren kann. Ich habe vielleicht eine eigene Art, das darzustellen. Aber was nicht sichergestellt ist, ist, wie die deutschen Industrieinteressen in die Prozesse in Brüssel hineinkommen. Das ist mein Punkt. Und Herr Raab, wir haben uns ja in Brüssel kennengelernt, kennt das aus dem Effeff. Er weiß, an wie vielen Stellen die Lobbyisten Deutsche nicht berücksichtigen. Nichts anderes will ich hier sagen.

NN:

Ich stelle erst einmal die Frage, damit ich das nicht vergesse. Die Frage geht an Sie. Ist denn Regulierung angemessen Selbstverantwortung oder ist das der freie Markt dabei? Folgendes Beispiel: wir haben Cash (?) dahingehend, dass wir die kurzzeitige Zyklen der IT-Technologie mit den langfristigen Zyklen der Investitionsgüterindustrie vermengen. Das führt zu Konflikten. Beispielsweise sieht man daran, wie Produkte eben langfristig, die Schwachstellen werden relativ kurzfristig rausgepackt, werden nur Patches geliefert nach Produkthaftungsgesetz. Wenn es an den Markt kommt, ist es in Ordnung. Aber später ist es nicht in Ordnung. Wenn die Patches nicht kommen, kann ich das Produkt oft lange Zeit nicht nutzen, d, h, ich habe ein Problem dabei. Muss man das regulieren? Werden solche Patches betrachtet wie Ersatzteile? Kann man sagen, dass man etwas erfinden muss wie die Ersatzteilpflicht, Regulierung oder Selbstverantwortung?

Ein anderes schönes Beispiel, dass es noch schlimmer wird, kriegen wir mit den Cloud Diensten. In den USA ist jetzt etwas Wunderschönes passiert und damit kann man sehen, wie schlimm es im Konsumgüterbereich ist. Wir können es aber auch im Investitionsgüterbereich sehen. Das hat die Firma Nest die Firma Re gekauft, die ein kleines Smartphone Artikel hat für 200 $. Damit können Sie Ihr Smartphone steuern. Ich hab das nicht wegen des Produktes gekauft sondern wegen der Leute. Nach gut eineinhalb Jahren haben die gesagt, dass sie die Cloud abschalten. Damit hatten die Leute zuhause zwar ein funktionsfähiges Produkt, Hardware, Software lief, Cloud lief nicht. Die Konsequenz war, dass sie etwas wegwerfen konnten. Die Firma übernahm keine Gewährleistung, weil ein Jahr vorbei war.

Das heißt, dass wir zukünftig auch eine verlässliche Cloud brauchen. Die Firma muss sicherstellen, dass der Cloud Dienst entsprechend läuft. Wenn sie insolvent ist, haben Sie eh ein Problem. Aber hier haben wir keine Insolvenz. Hier haben wir einfach auch ein Gewinnstreben dabei, was eine Abschaltung ist. Da ist die Frage: muss man da nicht regulieren aus Selbstverantwortung heraus oder muss man da gar nichts machen?

Herr Raab:

An dem letzten Beispiel, haben Sie ein Beispiel beschrieben, wo es bei dem Messgerät vielleicht nicht, aber wenn man sich andere Lebensnotwendigkeiten vorstellt, wo man an die Frage kommt, ob wir es mit etwas zu tun haben, was wir in anderen Zeiten mit dem schönen Wort Daseinsvorsorge verbunden hatten. Wir bekommen solche Phasen, wo wir in unserer Lebenssituation sind, wo wir darauf angewiesen sind, dass etwas funktioniert. Wenn man das unter dem Aspekt betrachtet, dass hier ein Unternehmen entscheidet, wie es das für richtig hält und plötzlich stehen die Kunden da und es funktioniert nicht mehr, wird es einen Aufschrei nach Sicherheit geben. So würde ich das einmal nennen. Und wie die dann hergestellt wird, ist eine interessante Frage. Aber da gibt es dann so etwas wie, gibt eine Garantenstellung von jemandem, der dafür einsteht, dass das funktioniert. Ist das der Staat oder was erwarten wir da von ihm? Diese Fragen gehören mit auf die Agenda, wenn wir über Stabilität in der digitalen Zeit reden wollen.

Herr Raab:

Ich glaube, dass das ein typisches Beispiel, wo ich, der ich eine Lanze für die Regulierung gebrochen habe, nicht von Regulierung ausgehen würde. Das ist ein typisches Beispiel von ‚wenn ich diesen Service länger erhalten will, dann muss ich mehr Geld dafür in die Hand nehmen'. Sie haben gerade selber gesagt, dass das 200 $ gekostet hat, ein Pfennigartikel sozusagen. Das macht die Bundeswehr ja täglich. Die Bundeswehr sagt: ich will, dass dieses Device 30 Jahre lang verfügbar ist, diese Karte in dieser Fregatte, jetzt einmal zugespitzt gesagt. Dann verkauft die der auch jemand, der aber mehr Geld dafür haben will. Das ist diese Liefersicherheit, und das regelt sich über den Preis und den Markt.

Herr Sturm:

Im Stenogrammstil stehen ein paar Assoziationen zu dem gesagten. Einen Punkt haben Sie gerade schon genannt. Ersten einmal überwiegen die Chancen der Digitalisierung die Risiken bei weitem. Wir haben natürlich gesellschaftliche Herausforderungen, die wir auch

bewältigen müssen, aber wenn die Digitalisierung schon da ist, müssen wir die Risiken adäquat managen. Wenn wir die Risiken adäquat managen müssen, dann müssen wir uns entsprechend dafür die Frage stellen. Ob wir dafür Regulierung brauchen. Ja, natürlich brauchen wir Regulierung. Aber bitte nicht technische Regulierung, weil nach meiner Erfahrung der technische Fortschritt viel schneller ist als die Regulierung. Ich bin jetzt einige Jahre in Konzernverantwortung. Wenn Sie global im Unternehmen das BDSG (?) umsetzen wollen, ist da die Datenvertragsverarbeitung eine echte Herausforderung. Sie sind ja auch im Unternehmen ein Cloud Provider für legale Einheiten, die weltweit verteilt sind. Es ist eine ziemlich komplexe Herausforderung. Aber immerhin ist es insofern schon einmal gut. Es ist nicht technisch gelöst, sondern es ist logisch gelöst.

Ich nenne Ihnen ein Beispiel der logischen Geschichte. Autonomes Fahren wird momentan im VDA logisch diskutiert. Welche Datenklassen gibt es denn in einem autonomen Fahrzeug und welche sollen, müssen auch aus regulatorischem Auftrag allen bereitgestellt werden? Welche sollten markenspezifisch bereitgestellt werden oder auch der ganzen Branche, die dann als independent Aftermarket auch in der Wertschöpfungskette Zugriff haben sollte? Dann gibt es noch die Klasse, welche Daten dann wirklich in der individuellen Selbstbestimmung des Konsumenten sein sollten, der dann ebenfalls mit einem Wertschöpfungspartner, BMW, Opel oder wem auch immer, direkt in einer Beziehung stehen kann und sagen, dass er diese Daten nur bei sich haben will. Das wird logisch gelöst und wird jetzt auch vom VDA nach Brüssel gelangen. Dann müssen wir sehen, wie es weitergeht. Dann muss die Industrie technisch Lösungen finden. Ich fand den Grundbegriff toll, Herr Raab, need to connect. Es kann sein, dass wir Produkte technisch machen müssen, die dann nie zu connect. Oder in China muss das Elektromobil alle Daten abgeben. Da gibt es nichts zu diskutieren, wenn dann die Gesetzeslage so ist. Wir halten uns an Recht und Gesetz. Deswegen haben sie gar keine andere Wahl, wenn es in dem Land so reguliert ist. Oder Sie sind aus dem Markt. Ich will dann aber eventuell, wenn ich den i3 in Europa kaufe, meine Robinsontaste haben mit dem Schieberegler, so ähnlich wie ich im Browser meine Sicherheitslevel einstellen kann. Lieber mehr Sicherheit und weniger Nutzen, oder ich will mehr Nutzen und weniger Sicherheit. Dafür brauchen wir dann technische Lösungen, weil es nützt überhaupt nicht, etwas zu regulieren, was man dann technisch nicht umsetzen kann.

Prof. Eckert:

Für die, die die Robinsontaste nicht kennen – ich kannte sie auch nicht und Herr Sturm hat sie mir auch erklärt -, das ist die Taste, die Sie dann auf eine einsame Insel katapultiert. Sie werden abgeschottet, also isoliert. Herr Arnold war der nächste.

NN:

Ich hätte eine andere Frage. Was wir heute noch kaum beleuchtet haben, ist folgendes. Regulierung, Selbstregulierung, Verantwortung ist fast wie: die guten Jungs sagen den guten Firmen wie sie gute Produkte bauen sollen. Unsere neuen Services kommen vielleicht deshalb gar nicht zustande. Es gibt nämlich auch die andere Seite, mit der wie jeden Tag konfrontiert sind. Die bösen Jungs schalten diese Services einfach ab. Wer haftet dann beispielsweise? Weil wir vorher das Thema Produkthaftung hatten. Ist das dann so wie in meinem Vertrag für mein Haus? Eigentlich gegen alles versichert, aber wenn das Atomkraftwerk durchgeht, hast du einfach Pech gehabt. Ist zwar alles kaputt, aber es gibt keinen mehr. Wer haftet bei solchen aktiven Disruptions? Wer steht da in der Pflicht? Wer tut was? Jetzt haben wir leider nur noch einen Regierungsvertreter hier. Was tun wir denn, um diese bösen Jungs aus dem Spiel zu nehmen, dass wir dieses Problem gar nicht haben? Sonst sind diese kleinen technischen Regulierungsfragen, wenn einer die Gesundheitskarte abschaltet, wenn einer den ganzen Verkehr auf der Autobahn lahmlegt und Hunderte rasen ineinander ein. Da stellen sich andere Fragen Das ist nicht nur ein bisschen Technik, sondern da hat aktiv einer etwas gemacht. Wie geht man mit diesem Thema um?

Prof. Eckert:

Ist das eine neue Fragestellung Herr Duisberg oder ist das nicht einfach auch durch eine normale Verletzung oder durch irgendwas im Strafrecht auch schon abgedeckt?

Dr. Duisberg:

Wenn sich die Frage auch an mich richtet und Sie sozusagen das Opfer eines Cyberangriffes werden, dann müssen Sie sich zunächst einmal an den Angreifer wenden. Das ist eigentlich die Logik. Wenn Sie einen CIO haben, der dafür gesorgt hat, dass Ihre Systeme robust sind, dann ist es nicht zum Cyberangriff gekommen. Wenn es trotzdem zum Cyberangriff gekommen ist, dann ist die Frage, wie sorgfältig Sie mit Ihrer Ausstattung waren. Und dann kommen Sie irgendwann in die Betrachtung, wie gut eigentlich dieses Produkt war, das in den Verkehr gebracht wurde und gab es möglicherweise doch eine Verpflichtung des Herstellers

gab, eigentlich für eine Cyberrobustheit des Produktes zu sorgen. Nach dem Stand heute haben Sie erst einmal Pech gehabt.

Nur, wenn Sie ein Fahrzeug heutzutage auf die Straße bringen, das sozusagen ein offenes Scheunentor ist für jede Art pure Invasion, dann handeln sie vielleicht sorgfaltswidrig, weil Sie wissen, dass das passieren kann. Das heißt, es gibt schon eine gewisse Eigenverantwortung des Herstellers und das ist die Frage, in welchem Grad Sie sich eigentlich bewegen. So würde man das betrachten, und das sagen Ihnen ohne Regulierung irgendwann die Gerichte.

Prof. Helmbrecht:

Das Problem ist ja folgendes. Wenn Sie Europa mit in den Lissabon Vertrag nehmen, ist das reiner Binnenmarkt. Das heißt, für alles was die Kommission macht, Oettinger und andere machen, ist das Ziel, diesen europäische Wirtschaft voranzubringen. Das Problem in unserem Geschäft ist, wenn IT-Sicherheit ist und diese Angriffe da sind, dann müssen Sie erst einmal ganz klar sagen, ob das Computerkriminalität oder Sabotage ist. Dann ist die nächste Frage, ob das in einem Mitgliedsland ist. Wenn es in einem Mitgliedsland ist, dann ist es die Zuständigkeit des Mitgliedslandes. Da macht keiner europäisch etwas. Nur wenn es mehrere Mitgliedsländer betrifft, also grenzüberschreitend ist, dann – und da haben wir in Europa noch ein Problem – ist die Frage, wie wir damit umgehen. Das ist immer noch ein Fragezeichen. Wenn Sie 2007 Estland kennen und das würde heute wieder passieren, würde wieder keiner etwas machen. Das ist das Schuldproblem. Wir von der ENISA machen – das haben wir gerade heute Morgen begonnen - alle zwei Jahre eine Jahre eine Cybersäuberung in Europa. In unserem Abschlussbericht, letzter war 2005 Dezember, steht jedes Mal drin, dass es in der technischen Ebene wunderbar funktioniert. Wenn so etwas passiert, können Sie mit Verbund der anderen Staaten, wir haben ungefähr 1000 Institutionen dieses Mal dabei, sich mit denen unterhalten, aber einfach nur in dem Sinne, wie Sie das Problem lösen. Dass Sie nur technisch lösen, dass es hinterher wieder läuft, aber nicht juristisch. Es steht jedes Mal in unserem Bericht, dass die horizontale Ebene funktioniert und die vertikale nicht. Es gibt kein europäisches Krisenmanagement. Es gibt keinen zuständigen Kommissar. Das gibt es heute nicht. Das ist ein weißer Fleck in der europäischen Landkarte.

NN:

Ich möchte noch etwas ganz anderes sagen Wir reden über Begriffe, über das richtige Maß und mich würde interessieren, wie wir dazu kommen. Wir brauchen für das richtige Maß auch einen Qualitätsbegriff. Entsteht der jetzt deduktiv direktiv in Brüssel oder müssen wir uns dem deduktiv iterativ in der Bemühung der kollektiven Intelligenz des Teams bemühen? Und wenn wir iterativ induktiv arbeiten müssen, haben wir dann überhaupt die richtigen Strukturen, um die kollektive Intelligenz zu aktivieren, das einzusammeln? Ich bin Mathematiker und habe das früher einmal ganz intensiv gemacht mit dem Security und wollte das eigentlich nie mehr tun, weil mich das vor zehn Jahren schon gestört hat. Ich bin jetzt wieder in dem Thema. Wir haben es hier mit Emergenz zu tun. Security passiert in einem Kontext, wo ich Dinge nicht voraussehen konnte. In dem Begriff Komplexität steckt Emergenz. Jetzt muss man sich überlegen, ob man Emergenz deduktiv überhaupt beherrschen kann. Der Begriff Emergenz existiert dadurch, weil es deduktiv nicht geht. Also, muss man mit Emergenz iterativ induktiv arbeiten. Alle Dinge, die ich hier von Ihnen sehe, sind alles deduktive Weisheiten. Damit kriegen sie es nach meiner Erfahrung nicht hin. Ich bin jetzt bei Bosch in diesem Gremium, mit dieser Strategie und wir werden versuchen, dass ein bisschen anders zu machen, und vielleicht kann ich meine Theorie verkaufen. Und vielleicht können Sie mir helfen. Finden Sie einen Qualitätsbegriff und erklären Sie mir, wie Sie zu dieser Erkenntnis kommen wollen!

Herr Raab oder Dr. Duisberg:

Ich antworte nicht ganz genau darauf, weil ich intellektuell nicht ganz folgen konnte und weil ich kein Mathematiker bin. Aber ich glaube, um das auch noch einmal zu sagen, dass es eine Riesenchance ist, worüber wir gerade hier reden. Überlegen Sie sich einmal, wie wir vor einigen Jahren über das Thema Umwelt geredet haben. Wie wir hier alle saßen und dann eine Energiewende kam und wir alle gesagt haben, dass jetzt die Welt zusammenbricht. Auf einmal ist die deutsche Industrie, ein Siemens Weltmarktführer in Windkraftwerken. Auf einmal haben wir Innovationen. So ein bisschen sehe ich die Analogie zu diesem Thema Security.

Herr Duisberg:

Das finde ich fair, dass Sie polemisch antworten, weil ich auch polemisch begonnen habe. Aber ich sehe das wirklich so. Sie kriegen mich hier auch nicht runter. Und da können Sie noch eine Stunde mit mir diskutieren. Ich sehe hier Chancen. Ich sehe hier eine Chance für

unseren Standort qualitativ inhaltlich. Dass wir nämlich unsere Produkte, unsere Dienstleistungen mit einer Qualität versehen, die sich Security nennt. Die wird nie 100%ig sein, weil wir sie nie 100%ig hinkriegen. Insofern sehe ich hier die gleiche Analogie wie mit dem Thema Umwelt. Erinnern Sie sich an die Diskussion, die wir hatten und wenden Sie das auf das an, was wir heute diskutiert hatten. Genau deshalb finde ich das Thema so wichtig. Aber noch einmal, es ist ein so komplexes Thema; das Thema Datenschutz habe ich jetzt nicht adressiert. Das sind noch ganz andere Themen. Jetzt einfach mal auf das Thema Security und Qualität. Es kam und wir sehen eine Riesenchance für uns. Und nächste Woche beginnt die ETSA (?). Genua ist das. Gehen Sie auf die ETSA! Das ist die Weltmarktmesse für Security. Ja, die ist wirklich klein, wird aber immer größer und da sind mittlerweile alle großen Unternehmen vertreten. So müssen wir das Thema angehen, und da muss Europa mit helfen. Da müssen wir als Deutschland mitwirken, dass wir das Thema so hinkriegen.
Deswegen sage ich hier, dass das eine Riesenchance für uns ist.

Herr Barth:
Ich wollte direkt etwas dazu sagen, weil da war anscheinend etwas, was Sie extrem gestört hat, aber nicht so sehr, als dass es Sie jetzt noch interessieren würde. Ich weiß nicht, ob Ihnen das reicht. Aber so rein aus technischer Sicht gibt es Evaluierungs- und auch Nachweisführungsmodelle, die mathematisch nachweisen können, ob ein System oder eine Plattform nach dem Kenntnisstand, den wir haben, sicher ist oder nicht.

Prof. Eckert:
In diese Diskussion können wir uns jetzt beliebig einlassen, aber das wollen wir nicht.

NN:
Diese Diskussion läuft ähnlich divergent wie ich sie seit zehn Jahre kenne, wenn es um die Prinzipien geht, mit denen wir vorgehen. Es geht um Methodenfragen. Wir haben Dinge, die absolut gesichert sind. Das ist unser Rechtsrahmen. Nehmen Sie das Zivilrecht, das Ordnungsrecht und als Letztes die Verfassung. Was wir jetzt neu bestimmen müssen, ist keine neue Regulierung, sondern wir müssen der Regulierung, die es schon gibt, Geltung im Internet verschaffen. Da kommt dann die Frage von jemand wie ‚ich darf im Internet nicht bescheißen'. Ich denke, das ist ein Freiraum. Und das müssen wir begrenzen. Es gibt auch Naturgesetze, die wir nicht außer Kraft setzen können. Nehmen wir die Schwerkraft. Da läuft das Wasser den Berg runter und warme Luft steigt nach oben. Da können wir keinen

Kompromiss machen, weil die EU sich nicht einigen kann. Wir haben doch einfach Rahmenbedingungen und allgemeine Zusammenhänge, die wir nicht negieren können. Wir müssen das, was wir leben, fortschreiben und wir müssen dort, wo Fehler sind, Anpassungen vornehmen. Und das ist ein Fortschritt in der Kultur. Im Grunde genommen arbeiten wir an unserer ganzen Zivilisation und darein müssen wir investieren, damit wir eine Zukunft haben. So können wir nicht weitermachen. Wir fahren die Kugel vor die Wand.

Das Internet ist ein wertvolles Werkzeug, um Probleme wie demografischer Wandel, Energiewende in den Griff zu bekommen. Daran müssen wir arbeiten. Wenn Sie durch Regulierung eine Hemmung in der Innovation befürchten, dann stimmt das nicht, denn Sie erfüllen nur eine zusätzliche Anforderung. Innovativ können Sie immer bleiben. Sie dürfen es nur nicht als Regulierung empfinden, sondern Sie müssen ein Leistungsbewusstsein haben, um die Anforderung mit zu erfüllen. Die Anforderung IT-Security ist eine absolut notwendige, sonst läuft unsere Zivilisation aus dem Ruder. Noch einmal: Milliarden von Geräten ohne Identität, die beliebig zusammenwirken, das ist Chaos. Und Chaos können wir uns nicht leisten.

Dr. Sturm:
Wenn Sie mich direkt angesprochen haben, so habe ich Sie verstanden, stimme ich Ihnen zu. Wenn es so rüberkam, dass die Regulierung, wenn wir aber falsch regulieren und genau versuchen, solche Themen Technik zu begrenzen. Ich stimme Ihnen zu. Es war genau mein erstes Statement, dass die Chancen der Digitalisierung bei weitem die Risiken überwiegen. Wir müssen die Risiken managen. Ich kann Ihnen mathematisch nicht folgen, aber wir müssen uns iterativ da hineinbewegen, wie sämtliche kulturellen und industriellen Revolution…. Da gab es immer Turbulenz und wenn Sie nicht entsprechend nicht in der Turbulenz und iterativ rangehen, gibt es keinen Fortschritt.

NN:
Ich kann nur zustimmen. Wenn ich das im Unternehmenskontext betrachte, aus dem Blickwinkel einer unternehmensinternen Security Governance. Wenn ich als Security Verantwortlicher im Unternehmen zu strikt, meine Forderungen zu hoch ansetze, dann bin ich durchaus in der Lage Innovationen abzuwürgen, bevor sie überhaupt das Licht der Welt erblickt haben. Das ist etwas, wo man sehr vorsichtig sein muss. Natürlich versuchen wir immer, das Risiko gegen null zu managen. Wir wissen, dass die Kosten gegen unendlich

gehen und versuchen das näherungsweise iterativ irgendwie zu optimieren, weil wir nicht genau wissen, wo der Punkt liegt. Was viele aber ignorieren, und da nehme ich gerade die Sicherheitsverantwortlichen in die Pflicht, ist die Fähigkeit, Innovationen zu . Wenn ich zu wenig in Security investiere, laufen meine Innovationen vor die Wand, weil ich dem Kundenaspekt nicht genügend Rechnung getragen habe. Wenn ich aber zu strikt bin, würge ich Innovationen ab, bevor ich überhaupt verstanden habe, wie das Geschäftsmodell dahinter aussehen kann. Auch da muss man vorsichtig sein. Man kann nicht die Latte immer so hoch legen, weil es das Maximum ist, was ich…..

NN:
Wie Sony und wir diskutieren über die Festlegung der Grenzwerte. Da gibt es eben Schutzklasse 1. Das ist und Schutzklasse 7 ist das Handy von Frau Merkel. Wir müssen für jede Anwendung sagen, was wir uns an Schutzbedarf von dieser Anwendung vorstellen. Das ist eine einfache Diskussion mit den Marktteilnehmern. Dann legt man das fest. Die Schutzklasse für Gesundheit

NN:
Die Diskussion läuft schon im vierten Jahrzehnt. Ich bin aktiv teilnehmender Beobachter und sozusagen Experte über die Diskussion. Mich überraschen einzelne Positionen nicht, weil die immer wieder kommen. Wir führen die Diskussion sehr intensiv und sind uns insgesamt nicht sicher, ob wir uns im Kreis bewegen oder auf der Stelle treten. Aber eins von beiden muss es sein.

Herr Sturm hat vorher ein Beispiel gebracht, wo man sich einig sein muss. Zu Herrn Holz weiß ich, dass eine Akteurs gruppe hier fehlt, die uns seit fast 40 Jahren Probleme macht und das es auf Dinge ankommt, die gemeinsam getan werden müssen.

Ein konkretes Beispiel. Sie erinnern sich, die digitale Signatur hat dadurch stattgefunden, dass ich in der Lage war, dem Alexander Roßnagel an der Uni Darmstadt ein ganz hoch modernes Faxgerät zur Verfügung zu stellen. Dann lief zwischen unseren Faxgeräten die Entwicklung der digitalen Signatur. Da war eine der klaren Forderungen, da waren alle Definitionen drin, die wir heute genannt haben. Da waren alle Forderungen drin. Aber dann ging es los, dass man sagte, dass sich alle zusammentun müssen. Interessanterweise ist der Satz heute nicht gefallen. Der müsste noch kommen. IT-Sicherheit kostet Geld, und zwar richtig Geld. Jetzt ist

es so, dass alle um den Tisch rumsitzen und sagen, dass diese digitale Signatur eine prima Idee ist und alle wollen mitmachen, die Banken, die Sparkassen usw. Blöderweise hat sich niemand gefunden, der anfängt. Jeder hat gesagt, dass der andere anfangen soll. Das ist ein Gesetz, was wir nun einmal in der Wirtschaft haben. Wer anfängt, ist nicht immer der Gewinner. Jetzt kommen wir auf den Punkt, der bei der Breitbandentwicklung eine Rolle gespielt hat. Ihr Beispiel kann ich da deutlich sagen. Es müssen tatsächlich einheitliche Regeln umgesetzt werden von allen beteiligten Unternehmen. Stellen Sie sich einmal vor, dass fünf Unternehmen zusammen arbeiten und locker die Milliarde für Vorausinvestitionen ausgeben wollen. Das wird sogar noch unterstützt vom Staat. Sie bekommen Forschungszuschuss. Kooperiert doch! Jetzt ist nun einmal so, dass wir als Unternehmen überlegen müssen, wo unser Payback ist. Und dann möchte der, der mit 200 Millionen beteiligt ist, 20% von dem Markt zurückhaben. Und der nächste möchte 30% zurück. Spätestens dann kommen die Handschellen vom Kartellamt.

Diese simple Sache, dass wir im Wettbewerb alles zusammen machen dürfen außer wirtschaften. Das dürfen wir nicht zusammen.

Mein letzter Punkt sind die Amerikaner, und es gibt gleich eine Antwort auf Herrn Holz. Ich habe gerade selber eine Analyse gemacht, nach der die Amerikaner bis heute glauben, dass die Lösungen für IT-Sicherheit eigentlich von den Deutschen kommen müssen. Die sind fest davon überzeugt und wundern sich, dass von denen nichts kommt. Die fangen jetzt schon selber an, nach dem deutschen Prinzip zu machen. Ich möchte diesen Unterschied einfach noch einmal nennen. Wenn zwei amerikanische Unternehmen sich um einen Markt streiten, sind die sich einig, ohne ein Wort miteinander gewechselt zu haben, dass kein Ausländer diesen Markt kriegen wird. Einer von ihnen kriegt es, der Überlebende, aber kein Ausländer. Da reden die nicht drüber. Da gibt es keine Verabredung. Da gibt es nicht wie bei BSI (?), Siemens und SEL Telefonate, damit es einheitlich wird.

Das passiert in Europa und speziell in Deutschland nicht. Da ist wieder dieser Kreislauf unter dem Motto ‚der Beste wird gewinnen' egal ob das ein Ausländer ist. Weil der Name Merkel fiel, muss man ein einem Punkt sagen, dass sich Frau Merkel in einem Zusammenhang mit dem IT Gipfel, als sie den von der vorigen Regierung übernehmen sollte, an einem Wochenende in alles eingearbeitet und festgestellt, dass alles, was wir in der IT Branche produziert hatten an Charts und Power Point Orgien, heiße Luft ist. Sie hat dann auf dem IT

Gipfel, den sie doch gemacht hat, Bitkom gelobt. Ich saß hinten drin und habe es verstanden. Sie hat gesagt: ich mag einfach alle Exportbranchen, weil das bei uns die Arbeitsplätze sichert. Aber die IT Branche war und ist keine sondern das ist eine Importbranche.

Das ist heute auch in unserer Diskussion ganz schwierig zu sagen, wenn wir eine neue Sicherheitsarchitektur brauchen, müssen wir auch sehen, ob wir Zugriff auf die Architekten haben, die das machen. Und das ist der Punkt. Da haben wir eine Schwäche, weil wir immer wieder sagen: exportiere doch die gute Idee nach USA und reimportiere sie nach amerikanischem Muster, dann liegen wir richtig. Wir brauchen, und da gebe ich Ihnen vollkommen Recht, viel mehr Selbstbewusstsein und diesen Kooperationsgeist. Notfalls machen wir die Verhandlungen im Innenhof vom Kartellamt. Da geht das.

Eine Fußnote muss noch erlaubt sein, die Versicherungen bei dem Auto und beim autonomen Fahren oder überhaupt bei dem vernetzten Auto. Das ist heute schon sehr gut gesagt worden. Aber stellen Sie sich einmal vor, dass jetzt der erste Fall in den USA eingetreten ist, dass ein Versicherungsnehmer einen Unfall gehabt hat. Er hat seine Daten für einen billigeren Tarif abgeliefert und die Versicherung hat festgestellt, dass der eine Mitschuld hat aufgrund der Daten, die er selber abgeliefert hat. Jetzt ist sein Vertrauen in seine eigene Versicherung ein bisschen verloren gegangen. Sie verstehen, was ich damit sagen will. Das wird hier überhaupt nicht diskutiert, sondern es wird gesagt: Daten, wem gehören die? Das ist auf jeden Fall ein Geschäftsmodell und ich bin gespannt, wie das juristisch behandelt wird. Aber ich will es dabei belassen.

NN:

In aller Kürze. Ich hatte gehofft, Herr Holz würde sich noch äußern. Zu dem Thema hat er gemeint, Security verkauft sich wie Butter und Brot. Ich bin jetzt seit über 20 Jahren in der Branche und ich kann Ihnen versichern, Security ist total unsexy. Keiner gibt gern Geld aus für das Thema. Es kostet Geld. Kein Return of Investment. Die Stakeholder verstehen in der Regel nicht, wofür sie ihr Geld ausgeben, die CEOs dieser Welt. Dann kommt einer um die Ecke und erzählt, dass er seine Infrastruktur absichern muss. Wo haben die gelebt, kein Richter und kein Henker. Bei mir gibt es keine bösen Jungs und wir werden nicht angegriffen. Das dazu.

Vielleicht noch abschließend eine Sache. Im Bereich Security wird immer diskutiert, welche Daten erhoben werden, was damit gemacht wird. Wir haben noch nicht beleuchtet, wieso wir immer davon ausgehen, dass diejenigen, die die Daten eventuell abholen, vielleicht gar nicht das Recht haben, diese Daten zu erheben, nichts Gutes im Schilde führen. Das heißt, die Daten werden nicht dafür genutzt , sondern die Daten werden erhoben, um zu wissen, wer man ist, was man macht etc. Also, es gibt nie gute Vorsätze, was diese Daten angeht und was diese Datenauswertung angeht.

Prof. Eckert:
Gut. Jetzt muss ich etwas tun, um dieses Black Szenario, was gerade über uns schwebt, wieder ins Positive zu drehen. Wir haben geendet mit den bösen Jungs, die unsere Daten für ungute Zwecke absichern. Ich ende einfach mit einem Dank.

Wir haben genau das erreicht, was wir erreichen wollten, die verschiedensten Aspekte hier einfach einmal breit zu diskutieren. Es war klar, dass wir hier nicht zu Lösungen kommen werden. Es war klar, dass hier Dinge aufeinander prallen. So stark habe ich es nicht erwartet.
Ich denke, dass es viele unterschiedliche Sichten gab und das ist auch gut so. Wir sind überhaupt nicht am Ende von einer solchen Diskussion.

Ich möchte mich ganz herzlich bei allen Panellisten bedanken für den wertvollen Input, ihre Bereitschaft, bis in die späte Nacht Rede und Antwort zu stehen.
Ich möchte mich bei Ihnen bedanken und das letzte Wort hat Heinz Thielmann.

Prof. Thielmann:
Ich möchte mich auch noch einmal ganz herzlich bedanken im Namen des MÜNCHNER KREISES. Ich hoffe, Sie haben einen Eindruck mitgenommen für die, die zum ersten Mal bei einem Berliner Gespräch dabei waren, wie wir im MÜNCHNER KREIS arbeiten, nämlich möglichst viel Diskussion angeregt durch ein paar Impulsvorträge und Statements. Das ist uns, glaube ich, auch gelungen. Vielen Dank auch noch mal von mir. Wir haben die gesamte Diskussion aufgezeichnet, was aber kein Thema für den Datenschutz ist. Das bleibt bei uns. Wir werden aber die Aufzeichnung auswerten und ein paar wesentliche Statements anonymisiert Ihnen mitgeben oder bereitstellen. Wir werden auch daraus für das nächste Jahr eine eintägige Fachkonferenz gemeinsam planen. Wenn sich abzeichnet, mit parallelen Workshops zu einzelnen Themen. Ich denke, dass wir vielleicht noch einmal eine Abfrage bei

allen Teilnehmern machen können, welche Themen für Sie wichtig sind. Das soweit zum Abschluss, zum Organisatorischen. Vielen Dank und bis zum nächsten Mal.

Prof. Eckert:

Darf ich noch mit dem allerletzten Wort enden? Wir haben einen neuen Arbeitskreis Cyber Security gegründet im MÜNCHNER KREISES. Das ist eine Veranstaltung aus unserem Arbeitskreis heraus. Viele von den hier Anwesenden arbeiten da schon aktiv mit. Wenn Sie Interesse haben, dort auch mitzuwirken, herzlich gern. Schreiben Sie mir eine Mail. Sie werden aufgenommen, bekommen auch Zugang zu den Protokollen, zu den Aktivitäten, die schon gelaufen sind. Wir freuen uns um weiteren Input, denn der heutige Abend hat es gezeigt: je mehr, je vielfältiger wir diese Themen vorantreiben in den internen Diskussionen, um sie dann wieder nach draußen zu bringen, desto besser. Also, machen Sie mit, gestalten Sie mjt! Das wäre meine Bitte.