Michael Dowling
Jörg Eberspächer
Heinz Thielmann

Herausgeber

Stärkung der IT-Sicherheitswirtschaft in Deutschland

MÜNCHNER KREIS
Übernationale Vereinigung für Kommunikationsforschung
Supranational Association for Communications Reseach

Impressum

Herausgeber:

Prof. Dr. Michael Dowling
Universität Regensburg
LS f. Innovations- und Technologiemanagement
93040 Regensburg
michael.dowling@wiwi.uni-regensburg.de

Prof. Dr.-Ing. Joerg Eberspächer
Technische Universität München
Kommunikationsnetze
Arcisstr. 21
80333 München
joerg.eberspaecher@tum.de

Prof. Dr. Heinz Thielmann
Emphasys GmbH
Eichenstr. 11
90562 Heroldsberg
heinz.thielmann@t-online.de

Reihenherausgeber:
Münchner Kreis – Übernationale Vereinigung für Kommunikationsforschung e.V.
Tal 16
80331 München
www.muenchner-kreis.de
office@muenchner-kreis.de

Redaktion:
Dipl.-Phys. Volker Gehrling
Münchner Kreis – Übernationale Vereinigung für Kommunikationsforschung e.V.
v.gehrling@muenchner-kreis.de

Print:
Knecht-Druck, München

ISBN 978-3-944837-06-2

Vorwort

Die deutsche Sicherheitswirtschaft ist sehr „kleinteilig“ aufgestellt. Das belegen die Studien „Die Sicherheitswirtschaft in Deutschland“ und „Der IT-Sicherheitsmarkt in Deutschland“ im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi) aus dem Jahr 2013: Von ca. 10.000 Unternehmen mit ca. 450.000 Mitarbeitern (vorwiegend KMUs) in den Segmenten Produkte, Dienstleistungen und Beratung sind ca. 70 - 80% ausschließlich auf dem nationalen Absatzmarkt aktiv. Die ausgeprägte Fachkompetenz in den Unternehmen und in der Forschung (Universitäten, F&E-Organisationen, etc.) könnte der deutschen ITSicherheitswirtschaft eine starke Position im Weltmarkt verschaffen, wenn technisch und vertrieblich die Kräfte besser gebündelt würden.

Für das Auftreten in internationalen Märkten sind Referenzen, Größe und Gesamtangebote von Lösungen in der Regel entscheidend. Hier ist auch ein „Mitnehmen“ der KMUs durch große im globalen Markt tätige Unternehmen für alle Seiten vorteilhaft. Die KMUs sind überwiegend „gesund“ und aus eigenen Mitteln finanziert, jedoch fehlt oft der Anreiz für eine Bündelung der Kräfte durch öffentliche Auftraggeber bzw. durch die Wirtschaft als Kunden. Die aktuelle Diskussion über Cybersicherheit hat einen wachsenden Bedarf nach gesamtheitlichen Sicherheitslösungen für die öffentliche Verwaltung und für die gesamte Wirtschaft verstärkt.

Die Zeit ist also reif für eine zielgerichtete Diskussion und Handlungsoptionen zur Stärkung der IT-Sicherheitswirtschaft in Deutschland. Für den internationalen Markt fehlt neben den Referenzen aus dem Heimatmarkt oft auch eine Wachstumsfinanzierung. Neben evtl. staatlichen Hilfen ist vor allem die Finanzwirtschaft gefordert (Venture Capital, Business Angel etc.). Einige wenige VCs sehen hier Möglichkeiten für eine stärkere Fokussierung ihrer Investments.

Der MÜNCHNER KREIS hat bei einem Gespräch mit Herstellern, Anwendern/Bedarfsträgern, Systemintegratoren, Finanzinvestoren und Politik/Ministerien die Situation der IT-Wirtschaft und Handlungsoptionen diskutiert. Der vorliegende Tagungsband enthält die Vorträge und die überarbeiteten Mitschriften der Diskussionen.

Allen Referenten und Diskutanten sowie allen, die zum Gelingen der Konferenz und zur Erstellung dieses Buches beigetragen haben, gilt unser herzlicher Dank!

Michael Dowling Jörg Eberspächer Heinz Thielmann

Inhalt

1 Begrüßung und Einführung

Prof. Dowling, Universität Regensburg und MÜNCHNER KREIS

Sehr geehrte Damen und Herren, für diejenigen, die mich noch nicht kennen: mein Name ist Michael Dowling, und ich bin der Vorstandsvorsitzende des MÜNCHNER KREIS und Professor an der schönen Universität Regensburg.

Ich freue mich, dass so viele an unserem 7. Berliner Gespräch teilnehmen. Prof. Dr. Heinz Thielmann organisierte während der vergangenen Jahre sieben Gesprächsabende zu vielen verschiedenen Themen. Bei den letzten ging es um das Thema „Energy“, aber heute Abend sprechen wir über IT- Sicherheit in Deutschland.

Und dies ist gerade für den MÜNCHNER KREIS ein besonders aktuelles Thema, da der Chef unseres Forschungsausschusses, Prof. Dr. Eberspächer, gestern um 6 Uhr bemerkte, dass unsere Webpage gehackt wurde. Es dauerte etwas, aber nun sind wir wieder online. Keine Sorge, Sie finden uns weiterhin unter der gewohnten Webadresse, und die Präsentationen dieser Veranstaltung werden ins Netz gestellt.

Ich übergebe an Herrn Bub von EIT ICT Labs, der heute Abend unser Gastgeber ist und der Sie ebenfalls kurz begrüßen möchte, bevor Herr Thielmann thematisch in den Abend einführen wird.

2 Ausgangspunkt und Ziel der Veranstaltung

Prof. Heinz Thielmann, MÜNCHNER KREIS

Guten Abend meine Damen und meine Herren. Ich darf zunächst begrüßen Herrn Martin Schallbruch, IT-Direktor des Bundes im Bundesinnenministerium des Innern (BMI), und Herrn Andreas Reisen, Referatsleiter im BMI, sowie vom Bundeswirtschaftsministerium Herrn Dr. Grabowski, Referat Sicherheitswirtschaft, und Sie alle als Gäste aus der Wirtschaft und aus der Forschung.

Unser Thema heißt heute „Stärkung der IT-Sicherheitswirtschaft in Deutschland“, wozu wir einige Impulsvorträge vorgesehen haben.

Zunächst möchte ich mich bei Herrn Dr. Bub und seinen Mitarbeiterinnen und Mitarbeitern bedanken, die hier für die Logistik und die Räumlichkeiten gesorgt haben. Wie Herr Bub bereits angedeutet hat, war es mit der Vielzahl der Anmeldungen etwas schwierig, aber wir haben trotzdem für 100 Teilnehmer Platz gefunden.

Ich möchte mich auch bei unserem Programmausschuss bedanken, der bei der Vorbereitung mitgeholfen hat, und bei unserem Team des MÜNCHNER KREIS.

Der Anlass für diese Veranstaltung – der MÜNCHNER KREIS ist ja eine neutrale Plattform zwischen Politik, Wirtschaft und Wissenschaft - sind zwei Studien des Bundeswirtschaftsministeriums zur Sicherheitswirtschaft in Deutschland und zum IT-Sicherheitsmarkt in Deutschland im letzten Jahr. Bei der einen Studie hat die Organisation BIGS und das Unternehmen IABG mitgewirkt - Herr Dr. Stuchtey und Herr Köhler sind hier anwesend - und es gab noch eine weitere Studie zur IT-Sicherheitswirtschaft. Beide sind im Netz zum Download verfügbar. Die Zahlen zeigen, dass ca. 10.000 Unternehmen mit 450.000 Mitarbeitern vorwiegend KMU‘s in den Segmenten Produkte, Dienstleistungen und Beratungen tätig und davon ca. 70% ausschließlich auf dem nationalen Absatzmarkt aktiv sind. Das war für uns, den MÜNCHNER KREIS, der Auslöser, doch einmal mit Ihnen zu diskutieren und zu überlegen, ob wir nicht in der deutschen Sicherheitswirtschaft unsere Kräfte und unser Wissen besser zusammenführen können, um unsere Position in Markt und Technik zu stärken.

Es gibt auch eine Pressemitteilung vom Institut BIGS vom 19. Mai 2014, die zeigt, dass die IT-Sicherheitswirtschaft in diesem Jahr um ca. 6% wächst. Und es gibt eine Mitteilung des Bundeswirtschaftsministeriums vom 5. September 2014 mit Wirtschaftsminister Gabriel, die die deutsche Sicherheitsindustrie betraf und auch zu dem Thema IT-Sicherheit, Security Stellung genommen hat.

Der Ablauf des Programms liegt Ihnen vor; ich werde die Vortragenden der jeweiligen Vorträge und Impulsvorträge ankündigen. Wir werden eine Audioaufzeichnung von der gesamten Veranstaltung machen und Sie werden einzeln, sowohl diejenigen, die die jeweiligen Vorträge und Impulsvorträge halten, wie auch die Teilnehmer der Diskussion, den Text zum Redigieren bekommen. Wir werden dann alles in einem E-Book zusammenfassen, sowohl die Statements als auch die Diskussionsbeiträge und Ihnen zur Verfügung stellen. Wer von Ihnen ergänzend dazu für sein Unternehmen eine PowerPoint Präsentation schicken möchte, die wir mit in das E-Book aufnehmen, kann das gern tun.

Ich habe in meinem Handout als Teil Ihrer Unterlagen ein paar Fragen zusammengestellt. Es geht um die Fragen wie z.B., welche IT-Sicherheitsunternehmen Partner suchen, sowie Stärken und Schwächen der Sicherheitsunternehmen; alles Themen, von denen ich erwarte, dass sie im Laufe des Abends diskutiert werden. Ich würde mir wünschen, wenn wir zum Schluss vielleicht ein paar Themen selektieren, zu denen sich kleinere Gruppen zusammenfinden, die dann die Fragen über Zusammenarbeit und Handlungsbedarf weiter vertiefen. Eventuell können wir auch ein Positionspapier an die Politik, die Kanzlerin oder den Wirtschaftsminister formulieren als Ergebnis aus der heutigen Veranstaltung. Wenn die heutige Veranstaltung positive Ergebnisse bringt, haben wir vorgesehen, dass wir im nächsten Jahr einige Folgeveranstaltungen dazu durchführen werden.

Das kurz zu meiner Einführung. Ich darf jetzt Herrn Schallbruch bitten, zum Thema „Deutsche Technologiekompetenz: Grundlage für vertrauenswürdige IT“ zu sprechen.

3 Deutsche Technologiekompetenz: Grundlage für vertrauenswürdige IT

Martin Schallbruch, IT-Direktor im Bundesministerium des Innern, Berlin

Guten Tag, meine sehr geehrten Damen und Herren. Ich freue mich, dass der MÜNCHNER KREIS das Thema „Stärkung der deutschen Sicherheitswirtschaft“ erneut aufgreift. Das ist kein Thema, das wir zum ersten Mal diskutieren, das völlig neu ist. Wir diskutieren diese Fragestellung seit bestimmt 20 Jahren und man kann sich natürlich fragen, ob es zu diesem Thema eigentlich hier und heute Neues beizutragen gibt. Als ich den Titel gelesen habe, dachte ich, das ist ein Thema, das mit altbekannt vorkommt und von dir wird erwartet, dass du Neues dazu beiträgst. Kannst du diese Erwartung eigentlich erfüllen?

Wenn ich so ungefähr 20 Jahre zurückdenke – das BSI war gerade im Kindergarten und dürfte ungefähr so 3, 4 Jahre alt gewesen sein -, dann war die Frage der IT-Sicherheit auch damals schon eine Frage, die aktuell war. Wir haben uns damals mit der Frage beschäftigt, wie sicher dieses oder jenes System und wie ein System abzusichern war, welche Risiken bestehen und was man dagegen tun kann.

Seit damals haben wir eine Entwicklung erlebt, die wir heute mit dem Wort Digitalisierung beschreiben, die Digitalisierung des Lebens, der Wirtschaft auch dessen, was der Staat tut. Die klassischen Industrien werden digitalisiert mit allen Chancen, die damit verbunden sind. Start-ups entwickeln neue Ideen, die alte Geschäftsmodelle in Frage stellen, teilweise zerstören. Die Gesellschaft hat IT und Internetkommunikation in ihr Zusammenleben integriert. Wir zahlen mit Daten, nicht mehr nur mit Euros.

Wir haben uns durch die Diskussion über die Snowden-Folien und über die Möglichkeiten der amerikanischen Nachrichtendienste auch sehr intensiv damit beschäftigt, welche Kompromittierung dieser digitalisierten Wirtschaft, Verwaltung und Gesellschaft möglich ist.

Heute, 20 Jahre später, stellt sich nicht mehr so sehr die Frage, wie wir dieses oder jenes System schützen mit dieser oder jener Technologie. Heute fragen sich die Menschen, wie sie sicher im Netz leben und handeln können. Die Unternehmen fragen sich, wie sie ihr Know-how noch schützen können gegen Spionage. Wie sie ihre digitalisierte Produktion schützen können gegen Sabotageangriffe. Der Staat fragt sich, wie er die Bürgerinnen und Bürger, die elektronische Prozesse im eGovernment abwickeln wollen, ausreichend schützen kann. Insofern ist die Frage nach der IT-Sicherheit heute eine ganz andere als vor 20 Jahren. Und die Frage nach der IT-Sicherheit dominiert mittlerweile die sicherheitspolitischen Diskussionen in einem großen Umfang, weil Sicherheitsfragen und IT-Sicherheitsfragen zusammengewachsen sind. Dies bezeichnen wir mit dem Begriff der Cybersicherheit, unter dem wir das Thema seit einigen Jahren diskutieren. Wir stellen uns zum Beispiel die Frage nach der Sicherheit des PKW. Insbesondere wenn es um car-to-car-Kommunikation, die Kommunikation mit Notrufzentralen oder gar um autonomes Fahren geht.

Wir stellen uns die Frage nach der Funktionsfähigkeit von Medizintechnik bis hin zur Funktionsfähigkeit des Gesundheitswesens. Wir stellen uns die Frage nach der Sicherheit der Energieversorgung, so sie denn digitalisiert ist. Wir stellen uns die Frage nach der Cybersicherheit staatlicher Stellen, die elektronisch die Prozesse elektronisch bearbeiten, Bürgerdaten verarbeiten, Bescheide erstellen und Ähnliches.

Deshalb ist die Frage nach der IT-Sicherheit heute eine gesellschaftliche und politische Frage von größerer Tragweite als vor 20 Jahren. Und die heute hier als Gegenstand gewählte Frage „Wie können wir die deutsche IT-Sicherheitswirtschaft stärken“ ist für uns eine der Kernfragen auch unserer Cyber-Sicherheitspolitik und auch der digitalen Agenda. Die Bundesregierung hat sich mit der digitalen Agenda Ende August, wie es ein Minister so schön formuliert hat, ein Hausaufgabenheft für die Gesamtfragen der Digitalisierung gestellt. Wir haben gemeinsam mit dem Bundeswirtschaftsministerium und dem Ministerium für Verkehr und digitale Infrastruktur für die Bundesregierung insgesamt zusammengestellt, wie wir in dieser Wahlperiode die Digitalisierung begleiten, voranbringen, ein Stück weit auch lenken wollen. Die Entwicklung und der Einsatz vertrauenswürdiger Produkte und Dienstleistungen sind auch ein Gegenstand der digitalen Agenda und etwas, was wir in unserer Digitalisierungspolitik mit dem Wirtschaftsministerium gemeinsam engagiert vorantreiben.
Aus unserer Sicht hat der Staat drei Funktionen bei der Digitalisierung. Das ist zum einen eine Freiheits- und Ausgleichsfunktion. Die Nutzung des Netzes und der Zugriff auf das Internet dürfen möglichst nicht begrenzt werden, gerade angesichts der technischen Entwicklung und des sich abzeichnenden Mangels an Transportkapazität. Das Internet ist auch ein Raum der freien Persönlichkeitsentfaltung, wo wir Abwägungen zu treffen haben, Abwägungen zwischen widerstreitenden individuellen Grundrechten.

Zweitens: der Staat hat eine Schutz und Gewährleistungsfunktion. Wir tragen eine Mitverantwortung für die wichtigen gesellschaftlichen Infrastrukturen, und das Internet ist auch eine Infrastruktur, die für alle zugängig sein und zuverlässig funktionieren muss. Der Schutz des Internets ist eben auch eine Aufgabe, zu der wir uns berufen sehen und es gibt beispielsweise in der Europäischen Union eine Diskussion über ein entsprechendes Regulierungsvorhaben. Dies ist die Richtlinie über Netzwerk und Informationssicherheit, welche sehr intensiv diskutiert wird. Was im Internet müssen wir eigentlich alles schützen, damit die Funktionsfähigkeit unserer digitalisierten Gesellschaften erhalten bleibt?

Und drittens hat der Staat auch eine Angebots- und Innovationsfunktion. Es ist eine Aufgabe des Staates, ein innovationsfreundliches Klima zu schaffen und Entwicklungen zu fördern. Wir haben beispielsweise eine neue Hightech- Strategie unter Federführung des Forschungsministeriums verabschiedet. Wir sehen uns auch mit der Digitalisierung des Staates selbst, mit Fragen des innovativen Staates und des eGovernment aufgerufen, diese Innovationen voranzutreiben. Mit diesem Rollenverständnis wollen wir auch den Einsatz vertrauenswürdiger Informationstechnik in allen Bereichen fördern.

Vertrauenswürdige IT ist für alle Bereiche der Gesellschaft wichtig, für die Bürgerinnen und Bürger, die mit höchster Sicherheit im Netz agieren wollen und die ihre Persönlichkeitsrechte effektiv geschützt sehen wollen. Hierfür brauchen wir nicht beispielsweise mehr Verschlüsselung der Datenkommunikation. Wir brauchen eine Weiterentwicklung und einen Ausbau von kryptografischen Verfahren. Wir brauchen den Einsatz von Sicherheitstechnologien, die auf bewährten kryptografischen Verfahren basieren, wie wir sie mit der De-Mail oder der eID-Funktion des Personalausweises entwickelt haben. Wir brauchen auch eine Reform des Datenschutzrechtes, an der wir auf europäischer Ebene arbeiten, die internettauglich ist und auch Technik gestützten Datenschutz, Datenschutz durch Technik, datenschutzfreundliche Techniken fördert. Und wir brauchen natürlich auch eine Sensibilisierung der Anwenderinnen und Anwender für vertrauenswürdige Informationstechnik, für die Möglichkeiten und Grenzen.

Wir haben in Deutschland eine Diskussionslage, die bei diesem Thema sehr stark schwarzweiß geführt wird. Ist denn dieses System jetzt sicher, wenn ich die Firewall X oder das

Intrusion Detection System Y einsetze? Und wenn dann ein Experte eine sichere Technologie empfiehlt, kommt sofort ein anderer Experte und behauptet, dass das aber nicht 100% ig sicher ist.

Dieser für die Menschen kaum nachvollziehbare Diskurs der Experten über „wirkliche IT-Sicherheit“ ist ein Problem. Wir tun uns schwer, für vertrauenswürdige Informationstechnik in der Öffentlichkeit zu werben, wenn andere Sicherheitsexperten das nicht für 100%ig sicher halten. Wir brauchen daher ein Stück weit auch eine Veränderung der öffentlichen Kommunikation. Wir brauchen ein Klima, in dem wir zu sukzessiver Steigerung der IT-Sicherheit kommen und wo auch nach Möglichkeit die verschiedenen Experten, und da appelliere ich auch an alle, die hier im Raum sind, sich zurückzuhalten mit überzogener Kritik nach dem Motto, dass es nicht absolut sicher ist, sondern dann lieber sagen: ja, das ist ein Schritt – aber man kann natürlich auch noch mehr machen.

Mir wird zum Beispiel immer unterstellt, dass ich sage, dass die De-Mail perfekt und damit alle elektronische Kommunikation per De-Mail sicher ist. Das haben wir nie gesagt. Aber mit der De-Mail wird die Kommunikation zwischen dem Nutzern und dem Provider verschlüsselt. Das ist ein großer Sicherheitsfortschritt und wer noch mehr Sicherheit haben will und sagt, dass er eine Ende-zu-Ende-Verschlüsselung zwischen Nutzer und Nutzer darauf aufsetzt, der hat noch einmal weitere Sicherheitsfortschritte. Eine solche differenzierte öffentliche Kommunikation wäre hilfreich und könnte vertrauenswürdige IT gerade auch im Bereich der Bürgerinnen und Bürger stärker fördern.

Ein anderer Bereich, der die vertrauenswürdige Informationstechnik braucht, sind die kritischen Infrastrukturen. Mit dem IT-Sicherheitsgesetz wollen wir in Deutschland branchenweite Standards für die kritischen Infrastrukturen einführen. Wir beraten diesen Gesetzentwurf gerade innerhalb der Bundesregierung. Unser Ziel – der Entwurf ist veröffentlicht – ist es, in den Bereichen kritischer Infrastruktur Energie, Telekommunikation, Transport, Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Sicherheitsniveaus zu definieren.

Wir haben hier einen Ansatz gewählt, den ich als kooperativen Ansatz bezeichnen würde, bei dem keine Sicherheitsstandards vorgegeben werden sondern die einzelnen Wirtschaftszweige aufgerufen sind, selbst branchenspezifische IT-Sicherheitsstandards zu entwickeln. Das greift auch auf, dass es das in manchen Branchen schon gibt. Das was z.B. bei den Banken mit den MA – Risk bereits funktioniert, wollen wir gern aufgreifen.

Wir werden aber natürlich das Bundesamt für Sicherheit in der Informationstechnik beauftragen, diese branchenspezifischen Standards zu prüfen und festzustellen, ob die gesetzlichen Anforderungen erfüllt sind. An dieser Stelle werden wir natürlich auch auf den Einsatz vertrauenswürdiger Informationstechnik achten. Wenn es beispielsweise um die Steuerung kritischer Anlagen geht, wird man eine vernünftige Identifizierung des Bedieners verlangen. Wenn es um die Kommunikation zwischen kritischen Prozessen in einer kritischen Infrastruktur geht, wird diese Kommunikation vernünftig abgesichert sein müssen - hinsichtlich Vertraulichkeit und Verfügbarkeit der Kommunikation. Über die kritischen Infrastrukturen hinaus, wird die Wirtschaft auch im Übrigen einen hohen Bedarf an vertrauenswürdiger Informationstechnik haben. Das gilt hauptsächlich für die Bereiche, in denen jetzt eine Digitalisierung des Kerngeschäfts stattfindet. Ein Schlagwort ist hier natürlich Industrie 4.0, die Digitalisierung der industriellen Fertigung, die den Unternehmen ganz neue Chancen bietet, aber auch ganz neue Risiken für die Verlässlichkeit der Produktion und die Steuerbarkeit der Produktion aufwirft.

Vorliegende Untersuchungen ergeben, dass wir - gerade im Mittelstand - zwar eine gewisse Sensibilität für IT-Sicherheit haben, das Knowhow aber noch entscheidend verbessert werden muss. Die Kenntnis über vertrauenswürdige Informationstechnik muss verbreitert werden, Anbieter und Nutzer in den Anwendungsbranchen stärker zusammengebracht.
Die Vernetzung in allen Bereichen der Industrie von dem Transport, Logistik, mobilen Anlagen, Energieversorgung usw. wird allein wegen der Produktivitätssteigerung, die damit verbunden sind, stark weiter voranschreiten. IT-Sicherheitsmechanismen werden nachgefragt werden, müssen dann aber auch zur Verfügung stehen.

Für die nationale und europäische IT-Sicherheitswirtschaft, also auch für die Kolleginnen und Kollegen, die hier im Raum sind, bedeutet das natürlich, dass sie sich hierzu positionieren müssen, Lösungen präsentieren müssen, die im Markt verständlich sind, die nutzbar sind. Mit unseren Überlegungen zur Weiterentwicklung vertrauenswürdiger Informationstechnik wollen wir Rahmenbedingungen verbessern, dass vertrauenswürdige IT in den relevanten Bereichen eingesetzt wird. Für uns gehören die IT Sicherheitskompetenzen und die IT-Sicherheitsunternehmen zu den Schlüsseltechnologien, zu den Kernkompetenzen und der Kernbranche Deutschlands in der Digitalisierung. Wir haben hierbei eine Notwendigkeit und eine Chance. Die deutsche IT-Sicherheitstechnik hat einen guten Ruf in der Welt. Gemeinsam müssen daran arbeiten, dass wir bei der IT-Sicherheit den Global Playern nicht das Feld überlassen, sondern die hier entwickelten Produkte stärker in den Einsatz kommen, dass die großen Anwendungsunternehmen, die in der Digitalisierung ihre Produktionsanlagen umstellen die Produkte auch einsetzen. Wir können dieses Ziel der breiteren Anwendung der IT-Sicherheitswirtschaft nur erreichen, wenn alle Beteiligten hier zusammenwirken.

Meine Damen und Herren, wir haben in den letzten Jahren vielfältige Initiativen unternommen, die IT-Sicherheitswirtschaft zu fördern. Beispielsweise haben wir im Bereich des BSI die Zertifizierung ausgebaut. Wir haben in der öffentlichen Verwaltung versucht, IT-Sicherheitsprodukte einzusetzen, haben dort auch zusätzliche Mittel in großem Umfang eingesetzt. Ich erinnere nur an das IT-Investitionsprogramm, in dem wir 240 Millionen allein für IT Sicherheitsprodukte zwischen 2009 und 2012 eingesetzt haben. Aber es ist noch nicht gelungen, eine kritische Masse zu erreichen. Und es ist noch nicht gelungen, die IT-Sicherheitsprodukte, die Sie anbieten, auch im Bereich der Anwendungswirtschaft zu Standardprodukten zu machen.

Deshalb freue ich mich, dass heute z.B. auch durch Beiträge von Voice und anderen die Anwendungswirtschaft vertreten ist und wir heute vielleicht die Diskussion darüber führen können, wie wir diese längerfristige Zusammenarbeit ausgestalten können. Wir würden als Bundesinnenministerium, und ich glaube, ich kann das auch für die Kollegen aus dem Bundeswirtschaftsministerium sagen, hierbei gern mitwirken. Aber wir sehen die Unternehmen in der Pflicht – auch angesichts der Innovationsgeschwindigkeit bei den Produkten – diesen Prozess zunächst einmal selbst zu treiben. Wir sind bereit, daran mitzuwirken. Dazu gehört selbstverständlich auch, dass wir uns als IT-Verantwortliche der öffentlichen Verwaltung in großem Umfang gerade im letzten Jahr darum bemühen, vertrauenswürdige IT Produkte stärker in den Einsatz zu bringen. Wir haben intensive Diskussionen und auch Entscheidungen im IT-Rat des Bundes und auch im IT-Planungsrat des Bundes und der Länder getroffen, Entscheidungen über Standardisierung, Entscheidung beispielsweise über Beschaffungspolitik und Beschaffungsverfahren. Ich will nur die No-Spy-Klausel als ein Beispiel erwähnen. Damit unterstützen wir vertrauenswürdige IT. Nun muss es gelingen, die Zusammenarbeit von IT-Sicherheits-, IT- und Anwenderwirtschaft auf Dauer zu organisieren. Das Bundesinnenministerium wird sich daran beteiligen.
Für uns ist das ein Schwerpunktthema, ein Kernthema unserer Cybersicherheitspolitik. Das drückt sich auch darin aus, dass wir im Sommer diesen Jahres im Rahmen der Neuorganisation

unseres Hauses nicht nur den Bereich Cybersicherheit insgesamt gestärkt haben, sondern dass wir für diese Fragestellung auch ein Referat eingerichtet haben, das sich um sichere Informationstechnik kümmert. Es wird geleitet von Herrn Reisen, der heute auch vor Ort ist. Insofern sind wir für Sie als Ansprech- und Gesprächspartner verfügbar und würden gern mit Ihnen gemeinsam daran wirken, dass wir vertrauenswürdige Informationstechnik als solche identifizieren, beschreiben, gemeinsam fortentwickeln und dann auch in den Einsatz in den relevanten Einsatzbereichen bringen.

4 Die Herausforderungen für deutsche IT-Unternehmen im internationalen Wettbewerb/ Die exportpolitische Flankierung durch das BMWi

Dr. Dirk Grabowski, Bundesministerium für Wirtschaft und Energie, Berlin

Einen schönen guten Abend, meine Damen und Herren, speziell Ihnen, Prof. Thielmann, dem ich die Einladung hier zu verdanken habe. Ich möchte zu Beginn meiner Ausführungen zwei Stichworte aufgreifen, die Herr Schallbruch gerade erwähnt hat, nämlich Zusammenarbeit, das wird ein Kernpunkt dessen sein, was ich hier vortrage, und neue Wege beschreiten. Ich muss zur Einführung, bevor ich hier darlege, was wir speziell im Wirtschaftsministerium machen, kurz erzählen, was wir nicht machen, denn das ist sehr wichtig für das Verständnis meiner Darlegungen. Ich bin anders als Herr Schallbruch, der als IT Direktor hier die Konzeptionen des BMI vortragen konnte, kein Experte für den IT-Bereich. Wie Sie alle wissen, liegt die Zuständigkeit für das Thema IT im BMWi in der Abt. VI „Innovations-, IT- und Kommunikationspolitik“. Herr Dauke, Leiter dieser Abteilung, der hier heute anwesend ist, kann Ihnen sicher dazu Einiges erzählen.

Ich stehe aus ganz anderen Gründen hier. Wir haben im Rahmen unserer seit dem Jahr 2012 bestehenden Exportinitiative „Zivile Sicherheitstechnologien“ ein neues Geschäftsfeld eröffnet: Die spezielle Unterstützung von Exportaktivitäten im IT-Bereich.

Was wir eigentlich versuchen, ist in gewisser Hinsicht ein Experiment, denn wir wollen das Thema IT-Sicherheit integrieren in unsere normale Initiative. Damit dieses Experiment in der Tat gelingt, auch gerade um die IT-Sicherheit hier in Deutschland zu stärken, brauchen wir das Zusammenspiel mehrerer Institutionen. Es ist daher meine Intention, Sie mit meinem Vortrag davon zu überzeugen, bei unserem Experiment mitzuspielen.

Wir haben im Bundeswirtschaftsministerium insgesamt vier spezifische Exportinitiativen für Erneuerbare Energien, für Energieeffizienz, für die Gesundheitswirtschaft und seit dem Jahre 2012 für die zivile Sicherheit. Wir organisieren im Rahmen dieser Exportinitiative Delegationsreisen in ausgewählte Länder. Beispiele sind: Brasilien, Chile, China, Indien Russland, Vietnam, Marokko, Türkei und die arabische Halbinsel.

Die Länderauswahl erfolgt in enger Abstimmung mit zahlreichen Partnern.
Dazu gehören Verbände wie BITKOM und Teletrust. Aber auch mehrere Ministerien sind vertreten, darunter das BMI und das AA. Hinzukommen weitere spezielle Institutionen wie die GTAI, das BAFA und der AUMA. Wir treffen uns gemeinsam einmal pro Jahr, um eine Länder- und Themenauswahl für das nächste Jahr festzulegen.

So haben wir im Laufe dieses Jahr beschlossen, diesen Kreis der Reisen, die wir organisieren, um den Bereich IT-Sicherheit zu erweitern. Wir haben am 18. November – und vielleicht kann der eine oder andere von Ihnen dabei sein -, eine Art Auftaktveranstaltung hier in Berlin. Dort wollen wir eruieren, ob bei einer Region wie Lateinamerika ausreichend Interesse besteht, um in 2015 eine Geschäftsanbahnungsreise durchzuführen.

Wir haben daneben vor knapp 14 Tagen beschlossen, dass wir auf jeden Fall versuchen werden, ein Land wie Singapur stellvertretend für diese Wachstumsregion Südostasien im nächsten Jahr zu bereisen. Und wir haben auch vor, ohne dass es im Augenblick exakt konkretisiert ist, uns des Themas Arabische Halbinsel speziell unter dem Stichwort IT-Sicherheit anzunehmen. Das sind die ersten Planungen für 2015.

Ergänzend möchte ich auf sogenannte politische Reisen hinweisen, bei denen wir in der Regel auf der Ebene Parlamentarischer Staatssekretärinnen und Staatssekretäre mit größeren Industriedelegationen und ausgewählten Themen in bestimmte Länder gehen. Allein für das erste Halbjahr 2015 haben wir sechs solcher Reisen vorgesehen. Es handelt sich dabei um Dubai, Indien, Brasilien, die USA, China und Australien. Sie können allein an dieser Zahl dass das Thema zivile Sicherheit in unserem Hause eine sehr hohe Bedeutung hat.

Herr Thielmann hat vorhin eine Veranstaltung am 05. September 2014 erwähnt, die Minister Gabriel durchgeführt hat. Da lag zwar der Schwerpunkt mehr auf der Verteidigungswirtschaft, aber ein zentraler Punkt dort war das Thema Diversifizierung. Also das Bestreben, Unternehmen aus dem wehrtechnischen Bereich verstärkt Möglichkeiten eines Engagements in der zivilen Sicherheit und damit, wo immer das möglich ist, auch in den Bereich IT-Sicherheit zu ermöglichen. Wir werden im nächsten Jahr dazu ein spezielles Innovationsprogramm auflegen.

Ich hatte am Anfang von Experiment und Unterstützung gesprochen. Wir können in der Tat das, was wir in Ihrem Interesse vorhaben, wirklich nur sinnvoll realisieren, wenn Sie mitarbeiten, denn ohne Ihren Sachverstand von der Unternehmensseite und aus der Wissenschaft heraus können wir diese Aktivitäten nicht durchführen, denn wenn sich niemand meldet, wenn wir die falschen Themen wählen, wenn wir die falschen Länder aussuchen, die falschen Ansprechpartner haben, dann ist das Ganze sehr schnell gescheitert und dann werden wir das logischerweise ganz schnell wieder einstellen. Das sind letztlich Ihre Steuergelder, die wir dort auch ausgeben.

Wie gesagt, meine dringende Bitte in Ihrem und auch unserem Interesse ist, engagieren Sie sich und vielleicht schaffen wir tatsächlich wirklich etwas gemeinsam auf die Beine zu stellen, um Ihre Perspektiven verbessern und dann letztlich das erreichen, was hier unter der Überschrift steht, nämlich die IT-Sicherheit in Deutschland zu stärken.

5 Handlungsempfehlungen

Christian Köhler, IABG mbH, Berlin

Ich stehe unter anderem hier, weil – wie es Prof. Thielmann bereits gesagt hat - im Jahr 2012 die Studie für die zivile Sicherheitswirtschaft gestartet ist, die wir im Herbst letzten Jahres abgeschlossen haben.

Vielleicht ist es bei den Vorrednern schon herausgekommen, dass das Problem bei den Analysen der Sicherheitswirtschaft die saubere Angrenzung ist, Sicherheitswirtschaft ist das eine, das andere ist IT-Sicherheitswirtschaft. Das haben wir in unseren Arbeiten auch gesehen. Ich habe nicht ganz so weit zurückgegriffen wie Herr Schallbruch. Aber zumindest habe ich in der Vorstellung fünf Jahre zurückgegriffen, denn das war zumindest der erste Punkt, wo wir uns mit dem Thema befasst haben, nämlich mit der ersten Marktstudie zum Potenzial der deutschen Sicherheitswirtschaft.

Bild 1

Die erste Studie zum Marktpotenzial – der eine oder andere hat sie gelesen - war vom VDI 2009 (Bild 1). Auch dort war das Thema IT-Sicherheit nicht als Kernthema enthalten sondern explizit als Querschnittsthema und somit nur ein Teil der ganzen konzeptionellen Untersuchung der Sicherheitswirtschaft. Daraus ableitend hat das BMWi 2010 eine industriepolitische Mitteilung zur zivilen Sicherheitswirtschaft abgeleitet, aus der dann weitere Arbeiten hervorgegangen sind, u.a. die Gründung der Koordinierungsstelle Sicherheitswirtschaft im DIN, die letztendlich dort auch koordinierende Tätigkeiten wahrnehmen soll, nicht nur im Kernaufgabenbereich des DIN (Standardisierung und Normung) sondern eben weit darüber hinausgehend ein Stückweit auch Themen aufgreifen soll, die aus Brüssel kommen und dort auch wieder zurückspielen. Auch bei der KoSi kommt das Abgrenzungsproblem schon zum Tragen, denn die Koordinierungsstelle Sicherheitswirtschaft ist nicht für das Thema IT-Sicherheit

zuständig. Ganz im Gegenteil gibt es mit der Koordinierungsstelle IT-Sicherheit (KITS) auch eine parallele Struktur beim DIN.

Herr Dr. Grabowski hat es bereits gesagt, die Exportinitiative Sicherheitswirtschaft ist im Jahr 2012 gestartet. Vorgelagert war auch hier die Untersuchung, wie wir mit der Exportinitiative an den Start gehen. Die Koordinierung der Exportinitiative findet in einem Steuerungskreis statt, wo die relevanten Verbände und ihre Vertreter sich letztendlich rechtzeitig vorher überlegen, welche Länder lohnenswert sind und wie wir das einplanen können.
Wir haben dann im Jahr 2012 mit dem Masterplan Sicherheitswirtschaft begonnen. Der ist im Herbst 2013 vorgestellt worden und inzwischen kommt das Thema IT-Sicherheitswirtschaft doch zum Tragen, indem wir ab 2014 mit Folgeaktivitäten gestartet haben, die das Thema IT-Sicherheitswirtschaft dann doch etwas enger in den Fokus genommen haben.

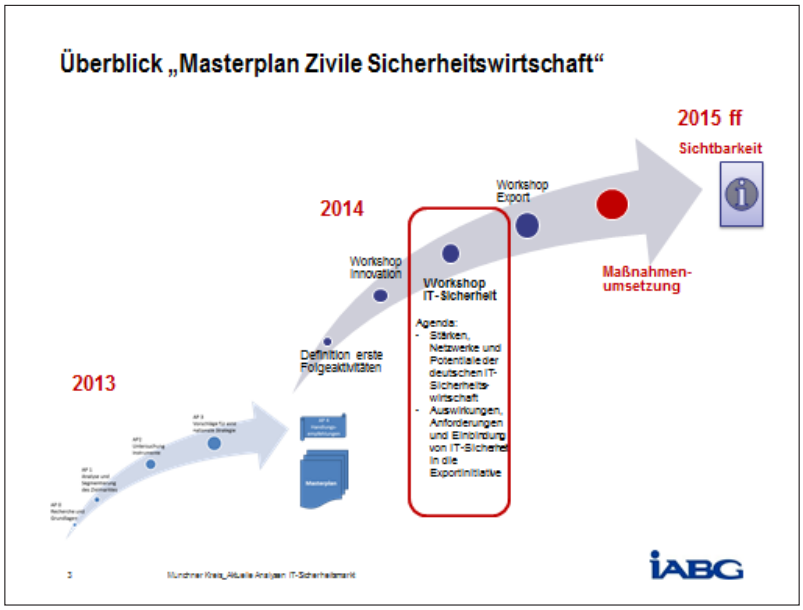


Bild 2

Der eine oder andere wird dies wissen, weil er an den Workshops dabei war. Wir haben drei Workshops in der Folge des Gutachtens zum Masterplan (Bild 2) in diesem Jahr durchgeführt, die sich mit den Fragen befasst, wie die deutsche Sicherheitswirtschaft in Brüssel erfolgreicher arbeiten kann, wie wir das Thema Innovationsfinanzierung besser in den Griff bekommen werden und wie wir das Thema IT-Sicherheitswirtschaft noch enger in die Exportinitiative Sicherheitswirtschaft einbauen können? Dazu gehören Fragen wie: welche Stärken sind vorhaben? Welche Netzwerke sind überhaupt in diesem Bereich unterwegs? Auch dort merkt man eine sehr starke regionale Struktur der Sicherheitsnetzwerke. Welche Einbindung und Anforderung gibt es überhaupt für die IT-Sicherheitswirtschaft? Das ist heute auch schon einmal angedeutet worden. Einerseits vielleicht eine engere Anbindung an die Anwenderbranchen, andererseits eine Einbindung der IT-Sicherheitswirtschaft im engeren Sinne, im eigenen Sinne. Gleichzeitig stellt sich natürlich die Frage: Wie stark kann man in einer kleinteilig organisierten IT-Wirtschaft im Export überhaupt sein? Die Aufgabe heute ist ja nicht, den ganzen Masterplan vorzustellen. Ich versuche das nur noch einmal einzusortieren. Der Masterplan Sicherheitswirtschaft des BMWi ist zum Download verfügbar.

Bild 3

Wir haben am Ende eine Vielzahl von Handlungsempfehlungen vorgestellt und detailliert ausgearbeitet, die sich in vier Säulen gliedern (Bild 3). Einerseits zum Thema Analysefähigkeit, zweitens das Thema nationaler Markt, drittens, Sie sehen es hier grün, das Thema Export und viertens, wie wir die ganzen Empfehlungen koordinieren. Ich habe versucht darzustellen, dass wir mit den drei Workshops, von denen nur einer über IT-Sicherheit war, anteilig einige Maßnahmen angefasst haben, d.h. das gesamte Bild noch nicht ansatzweise ganzheitlich bearbeitet wird. Es steht noch zur weiteren Bearbeitung zur Verfügung.

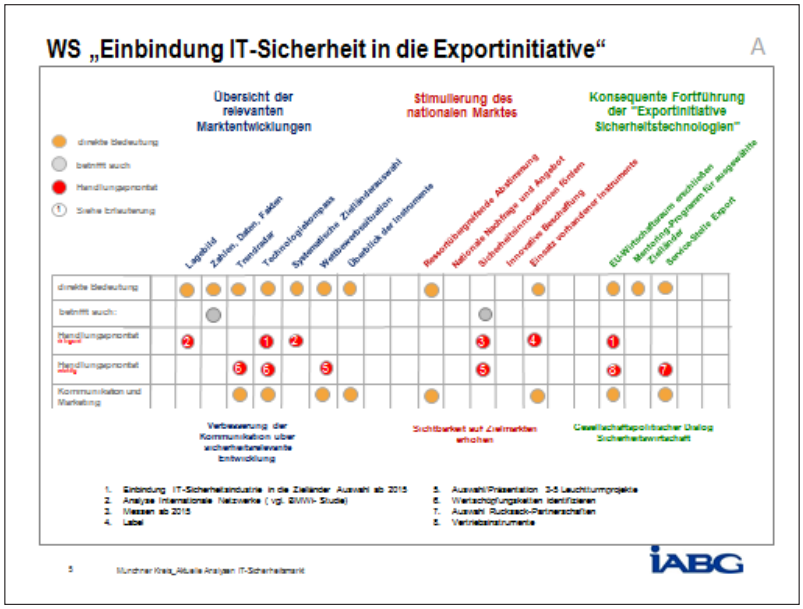


Bild 4

In dem Workshop IT-Sicherheit, den wir im Mai durchgeführt haben, haben wir einerseits mit den Beteiligten – es waren ungefähr 30 Unternehmen und Verbände dabei, auch Verwaltungen natürlich - versucht, die Schwerpunkte herauszuarbeiten, die einerseits zu den vier Säulen des Masterplans einsortiert werden sollten und diese in die Prioritätenliste zu geben (Bild 4). Dabei ist sicher zu beachten, dass ein Workshop a) nicht die Welt verändern kann und dies b) auch nicht in dem anschließenden Bericht möglich ist. Aber vielleicht kann man die eine oder andere Weichenstellung vorantreiben. Das Schöne, was man vielleicht sehen kann, ist, wenn man unmittelbare Ergebnisse umgesetzt sieht. Wir haben uns in dem Workshop mit der Frage befasst, wie man die IT-Sicherheitsindustrie in die Zielländer auch nach 2015 einbinden kann. Herr Dr. Grabowski hat es bereits gesagt, dass diese Aktivität schon gestartet und eigentlich schon in der Umsetzung ist. Somit ist dies eine ganz operative Maßnahme, die greift. Die Analyse der Netzwerke ist auch interessant, wenn wir über den Export der IT-Sicherheitsindustrie reden.

Dann stellt sich natürlich die Frage, ob nationale Netzwerke ausreichend sind oder ob vielleicht auch ein Vertriebskanal internationale Netzwerke ist. Im Moment entsteht im Referat von Herrn Dauke, also bei Frau Husch, eine Untersuchung, die sich mit dem Thema „was machen andere Initiativen in anderen Ländern, wie machen sie es und wie machen sie es vielleicht besser?“, befasst. Insofern ist das auch ein Ergebnis, welches hoffentlich in absehbarer Zeit zur Verfügung steht. Die Messen und Veranstaltungsplanung betrifft das Thema IT-Sicherheit genauso.

Wir haben uns auch mit der Frage eines Labels befasst, denn einige im Raum haben anfangs bei „IT-Security made in Germany (ITSMIG)“ mitgemacht, einer Initiative, die Hochs und Tiefs hatte. Ich will hier darüber nicht philosophieren sondern einfach nur festhalten , dass wir uns mit dieser Frage des Labels natürlich befasst haben und ich denke, dass man diese Frage zwingend aufgreifen muss, mit welchem Mantel, mit welchem Label – der eine mag den Begriff , der andere nicht – wir nach draußen gehen und welche Möglichkeiten es gibt.
Viele von uns haben z.B. auch die Markterkundungsstelle in der Golfregion schon einmal erlebt. Damit gibt es sicherlich auch gute und schlechte Erfahrungen. Aber es ist eben ein Teil des Instrumentenkoffers, den man zu betrachten hat, wenn man ins Ausland gehen will.
Die Auswahl von Leuchtturmprojekten finde ich ebenfalls wichtig. Ich glaube, es ist entscheidend, dass man nicht immer mit der ganzen Bandbreite unterwegs sein muss, sondern dass man vielleicht ganz besondere Sachen hervorheben muss. Herr Schallbruch hat die eine oder andere Fähigkeit schon einmal angesprochen, die auch im Ausland zu deutschen Stärken zählen oder die zumindest zu Aufmerksamkeiten geführt haben. Insofern ist hierbei wichtig, mit deutschen Stärken zu glänzen.

Die Frage der Einbindung der Anwendungsbranchen für integrierte IT-Sicherheitslösungen ist für uns eine viel diskutierte. Wir haben im Prinzip hervorgehoben, dass es das Thema Wertschöpfungsketten einschließt und vielleicht auch die Auswahl von Rucksackpartnerschaften, wie wir es hier genannt haben. Es gibt besonders IT-affine Branchen, die im Export besondere Stärken haben und wo wir eine KMU-getriebene Sicherheitswirtschaft einfach mit einem entweder großen Systemlieferanten oder einem großen Partner im Anwendungsbereich noch m Ausland stärken können.

Das letztgenannte Gebiet darf man nicht verhehlen, es geht um Vertriebsinstrumente. Ich bin der Meinung, dass man einer IT-Sicherheitsindustrie mit einfachen Vertriebsinstrumenten im Ausland, sprich: Förderung oder Ähnlichem, helfen könnte. Dabei ist sicher zu berücksichtigen, wie die Instrumente wettbewerbsorientiert zu werten sind. Dem einen oder anderen

IT-Sicherheitsanbieter würde es einfach helfen, wenn er eine Vertriebsunterstützung im Ausland unmittelbar über eine Förderung bekäme, denn an der Qualität unserer Produkten und Lösungen liegt es nicht.

Bild 5

Die Empfehlungen, die wir im Rahmen dieser drei Workshops ausgearbeitet haben, haben wir dann noch einmal kategorisiert in Marktvorbereitung, Markterschließung, –bearbeitung und Unterstützung (Bild 5). Dies ist nur noch einmal eine thematische Darstellung und lässt vielleicht eine bessere Eingruppierung zu. Womit könnte man anfangen? Was ist noch zu tun? Und was ist vielleicht auch im weiteren Schritt zu identifizieren?

Im Kern liegen eigentlich zwei aktuelle Studien den Überlegungen zugrunde. Wir haben im Rahmen unserer Aktivitäten des Masterplans die Möglichkeit gehabt, auf diese WISIND-Studie unmittelbar zuzugreifen, die in die Berichterstellung eingeflossen ist.

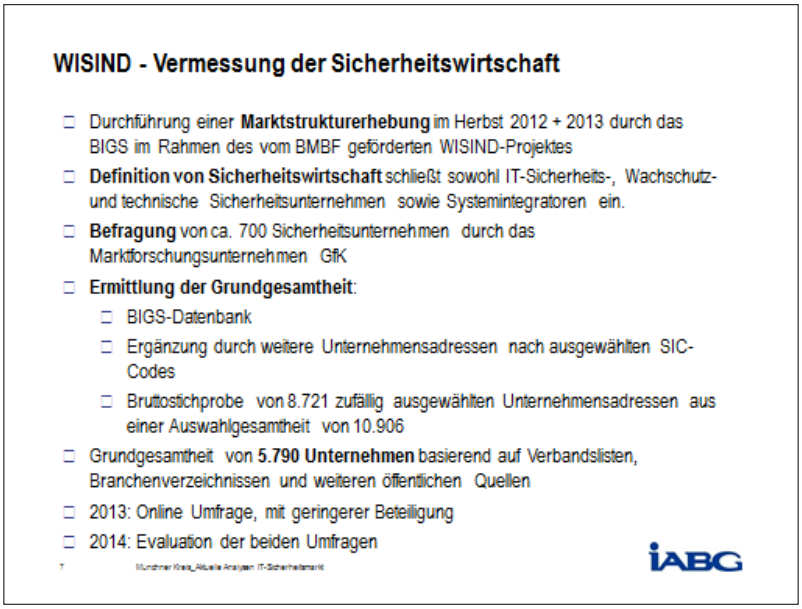
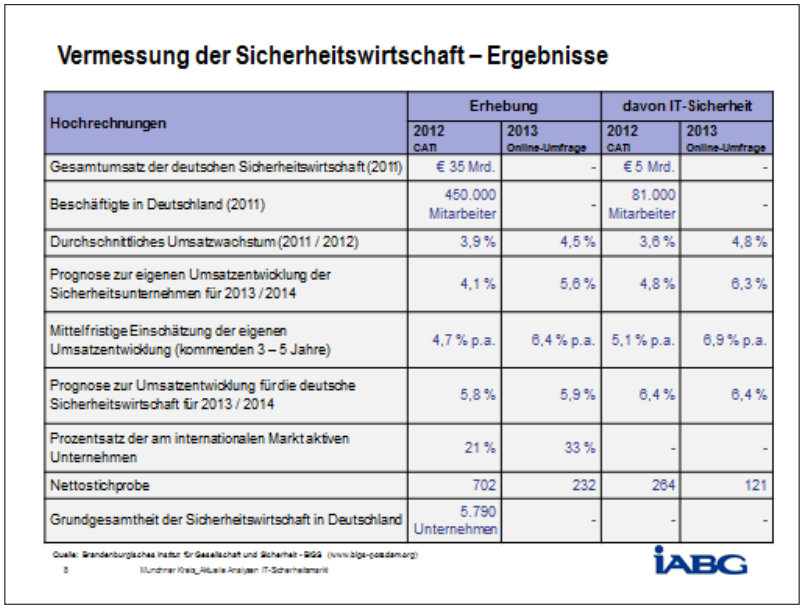


Bild 6

WISIND ist ein noch laufendes Projekt des Bundesministeriums für Bildung und Forschung, welches sich mit der Vermessung der Sicherheitsindustrie in Deutschland befasst (Bild 6). Zwei Umfragezyklen sind in diesem Bereich bereits gelaufen, durchgeführt durch das BIGS, Brandenburger Institut für Gesellschaft und Sicherheit, die Auftragnehmer mit uns gemeinsam an der Studie zum Masterplan waren. Die erste Befragung hat schon eine gewisse Besonderheit, weil man eine Direktbefragung mit der GFK, Gesellschaft für Konsumgüterforschung, durchgeführt hat und auf einer Grundgesamtheit von 5.800 Unternehmen eine Befragung gestartet hat, die somit eine Primärdatenerhebung war. In vergleichbarem Umfang gab es in den letzten Jahren keine Analysedaten.

Die weitere Befragung ist im Jahr 2013 erfolgt. Hierbei gab es eine Reduzierung des Befragungsumfangs, der Nettostichprobe, indem man diese online vorgenommen hat. Wenn ich richtig informiert bin, soll es auch 2014 noch einmal eine Umfrage geben. Insofern blüht dem einen oder anderen hier demnächst noch eine Befragung.



Vermessung der Sicherheitswirtschaft – Ergebnisse

Hochrechnungen	Erhebung		davon IT-Sicherheit	
	2012 CATI	2013 Online-Umfrage	2012 CATI	2013 Online-Umfrage
Gesamtumsatz der deutschen Sicherheitswirtschaft (2011)	€ 35 Mrd.	-	€ 5 Mrd.	-
Beschäftigte in Deutschland (2011)	450.000 Mitarbeiter	-	81.000 Mitarbeiter	-
Durchschnittliches Umsatzwachstum (2011 / 2012)	3,9 %	4,5 %	3,6 %	4,8 %
Prognose zur eigenen Umsatzentwicklung der Sicherheitsunternehmen für 2013 / 2014	4,1 %	5,6 %	4,8 %	6,3 %
Mittelfristige Einschätzung der eigenen Umsatzentwicklung (kommenden 3 – 5 Jahre)	4,7 % p.a.	6,4 % p.a.	5,1 % p.a.	6,9 % p.a.
Prognose zur Umsatzentwicklung für die deutsche Sicherheitswirtschaft für 2013 / 2014	5,8 %	5,9 %	6,4 %	6,4 %
Prozentsatz der am internationalen Markt aktiven Unternehmen	21 %	33 %	-	-
Nettostichprobe	702	232	284	121
Grundgesamtheit der Sicherheitswirtschaft in Deutschland	5.790 Unternehmen	-	-	-

Quelle: Brandenburgisches Institut für Gesellschaft und Sicherheit - BIGS (www.bigs-potsdam.org)

5 Münchner Kreis_Aktuelle Analysen IT-Sicherheitsmarkt

IABG

Bild 7

Bild 7 stellt dar, was ich aus den Analysen und Zahlen herausgezogen habe. Auch hier bitte ich zu beachten, dass es die Analyse die deutsche Sicherheitswirtschaft im Gesamtpaket erfasst. Man sieht hier ein Markt Volumen im Jahr 2012 von ungefähr 35 Mrd. € und davon IT-Sicherheit von ungefähr 5 Mrd. Das zieht sich jetzt bis unten durch, 81.000 Mitarbeitern im IT-Sicherheitsbereich.

Sowohl in der einen Befragung als auch in der Bewertung kommt zumindest aus diesen Studien heraus, dass das Wachstum der IT-Sicherheitswirtschaft prognostiziert zum Wachstum der sonstigen Wirtschaft deutlich stärker zunehmen sollte, wenn die Zahlen stimmen, als die Maßzahl in der Gesamtwirtschaft.

Die Nettostichprobe sieht man unten noch einmal. Wie gesagt wurden im Jahr 2012 5.790 Unternehmen befragt, von denen 702 geantwortet haben und im Jahre 2013 wurde es geringer. Die Zahlen können Sie alle nachlesen. Im Kopf behalten sollte man tatsächlich das Verhältnis der IT-Sicherheitswirtschaft. Wir reden also, wenn ich das so sagen darf, nicht über die Welt. Wir reden über ungefähr 80.000 Erwerbstätige mit ungefähr 5 Mrd. € Umsatz.
Die Zahl, die Sie hier sehen, ist aus dem Monitoring des BMWi gezogen, eine Darstellung der Gesamtbranche der IT-Wirtschaft in Deutschland mit ungefähr 228 Mrd. € Umsatz und ungefähr 900.000 Arbeitsplätzen, nur noch einmal im Verhältnis: gesamte IT-Wirtschaft in Deutschland, auch nicht von uns, sondern von TNS.

Wenn man jetzt die Studie von Wifor dagegenhält – Wifor ist ein Forschungsinstitut, das auch für das BMWi Studien in dem Bereich der IT-Sicherheitswirtschaft erstellt hat -, ist man hier anders vorgegangen als bei der WISIND-Studie. Die WISIND-Studie hat auf einer Primärdatenerhebung mit einer Befragung aufgesetzt, die Wifor-Studie hat sich an die deutsche Statistik gemacht und aus den vorhandenen Wirtschaftskennzahlen mit einer Verschneidung von Daten versucht, das herauszuholen, was IT-Sicherheitswirtschaft auch im engeren Sinne ist.

Der Vergleich der beiden Studien relativ interessant, weil es unterschiedliche Vorgehensweisen sind und eigentlich nur die beiden möglichen Methoden aufgreifen: nämlich Primärdaten erheben oder aus der deutschen Statistik Daten herauszufiltern und diese in ein eigenen Konto aufzuführen.

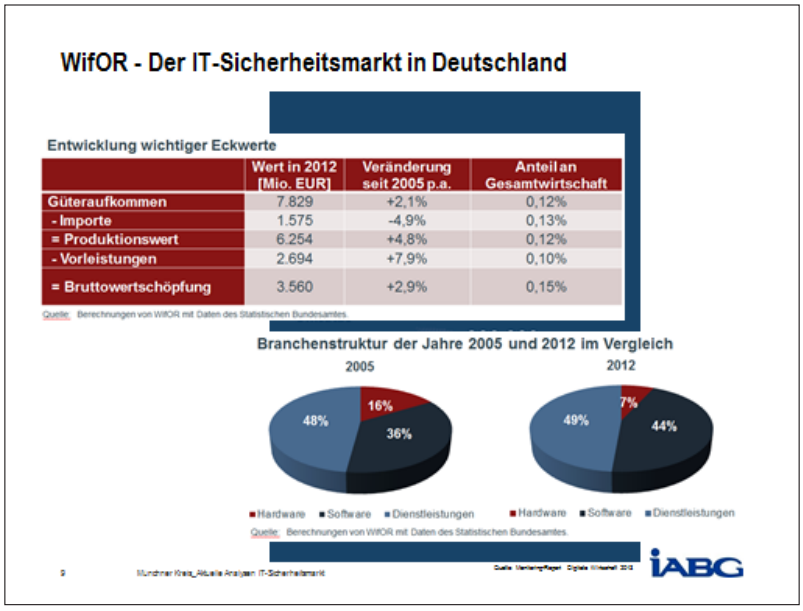


Bild 8

Man sieht hier (Bild 8 und 9) ungefähr einen Produktionswert der IT-Sicherheitswirtschaft von 6,2 Mrd. € in Deutschland zzgl. Importe von 1,575 Mio. €. 7,8 Mrd. € ist das gesamte Güteraufkommen, welches in Deutschland der IT-Sicherheit zuzurechnen ist, d.h. man bewegt sich in einem Anteil an der Gesamtwirtschaft von 0,15 %. Positiv gesagt heißt das: es ist da noch viel Luft nach oben.

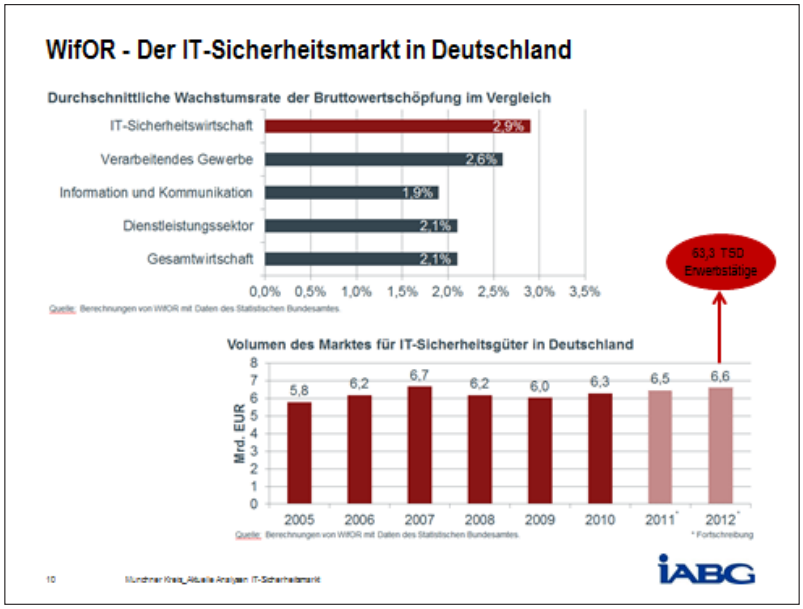


Bild 9

Interessant ist für uns auch in der Auswertung, wie stark z.B. der Export ins Rennen gehen kann und wie die Verteilung über Hardware, Software und Dienstleistungen ist. Der Hardwareanteil liegt bei ungefähr 50%, d.h. der Rest, Software und Dienstleistungen, verteilen sich mit 16 und 36%. Auch darauf ist zu achten, wenn man analysiert, dass man den Export steigern will. Es gibt dabei unterschiedliche Anforderungen, wenn Dienstleistungen im Vordergrund stehen, bzw. Hardware oder Software. Der Softwareanteil sehr gering dabei. Im Kopf haben wir noch die Wachstumszahlen, die das BIGS ermittelt hat

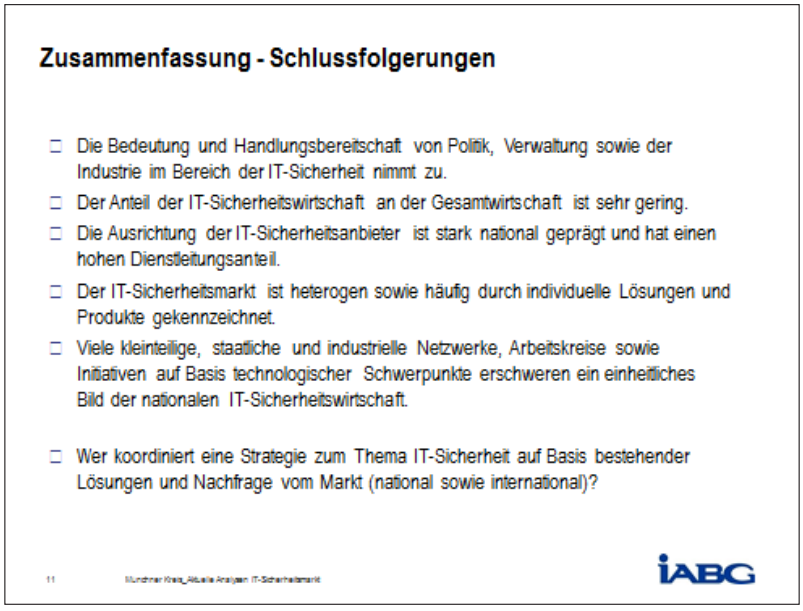


Bild 10

Meine Zusammenfassung (Bild 10) greift die Fragen auf, die Herr Mörl und ich uns für die spätere Diskussionsrunde vorgenommen haben. Die Bedeutung der Bereiche Politik, Verwaltung sowie in der Industrie im Bereich IT-Sicherheit nimmt zu. Herr Schallbruch hat das Thema über einen Zeitraum von 20 Jahren dargestellt. Ich bin der Überzeugung, dass die Entwicklung aus der Vergangenheit zeigen, dass das Thema IT-Sicherheit an Bedeutung zugenommen hat. Der Anteil der deutschen IT-Sicherheitswirtschaft an der Gesamtwirtschaft ist gering. Die Zahlen haben wir dargestellt. Diese sprechen für sich. Die Ausrichtung der deutschen Sicherheitswirtschaft ist stark durch den nationalen Markt geprägt. Wie gesagt, das Verhältnis ist ungefähr 6 ½ Mrd. € nationaler Markt und 1,2 Mrd. € Exporte. Auch die Zahlen sind selbsterklärend.

Der deutsche Sicherheitsmarkt ist heterogen sowie häufig durch individuelle Lösungen und Produkte gekennzeichnet. Dabei bleibt die Frage, wie können wir im Export besser werden, wenn wir sehr individuell auf Anfragen, auf Anforderungen nationale Lösung zugeschnitten haben. Daraus ergibt sich auch die Kernfrage: wie kann man mit individuellen Produkten, die einen kleinen Nachfragemarkt eigentlich nur abdecken, international besser werden?
Die vielen kleinteiligen staatlichen und industriellen Netzwerke, Arbeitskreise und Initiativen auf Basis technologischer Schwerpunkte erschweren nicht nur ein einheitliches Bild sondern auch eine einheitliche Strategie. Jeder darf sich selber organisieren. In der Studie zum Masterplan haben wir relevante Arbeitskreise im Bereich Sicherheitswirtschaft sowohl industrieller als auch in der Verwaltung aufgelistet. Ich glaube, wir waren bei über 100 Initiativen, die sowohl auf Bundes- als auch regionaler Ebene tätig sind. Daraus kann man ableiten, dass es bei vielen Initiativen, die alle individuell ihre Ziele verfolgen, schwierig wird, eine ganzheitliche Strategie zu entwickeln und verfolgen.

Deswegen wird sich Herr Mörl später noch einmal intensiv mit der Frage befassen, wer eine nationale Strategie zum Thema IT-Sicherheit koordiniert auf Basis bestehender Lösungen, noch fehlenden Technologien, einem geeigneten Integrationsgrad und der Nachfrage vom

Markt sowohl national wie auch international. Insofern ist meine letzte Folie ein bisschen als Übergang gedacht in die Podiumsdiskussion.

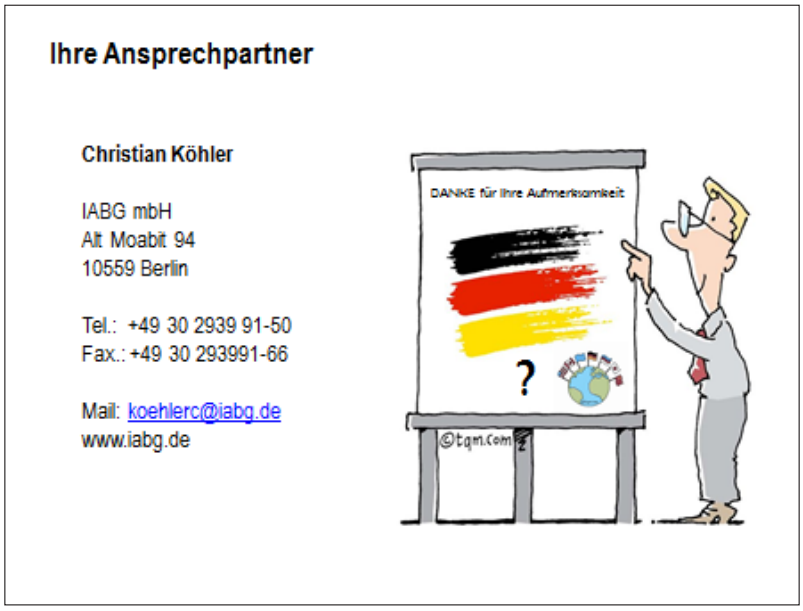


Bild 11

Der Folienzeichner hat sich noch Mühe gegeben bei der Frage: wie kommt man vom nationalen zum globalen Markt kommt (Bild 11). Das ist die Frage, die sich uns stellt.
Insofern war meine Aufgabe heute, die vorhandenen Studien darzustellen. Die enthaltenen Schwächen sind mir teilweise sehr bewusst, auch die Abgrenzung (Sicherheitswirtschaft und IT-Sicherheit) zu lösen war heute nicht meine Aufgabe. Für Fragen stehe ich gern zur Verfügung.

Fragen aus dem Plenum:

Frage: Haben Sie auch Zahlen der weltweiten Sicherheitswirtschaft?

Die Zahlen gibt es. Die habe ich für heute nicht aufbereitet. Da könnte man sicher noch einmal nachlesen. Für den Masterplan haben wir über 100 Studien analysiert. Da gibt es u.a. Gartner Studien, die auch verfügbar sind. Internationale Studien sind sehr stark verfügbar, europäische Studien gibt es einige. Es gibt einige Kerndienstleister, die für die Europäische Union relativ regelmäßig leisten. Nationale Studien gab es so gut wie keine, was auch ein Problem darstellt. Insofern waren wir in unseren Arbeiten froh, dass wir WISIND und das BIGS mit einbinden konnten. Im Nachhinein stellen wir auch fest, dass der Vergleich mit Wifor (Bild 9) ganz gut ist. Ich habe heute bewusst nur Zahlen zum deutschen IT-Sicherheitsmarkt aufbereitet und den Bezug zum deutschen IT-Markt gesucht. Aber natürlich gibt es internationale Studien.

Frage: Gab es den Versuch abzuschätzen, wie die Veröffentlichung der Snowden Dokumente die deutsche IT-Sicherheitswirtschaft beeinflusst?

Nein, gab es nicht. Wir haben auch in dem Gutachten zum Masterplan Sicherheitswirtschaft verschiedene Analysen versucht, z.B. mit dem DIN zusammen, ob man Wachstumspotenziale aus Normungsveröffentlichungen entnehmen kann, die in wissenschaftlichen Publikationen zu finden sind. Das DIN hat mit der DIN-Software auch einen Datenbestand, worauf wir versuchsweise zugreifen konnten. Wir wollten diese Analysemethode erst einmal überhaupt erproben. Es gibt somit ein kleines Kapitel im Masterplan, welches sich mit der Frage befasst, ob man, anhand von Veröffentlichungen im Bereich Normierung und Standardisierung ablesen kann, welche Wachstumspotenziale zu erkennen sind. So richtig ableiten konnten wir es erst einmal aus dem verfügbaren Datenbestand nicht. Möglicherweise sähe die Auswertung heute ganz anders aus.
Die Zahl hier (Wachstumsrate Wifor): Die ermittelte Wachstumsrate fällt geringer aus als in den Studien von WISIND, aber immerhin liegt sie auch hier wieder in dem Bereich des sonstigen Wachstums.
Ich versuche zwischen beiden Studien zu vergleichen. Bei Wifor erkennt man, dass sich der Sicherheitsmarkt bei 6,6 Mrd. € bewegt, Vergleich BIGS war 5 Mrd. €. Die Analysemethodik ist zwar unterschiedlich, aber die Größenordnung ist vielleicht durchaus relevant.
Auch hier noch einmal die Zahl (Erwerbstätige): das BIGS erfasst 81.000 Arbeitnehmern, bei Wifor sind es 63.000 Erwerbstätige. Natürlich gibt es da Abweichungen, die man auch noch einmal analysieren könnte. Eine Größenordnung an Beschäftigten, über die wir reden, haben wir schon einigermaßen erreicht.
Was ich noch entscheidend finde, um hierzu noch einmal zurückzugehen - sie haben die Zahl vielleicht im Kopf, ungefähr 6 ½ Mrd. € ist der Umsatz - ist die Exportquote der IT-Sicherheitswirtschaft, die ungefähr bei 1,2 Mrd. € liegt. Wir reden also über relativ geringes Exportvolumen. Nehmen wir uns noch einmal die Verteilung in Dienstleistung, Hardware und Software vor. Dabei reden wir insgesamt über 1,2 Mrd. € Exportleistung in dem Bereich. Die Importe, das haben wir vorhin gesehen, liegen bei 1,5 Mrd. €. Man kann demnach ableiten, dass Export relativ wenig stattfindet, bei einem sowieso schon relativ geringen Markt.

Frage: Wie versteht man das jetzt genau. Also, Importe in der Größenordnung von 1,5 Mrd. und Vorleistungen von 2,6 Mrd. Vorleistungen sind auch Importe?

Vorleistungen sind erst einmal Beschaffungen, Teile, die man für irgendeine Produktion vorher braucht. Das sind in dem Fall hier jetzt nicht Importe.

Frage: Also, beispielsweise Produkte einer Checkpoint Deutschland GmbH. Wie würden die hier aufgeteilt?

Die tauchen hier so erst einmal nicht auf. Das sind ja Daten aus der deutschen Statistik. Wenn Sie eine Checkpoint analysieren, dann tauchen letztendlich nur Leistungen, die Checkpoint in Deutschland erbringt -ich kenne die Struktur zu wenig -, in der deutschen Statistik auf. Ich kann im Moment nicht beurteilen, welcher Anteil der Leistungen über Importe geht, die von außen bezogen und hier nur vertrieben werden.

Frage: Das ist etwas, was als Anregung wirklich interessant ist, zu schauen wieviel Wertschöpfung von deutschen Unternehmen erbracht wird, wo die Entwicklung etc. hier stattfindet und wieviel von dem importiert wird, was an sozusagen Gesamtaufkommen hier umgesetzt wird? Das wäre vielleicht eine Anregung, ob man das noch einmal ausrechnen kann.

Nicht an mich. Ich weiß nicht, was dieses Jahr noch kommt. Diese Wifor Studie wird wohl auch dieses Jahr noch einmal aktualisiert. Aber es stimmt, es gibt ganz viele Fragen, die sich

daraus noch stellen. Was Sie natürlich hier auch nicht sehen, ist, wenn ein deutsches Unternehmen im Ausland auf Basis deutscher Vorleistung Produkte veredelt und im Ausland vertreibt. Es ist ja wie gesagt die Bruttowertschöpfung in Deutschland und nicht, was im Ausland passiert.
Ich finde übrigens auch die Unterscheidung nach Hardware, Software und Dienstleistungen ein bisschen grob, um wirklich detailliert analysieren zu können. Im Endeffekt kann man aber nur mit dem Datenschutz arbeiten, den man hat. Entweder er ist öffentlich verfügbar oder er muss mühsam erhoben werden. Nur die beiden Wege gibt es. Das habe ich heute versucht darzustellen.

Frage: Vielleicht haben Sie eine Erklärung dazu. Auf der Folie, wo die Relevanz, Maßnahmen und den Handlungsbedarf skizzieren sollte, gab es eine Spalte mit der Überschrift „Nationale Nachfrage" und da stand weder irgendetwas zur Relevanz noch zum Handlungsbedarf. Wenn ich mir überlege, dass es eigentlich um die Exportmöglichkeiten geht, dann frage ich mich, wie das zustande kommt, weil wie wollen Sie im Ausland etwas verkaufen, wenn hier nichts läuft.

Richtig. Erst einmal ist für den Masterplan ein Programm, Auftrag vorgegeben worden, wo – ohne viel zu verraten – das Thema nationale Lösungen auch bei der Bearbeitung des Masterplans schon eine Diskussion war. Es ist auch keine Frage, dass wir ähnlicher Meinung sind, dass man einen nationalen Referenzmarkt braucht, um auch international zu arbeiten. Unsere Aufgabe war es eine Studie, im Auftrag des BMWi zu erstellen. Der nationale Markt war hierbei nicht die Kernfrage des BMWi. Das ist vielleicht auch ein Punkt, den wir nachher noch einmal diskutieren können Kleinteilige Initiativen und Ressortzuständigkeiten beeinflussen die gesamte Strategie. Für unsere Arbeiten haben wir festgelegt, dass wir nur die 8Themen priorisieren, die wir beeinflussen können und das war hier unsere Methodik.

Frage: Bei uns kommt hier der Eindruck, dass die IT-Sicherheitswirtschaft eigentlich vernachlässigbar ist von den Umsätzen her. Ich glaube, wir müssen den Hebel betrachten, den diese Wirtschaft für die Gesamtwirtschaft bringt. Wir sind in Deutschland so gut, weil wir noch eine reale Wirtshaft haben. Wenn wir im Thema Industrie 4.0 oder Internet der Dinge wirklich Weltmarktführer werden wollen, dann geht es nur mit einer funktionierenden ITSicherheitswirtschaft. Man sollte einmal untersuchen, welchen Hebel diese Wirtshaft für die Gesamtwirtschaft hat. Dann kommen wir dem ganzen viel näher, nämlich der Bedeutung der IT-Sicherheit für die Industrie.

Meine Aufgabe war es, die aktuellen Marktzahlen darzustellen. Wahrscheinlich sind wir alle, die wir mit dem Thema IT-Sicherheit tagtäglich befasst sind, etwas geerdet worden durch die Zahlen besonders durch den geringen Prozentsatz des Marktanteils. Vielleicht hat der Eine oder Andere das anders eingeschätzt. Mehr wollte ich damit eigentlich nicht erreichen.

6 Der neue Arbeitskreis Sicherheitspolitik des BITKOM

Marc Fliehe, BITKOM e.V., Berlin

Wir sprechen über die Stärkung der IT-Sicherheitswirtschaft. Die Frage ist natürlich, welche Rolle die Verbände dabei spielen können. Zunächst einmal: Was sind die Aufgaben, die wir als Verband wahrnehmen? Im Prinzip geht es dabei darum, die Interessen der Wirtschaftsunternehmen, also die Interessen eines Verbandes in die Politik zu transportieren und umgekehrt auch die politischen Vorhaben zu unterstützen und mit dem Knowhow und auch der Expertise aus der Wirtschaft zu begleiten, um da gegenseitig zu einer guten Lösung zu kommen und im Sinne der IT-Sicherheit hier einen Beitrag zu leisten.

Es geht darum, Positionen und Interessen aufzunehmen und zu hören, wo denn Ihre Schmerzen sind, was die Ziele sind, die wir als Branche haben. Wo müssen wir vielleicht noch einmal nachjustieren? Wo können wir auch Unterstützung leisten?

Letztlich geht es dabei darum, dass die Verbände als Vermittler zwischen den politischen Sicherheitsinteressen und eben auch dem marktwirtschaftlichen Gesetzmäßigkeiten fungieren. Wie werden diese Ziele erreicht? Die Arbeitskreise sind eine Möglichkeit dazu, ein Instrument, das wir als Verband natürlich gerne nutzen. Wir haben den Arbeitskreis Sicherheitspolitik neu gegründet. Dazu ganz kurz ein paar Fakten. Wir haben im Mai die erste Sitzung gehabt und seitdem drei Sitzungen mit insgesamt 220 Teilnehmern. Die Themen, mit denen wir uns derzeit beschäftigen, sind natürlich das IT-Sicherheitsgesetz, auf der europäischen Ebene die NIS-Richtlinie. Auch die „Digitale Agenda“ ist nach wie vor ein Thema und die digitale Souveränität spielt eine Rolle.

Warum haben wir den Arbeitskreis Sicherheitspolitik neu gegründet? Zum einen, weil das Thema IT-Sicherheit an politischer Relevanz gewonnen hat, was auch eine gute Botschaft an die Branche als solche ist. Ausgelöst natürlich durch die Snowden Veröffentlichungen und die Diskussionen dazu, haben wir da einfach ein gewisses Mehr an Aufmerksamkeit gewonnen. Die Themen sind komplexer geworden, auch multidimensionaler. Gemeint ist damit, dass das nicht nur eine Sache von Technikern ist, sondern auch Datenschutzexperten mit im Boot sind, wenn wir über IT-Sicherheit reden. Dass wir Juristen brauchen, die sich mit der Thematik beschäftigen und eben die vielfältigen Aspekte der IT-Sicherheit dort abgebildet werden. Letztlich hat auch der Vertrauensverlust, den wir durch die ganzen Diskussionen im letzten Jahr erlitten haben, dazu beigetragen, dass wir uns hier stärker positionieren müssen.
Wenn wir uns ansehen, was die Ziele eines Arbeitskreises sind und warum es die Arbeitskreise überhaupt gibt, dann natürlich um eine bestimmte Form des Austauschs, der Diskussion, des Diskurses auch zu ermöglichen, die dazu führt, dass wir dann auch zu Positionen kommen, die wir in die Politik tragen können und wo wir die Politik auch unterstützen können. Letztlich geht es immer darum, sprechfähig zu sein als Verband natürlich, und auch darum, diese Position als Vermittler wahrnehmen zu können.
Die inhaltliche Ausrichtung dieses Arbeitskreises ist das Instrument der Kommunikation, Positionspapiere, politische Stellungnahmen auf verschiedenen Ebenen, wo die Kommunikation stattfindet mit Vertretern von Bundes- und Landesregierungen, nach geordneten Behörden wie dem BSI beispielsweise, mit Ministerien, Fachpolitikern.
Letztlich geht es hier dabei auch wirklich darum, einen Beitrag im Sinne der Fach- und Sacharbeit zu leisten.

Der Vollständigkeit halber ein ganz kurzer Überblick, damit Sie einordnen können, wo der Arbeitskreis Sicherheitspolitik im BITKOM verortet ist. Er ist im Bereich IT-Sicherheit angesiedelt zwischen den anderen Arbeitskreisen, die es seit Jahren gibt in diesem Sicherheitsmanagement, Sicherheitslösungen und Sicherheitstechnologien mit den zugehörigen Fachausschüssen und dem Dialogkreis, den auch der eine oder andere von Ihnen kennt. Wenn Sie da einen Beitrag leisten möchten – Herr Grabowski hat Sie heute schon herzlich eingeladen, sich aktiv zu beteiligen -, auch von mit gern die Einladung. Falls Sie Interesse haben, sich hier einzubringen, geben Sie mir ein Signal und ich würde mich natürlich freuen, wenn wir gemeinsam an den Themen weiterarbeiten können.

7 Impulsvorträge der IT-Sicherheitswirtschaft

7.1 Ramon Mörl, itWatch GmbH, München

Wir haben einen guten Auftakt hinter uns gehabt und ich möchte den Begriff von Herrn Schallbruch, das Näherzusammenrücken, aufnehmen. Bei mir – ich bin aus München - heißt das nationale Vertrauenskette. Meinen kurzen Beitrag möchte ich von hinten aufzäumen, also mit dem Ergebnis anfangen.

Ich bin der festen Überzeugung, wenn wir die nationale IT- Security stärken wollen, brauchen wir etwas, was in meinem Sprachgebrauch nationale IT-Security-Vertrauenskette heißt oder kurz nationale IT-Vertrauenskette. Über die Notwendigkeit dieser Handlung, brauchen wir uns nicht zu unterhalten. Wir haben die Forderung der digitalen Souveränität. Jeder, der ein größeres Unternehmen leitet, hat auch die Forderung der digitalen Souveränität, weil wenn ich meine Daten der Elektronik anvertraue, dann will ich souverän mit ihnen umgehen, also entscheiden, wer sie wo und wie verarbeitet. Insofern haben wir jetzt seit noch nicht allzu langer Zeit den Begriff der digitalen Souveränität, der unsere Handlungen motiviert.

Schauen wir ganz kurz, was die aktuelle Situation ist. Einige, die heute hier wieder im Kreis sitzen, haben sich gestern auch in einer ehrenhaften Runde versammelt und wir hatten zwei Podiumsdiskussionen. Ich kann Ihnen sagen, dass ich wieder erlebt habe, wie deutsche IT-Sicherheit funktioniert. Da sitzen zwei Hersteller, die total unterschiedliche Gebiete bewirtschaften und bevor sie über Integration nachdenken, schimpft der eine, dass der andere das nicht gut macht und er es viel besser könnte.

Wenn wir eine nationale Vertrauenskette oder das nach Herrn Schallbruch Näherzusammenrücken wirklich wollen, dann müssen wir schauen, wie das gehen kann. Also, nicht nur eine Lösung propagieren, sondern von einer Gesamtlösung sprechen. Wir klappen nicht 20 Logos an die Wand, sondern sehen, dass irgendjemand auf der Welt ein Problem hat, das wir kollektiv lösen können.

Dr. Grabowski hat es vorhin schon angesprochen. Ich glaube, er kann bestätigen, dass man zu dem Zeitpunkt, zu dem man mit 25 Leuten in einer Delegation auftritt, von denen jeder eine Story erzählt und alle anderen schon eingeschlafen sind, keinen im Ausland abholt. Wenn man ankommt und sagt: ihr habt Probleme, die wir alle in einem einzigen Antritt lösen können, dann hat man Fachleute dabei, die alle von unterschiedlichen Unternehmen sein können. Das ist alles kein Problem. Dann bekommt man auf einmal ein Lösungsverständnis und der andere hört zu.

Was finden wir in Deutschland vor? Christian Köhler hat es vorhin gesagt. Es ist zersplittert und der Kunde hat keine Lust mehr, 30 Pflaster auf eine Wunde zu kleben, mit 50 Anbietern zu reden und alle kommen mit ihren Unique Selling Points (Alleinstellungsmerkmalen) und sagen, dass sie viel besser wären. Der Markt der IT-Sicherheit möchte nach meiner Analyse auf Knopfdruck sicher werden. Wenn da jemand im Markt Cyber Security auf Knopfdruck versprechen würde; wir fangen heute klein, morgen geht es ein bisschen größer weiter und nach fünf Jahren haben wir das erreicht, weil die Marktbreite so groß ist, dass das machbar ist. Das ist ein ganz anderes herangehen. Wir reden dann über LifeCycle, über Einfachheit, also Reduzierung der Komplexität und all diese Dinge.

Was passiert genau? Christian Köhler hat Zahlen vorgestellt, alles ist ziemlich kompliziert. Ich habe gestern im Spaß gesagt, dass ich über die Komplexität der IT-Sicherheit heute nichts wiederholen will. Es ist alles nicht so kompliziert, wenn man es genau betrachtet. Wenn man digitale Souveränität machen will, dann kann man verschiedene Handlungsfelder identifizieren. Einer ist, dass die Amerikaner total Klasse in Start-ups sind. Wir könnten auf die Idee kommen, Start-ups ohne Ende zu fördern. Wir haben vorhin bereits gehört, dass der Markt ziemlich zersplittert ist. Was würden wir tun? Wir würden den zersplitterten Markt noch mehr zersplittern. Wir könnten auf die Idee kommen, es total einfach zu machen und 2 Mrd. in die Forschung geben. Wir wollen einfach das Thema IT-Sicherheit richtig verstehen und jetzt richtig forschen. Dazu muss man natürlich verstehen, dass wir Weltmeister im Forschen sind, aber extrem schwach im Umsetzen der Wertschöpfung auf Forschung. Das heißt, am Ende vom Tag wird passieren, dass die zwei Mrd. in die Forschung investiert sind und eine Menge tolle Ideen und Lösungen herauskommen. Wer macht das Geld damit? Amerikaner, Chinesen, Israelis. Die Frage ist, ob wir das wollen. Wenn wir die digitale Souveränität ernst nehmen, dann können wir das nicht wollen.

Was wollen wir eigentlich, wenn wir digitale Souveränität ernst nehmen? Wir wollen, dass wir auf den Assets, die wir verschenken, verkaufen, hergegeben haben, sicher operieren können.

Ich habe keine Lust, darüber zu reden, dass wir Kupferkabel zurückkaufen. Die sind weg. Das macht auch nichts. Wir müssen auch nicht neue Betriebssysteme entwickeln, die dann ganz sicher sind, weil es nie ein sicheres Betriebssystem geben wird. Das ist Utopie.
Wir brauchen jemand, der auf den ganzen unsicheren Dingen eine Sicherheitsarchitektur konzipiert hat, und ich möchte jetzt die Bauelemente für diese Sicherheitsarchitektur möglichst in einer vertrauensvollen Umgebung besetzen. Ich habe jetzt noch nicht national gesagt, aber natürlich ist es so, dass bei den höchsten Gütern, die man national verwaltet, auch die Herkunft einen Punkt macht.

Wir haben in der Lebensmittelindustrie eine genaue Bezeichnung dafür, welches Fleisch woher kommt, Gammelfleischskandal usw. In der IT-Security machen wir uns darum überhaupt keinen Kopf. Das Zeug hat irgendein schlecht schlafender Entwickler einmal in Thailand entwickelt und jetzt wird es weltweit verwendet. Dementsprechend ist auch die Sicherheit weltweit. Das heißt, mein Plädoyer, was wir tun sollten, ist, dass wir eine nationale Vertrauenskette haben sollten. Um die zu haben, müssten wir die Exzellenz bündeln ohne gegeneinander zu arbeiten und Folgendes festzustellen: Wo stehen wir heute? Welche Assets haben wir?

Erlauben Sie mir noch einen kleinen Einschub. Viele Teilnehmer im Markt, 80 Mio. Privatbürger, glauben, dass alles sicher ist, nur wenn man ein Passwort irgendwo eintippt. Die Expertise, zu unterscheiden welche Mechanismusstärke, welche Robustheit ein Verfahren in der IT-Sicherheit hat, haben in diesem Land ganz wenige. Das ist ganz schlecht für die IT-Sicherheit. Wir reden über Dinge, wo wir glauben, zu verstehen und daraus ziehen wir Schlüsse.

Ein aktuelles Beispiel: wenn ich der Meinung bin, dass ich die Wertschöpfung in Deutschland von IT-Sicherheit anschaue und das, was am intensivsten wertgeschöpft wird, exportiere ich. Dann komme ich sofort darauf, dass ich Dienstleistung exportieren muss. Gleichzeitig haben wir keine Fachleute. Wir haben einen extremen Fachpersonalmangel. Wenn ich also sage, Dienstleistung ist das, wo die höchste Wertschöpfung in Deutschland passiert, und das exportiere ich, dann gehe ich in eine Mangelwirtschaft, weil eine engpasskonzentrierte Strategie sagen würde, dass ich notwendigerweise fördern muss, was ich nicht habe: Personal.

Also, IT-Sicherheit entsteht durch sichere Lösungen. Lösungen brauchen ein ganzes Umfeld. Wenn wir unsere Experten zusammenpacken und denen sagen, wo wir stehen, was wir an Bord haben, identifiziert uns eine Sicherheitsarchitektur, die darauf funktioniert, identifiziert das Delta (was wir noch nicht haben) und dann brauchen wir einen katalytischen Effekt im Markt, der bewirkt, dass wir dieses Delta jetzt auch mit eigenen Ressourcen erstellen können. Dann hätten wir etwas geschafft, was die IT-Sicherheitsindustrie bündelt, zusammenbringt und tatsächlich in einem One-Klick Interface im besten Falle weltweit vertriebsfähig macht.
Das ist mein Statement. Ich bin Ramon Mörl, Gründer, Gesellschafter und Geschäftsführer von der itWatch. Wir machen Betriebssysteme, die relativ marktgängig sind, sicher, so dass man sie auch in geheimen Umgebungen einsetzen kann. Aber das ist nicht der Punkt, warum ich hier bin, sondern um anzuregen, diese nationale Vertrauenskette tatsächlich anzugehen zu bauen.

7.2 Dr. Magnus Harlander, genua GmbH, Kirchheim

Ich komme mir ein bisschen vor wie im Krankenhaus. Der Patient liegt auf dem Bett und jeder grübelt darüber, was er denn hat. Ich möchte mich anschließen, zuerst über den Patienten philosophieren und hinterher vielleicht eine Medikamentierung oder Behandlungsmethode präsentieren - zumindest aus meiner Sicht. Der Patient ist die IT- Sicherheitswirtschaft in Deutschland, die, wie alle immer sagen, ganz stark mittelständisch geprägt ist. Ich sehe das auch so, aber mit dem Begriff „mittelständisch geprägt" hat man die Sache nicht ganz erfasst, weil ein Mittelständler ganz individuell entstehen und sich aufstellen kann.

Wenn man auf die hier vertretenen Firmen blickt, gibt es ganz unterschiedliche Konstellationen. Es gibt Firmen, die als 100%ige Töchter oder mit sehr großen Anteilen an große Konzerne angegliedert sind. Secunet gehört dazu, Rhode & Schwarz - SIT, um nur einige zu nennen.

Es gibt Firmen, die von Anfang an über Venture Capital finanziert wurden und versuchen, sich auf diese Art und Weise weiterzuentwickeln. Es gibt erstaunlicherweise ganz wenig Start-ups. Das ist auch leicht verständlich. Start-ups müssen irgendwie schnell zu Geld kommen, weil die Investoren ihr Geld bald wieder sehen wollen und die IT-Sicherheitsbranche aber lange braucht, um etwas, was man entwickelt hat, auch zu Geld zu machen. Deswegen ist das eine Branche, die zu Start-ups ganz schlecht passt.

Dann gibt es Unternehmen, die sehr stark eigenfinanziert sind, zu denen wir, die genua, gehören. Ich bin selbst Gründer, Gesellschafter und Geschäftsführer des Unternehmens und seit 22 Jahren im Bereich IT-Sicherheit mit dem Fokus auf den Hochsicherheitsmarkt tätig. Wenn ich von Hochsicherheitsmarkt spreche, meine ich nicht nur den öffentlichen Anteil. Wir haben auch einen starken Fokus auf sehr sicherheitsbewusste Bereiche in der Industrie. Es ist für uns ganz wichtig, diese beiden Beine immer gleichmäßig ausgelastet zu bekommen
Wir arbeiten seit 22 Jahren sozusagen von der ersten Stunde an ohne fremdes Kapital im Unternehmen. Das ist etwas ungewöhnlich und konservativ. Wir fahren aber damit ganz gut und wissen auch, warum wir das so tun. Für uns bedeutet es, dass wir einfach komplett selbstbestimmt arbeiten können. Das ist wichtig, weil gerade im IT-Sicherheitsbereich ein langer Atem für Nachhaltigkeit eine ganz wichtige Größe ist. Man denke nur Zulassungsverfahren, die oft Jahre dauern, bis man dann mit dem Produkt sozusagen endlich durch ist. Das dauert einfach und es ist schwer, es dem Investor zu erklären. Man hat natürlich auch viel mehr Möglichkeiten, sein Unternehmen zu gestalten. Wir hätten, glaube ich, auch Schwierigkeiten, unseren Investoren zu erklären, warum wir so eine komische Kindertagesstätte betreiben und da jedes Jahr zig Tausend Euro zuschießen, weil das schon wieder 3% der Rendite kosten würde. Diese Spielräume nutzen wir, um einfacher an Mitarbeiter zu kommen und sie zu halten.

Jetzt ein kurzer Blick auf die Lage. Wir sind in Deutschland von Thema zu Thema ganz unterschiedlich aufgestellt. Ich denke, dass die Bedürfnisse der verschiedenen Teilnehmer in dem Markt doch etwas unterschiedlich sind, aber helfen kann man vielleicht allen mit den gleichen Mitteln. Ich möchte einen Blick auf die Themen werfen, die wir in Deutschland überhaupt bearbeiten können und sollten.
Ein ganz wichtiges Thema ist in jedem Fall Open Source. Open Source ist in Deutschland eine sehr stark verwurzelte Technologie. Eine Plattform mit starker Beteiligung an Entwicklern und weiter Verbreitung auf der Betriebssystem und Anwendungsebene. Ganz viele Open Source Komponenten finden sich in vielen Bereichen der Industrie und auch in der öffentlichen

Wirtschaft. Das ist ein wichtiges Thema, wo man sich technologisch auch leicht weiterentwickeln kann.

Ein zweites Thema, ist die Möglichkeit, überhaupt sichere Systeme bauen zu können, d.h. sichere Plattformen zu bauen. Ich bringe hier den Begriff „Microkernel basierte Separationssysteme“, ein Thema, das weltweit Aufmerksamkeit erregt. Die Leute, die das beherrschen, stehen momentan ganz oben auf der Akquisitionsliste. Kleine Firmen, die das können, wurden in den letzten Jahren fast alle von großen Firmen weg gekauft, meistens von Rüstungskonzernen. Wir haben noch solche Technologien im Land und die gilt es am Leben zu halten.

Der dritte Bereich, Kryptographie, ist etwas, was wir gut kennen und was Basis fast aller Sicherheitstechnologien sind. Da gilt es dranzubleiben.

Der vierte Bereich, vielleicht überraschend für den einen oder anderen, ist Hardware. Ich bin hier nicht dafür, Intel mit deutschen Technologien aus dem Markt zu drängen. Aber wir haben in Deutschland eine Infineon, eine NXP, die in der Lage sind, Prozessoren zu bauen und die auch in der Lage wären, Prozessoren zu bauen, die man insbesondere im Bereich Industrie 4.0, im Bereich kritischer Infrastrukturen an kritischen Übergabepunkten nutzen könnte. Ich denke an eine flexible ARM-basierte Hardwareplattform, die auch entsprechend leistungsfähig ist. Wenn man das wieder selber bauen könnte, könnte man in Deutschland sehr viel mehr machen. Das ist vielleicht auch ein Appell an die Bundesregierung, sich mal mit den Firmen in Verbindung setzen und das als Geschäftsmodell vorschlagen, so dass wir Mittelständler, zumindest wieder ein Stück vertrauenswürdige Hardware zurückbekommen.

Das sind die Themen. Was wären die konkreten Maßnahmen also Behandlungsmethoden? Ich habe hier ein paar Adressaten. Auf alle Fälle den öffentlichen Auftraggeber an allererster Stelle. Ich sagte vorhin schon, dass es für uns alle wichtig ist, eine zuverlässige Nachfragebasis in Deutschland zu haben. Ich erwähne immer wieder, dass die Bundeswehr seit zehn Jahren, obwohl ausreichende deutsche Kryptotechnologie zur Verfügung steht, diese nicht nutzt, sondern sich von amerikanischen Herstellern beliefern lässt. Das geht einfach nicht.

Zweiter Punkt: auch die Industrie ist jemand, der Nachfrage schaffen kann. Tatsächlich ist es sogar noch viel mehr Nachfrage als die öffentliche Hand. Ich denke, dass da ein Bewusstseinswandel einsetzen muss. Wir sehen, dass dieser mit Snowden eingesetzt hat, dass man im Bereich der Industrie nicht mehr nur diese klassische One-Shop Politik fährt, d.h. man geht zu McAfee oder Symantec, die von allem was im Portfolio haben, weil sie alles irgendwie zusammengekauft haben, was es in dem Bereich gibt. Der Einkäufer ist glücklich und hat wenig Arbeit. Ein Vertrag und alles ist gut.

Es wird in Deutschland wahrscheinlich keinen Konzern geben, der das anbieten wird. Deswegen muss man sich mit mittelständischen Unternehmen zusammentun und ich kann sagen, dass wir bisher so gut wie keinen Kunden verloren haben, weil wir mit den Kunden reden und mit uns reden lassen.

Auch das BSI ist eine ganz wichtige Instanz mit den Zertifizierungs- und Zulassungsverfahren. Das sind Dinge, die für uns sehr wichtig sind und die ich nicht missen möchte. Ich möchte aber einfach einmal festhalten, dass die Verfahren momentan für uns und wahrscheinlich für die meisten, die das durchmachen, sehr belastend sind, weil es sehr langwierige Prozesse sind und der Nutzen erst ganz am Ende entsteht, wenn man die entsprechenden Zulassungen hat. Da ist man oft schon zwei, drei oder noch mehr Jahre hinter dem Markt her. Time to market ist aber ein wichtiges Thema und gerade die IT-Industrie ist sehr schnelllebig und man kann nicht

jahrelang warten, bis man endlich ein Produkt zum Kunden bringt. Deswegen mein Plädoyer, auch in Richtung BSI, darüber nachzudenken, wie man die Prozesse und Verfahren vielleicht anders gestalten könnte.

Mein nächster Punkt sind Universitäten und der Ausbildungsbereich. Mit der IT-Sicherheit wird es hier in Deutschland nichts werden, wenn wir nicht mehr Leute haben, die sich hiermit auskennen und sich damit befassen wollen. Es muss nicht jeder Firewall Produkte entwickeln, aber es müssen viel mehr Leute in der Lage sein, zu verstehen, was man ihnen erzählt. Das gilt für die IT-Ausbildung und genauso für den Bereich der Ingenieurswissenschaften.

Elektrotechnik und Maschinenbau sind diejenigen, die dieses Industrie 4.0 Thema sozusagen in den Händen haben und mir wird ganz Angst und Bange, wenn ich überlege, wie die an das Thema ran gehen, weil sie einfach wenig Ahnung von IT-Sicherheit haben. Das ist einfach nicht Thema ihrer Ausbildung. Das ist ein ganz wichtiges Problem.

Wenn wir Export machen wollen, dann glaube ich, dass wir Mittelständler, so wie wir aufgestellt sind, nicht mal schnell den fernasiatischen Markt erobern wollen und können. Wir können das nur mit großen Systemhäusern zusammen. Deswegen mein Appell an die großen Systemhäuser, wie z.B. die T-Systems oder auch einer IBM, auch wenn sie aus USA kommen, sich auf uns einzulassen und sozusagen mit uns auf Augenhöhe zu reden und uns nicht als Bittsteller. zu behandeln.

7.3 Dr. Christoph Peylo, Trust2Core GmbH, Berlin

Wenn ich über den Patienten spreche, möchte ich Ihnen drei Kurven aufmalen (Bild 1) und zwar wenn wir hier ungefähr Kosten haben, hier die Zeit, dann sind die Kostenfunktionen, IT-Systeme abzusichern, was heute ungefähr so aussieht. Es wird also immer steiler und schwieriger.

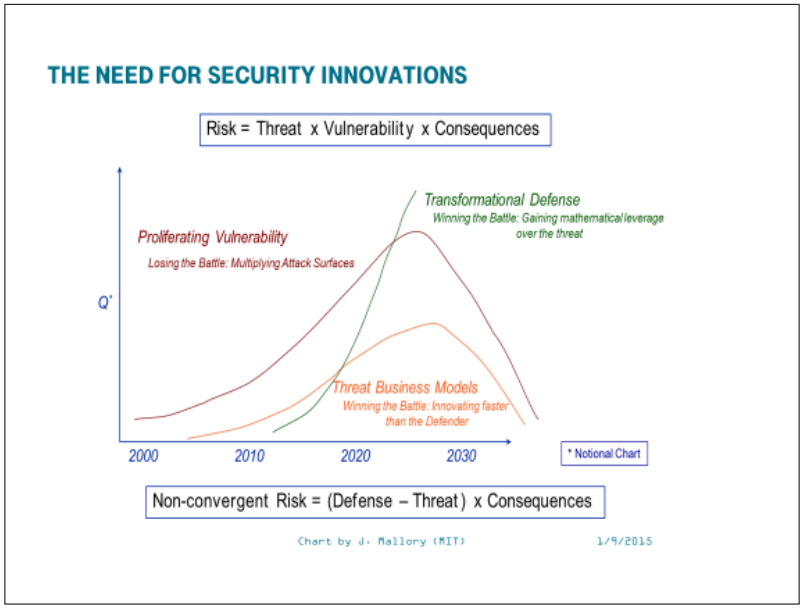


Bild 1

Das ist der Patient, d.h. dem Patient geht es eigentlich immer schlechter, weil es so viele Angriffsvektoren gibt. Andererseits vernetzen wir immer mehr. Ich bin nicht der Ansicht, dass das nichts ausmacht, dass wir unsichere Betriebssysteme haben und dass wir mit unsicheren Sprachen programmieren, sondern das führt dazu, dass die kompletten Systeme immer unsicherer werden. Vor allem ist es leider so, wenn ich auf eine wackelige Sache noch etwas Wackeliges stelle, wird das Fundament dadurch nicht besser. Wenn ich kein sicheres Betriebssystem habe, mit schwierigen Sprachen ein Programm geschrieben habe, dann ist es mir nicht mehr möglich, ein Trusted Execution Environment mit sicherer Laufzeitumgebung zu haben, in der ich dann auch verschlüsseln und entschlüsseln kann. Das ist das Problem. Da nützt mir auch die beste Krypto nichts, wenn ich keine Laufzeitumgebung habe, in der ich den Prozess absichern kann.

Diese Problematik spiegelt sich auch darin nieder: Wenn ich systematisch mein Geschäft sichern will, meine Supply Chain sichern möchte, dann wird das immer teurer. Damit wird es auch total unattraktiv, alles zu vernetzen. Das ist eben auch unser Problem als IT-Dienstleister oder IT-Sicherheitsdienstleister. Wenn die Effizienzersparnisse geringer sind als die Kosten das abzusichern, ist das komplett uninteressant, weil die Märkte, in denen wir über IT und das Internet of Things nachdenken, über M2M, dann sind das oft sehr margenschwache Märkte wie Handel, Logistik und da ist einfach nicht das Investitionskapital da, das so abzusichern. Die Schwierigkeit ist, dass für die Angreifer die Welt viel besser aussieht. Da ist die Kostenfunktion günstiger, weil die sich nur einen Angriffsvektor ausdenken müssen. Als Verteidiger

müssen Sie alles absichern. Sie wissen ja nicht, wie der Angreifer angreift, eine ungute Situation. Für den Angreifer ist es sehr bequem, und das Angreifen ist ein lukratives Geschäft geworden. Vor 10, 15 Jahren war das so, dass die Hacker eigentlich mit irgendetwas demonstrieren wollten, wie superklug sie sind. Heutzutage ist das ein echtes Geschäft geworden.

Was können wir machen, um das zu ändern? Wir müssen den Innovationsdruck, der jetzt auf dem Herstellern liegt, die Systeme irgendwie sicherer, die Schutzmechanismen ausgefeilter zu machen, erhöhen. Diese Innovationen kosten einfach Geld. Wir müssen eigentlich mit so stabilen Systemen und Architekturen arbeiten, dass es für den Angreifer schwieriger wird reinzukommen, dass der sozusagen den Investitionsdruck hat. Es wird für ihn dann immer teurer anzugreifen, um sichere Systeme zu knacken, wenn diese Systeme mehr modular aufgebaut sind. Herr Harlander hatte gerade mit der Microkernel Technologie, die wir auch anwenden, ein sehr gutes Beispiel genannt. Dann haben wir eine reelle Chance und können etwas erreichen.

Das Problem ist jetzt natürlich, dass wir gegen 40 Jahre Selektionsdruck in der IT-Industrie arbeiten müssen, weil der Selektionsdruck in dieser IT-Industrie so war, dass schnellere Systeme, user-freundlich entstanden sind, aber keine Sicherheitsarchitektur. Konzeptionell sind unsere Systeme eigentlich 60 Jahre zurück, und davon profitieren Angreifer. Wir brauchen hier einen Wechsel und das kann die Industrie aus meiner Sicht nicht ganz allein leisten. Bei diesem Paradigmenwechsel ist auch der Staat gefragt. Andere Staaten machen es vor. Es hieß gerade, dass es keine Security Start-ups gibt oder es schwierig für Security Start-ups ist. Das stimmt vor allem in Deutschland. In Israel sind in diesem Jahr 800 neue Security Start-ups schon gegründet worden. Man muss sagen, dass in den USA und in Israel eine ganz andere Förderung in dem Bereich gemacht wird, und das fängt auch schon früh an. Das ist vielleicht etwas, was man sich da als Vorbild nehmen könnte.

Für uns, für die Industrie, wäre es auch angemessen, nachzudenken über gewisse Technologien, über grundsätzliche Technologien, die wir brauchen, weil wir - machen wir uns nichts vor - im Hardwaremarkt oder im Markt für Betriebssysteme als deutsche Unternehmen eigentlich nichts mehr zu melden haben. Das ist komplett an uns vorbeigegangen, sehr schwierig.

Andererseits z.B. ist diese Microkernel Technologie, die übrigens auf eine Doktorarbeit an der TU Berlin zurückgeht, hier entwickelt worden ist und jetzt in alle Welt verkauft wird. Auch wir haben für unser sicheres mobiles Device auf einer Open Source Technologie aufgesetzt. Mit Open Source lässt sich auch Geld verdienen. Das machen auch andere Unternehmen vor. Die Schwierigkeit ist, dass man mit dem Knowhow, das in der Open Source Technologie steckt, Geld verdienen muss und nicht mit dem Quellcode an und für sich. Den Quellcode aber weiterzuentwickeln durch eine Community, die nicht nur Studenten sein müssen, sondern es kann auch ein Unternehmen sein, macht durchaus Sinn. Dann kann man in den Gebieten, wo man kollaborieren kann, wo man eine gemeinsame Infrastruktur braucht, wo man keinen Wettbewerb gegeneinander hat, kollaborieren und dann in seinen einzelnen Segmenten sein Geld verdienen. Dieser Paradigmenwechsel muss auch in den Köpfen stattfinden, und da sind die Unternehmen gefragt. Aber in dem 40jährigen gegen diese Selektion arbeiten, gestehe ich, dass das etwas ist, wo auch entsprechende Unterstützung der Öffentlichkeit notwendig ist.

Lassen Sie mich ganz kurz zusammenfassen: Die Situation ist relativ kritisch. Ich beurteile sie relativ pessimistisch, was die Absicherungsmöglichkeiten der Infrastruktur heute, auch der kritischen Infrastruktur anbelangt. Das Kind ist aber noch nicht vollkommen im Brunnen. Wir können da etwas machen. Die Rezepte liegen eigentlich auf dem Tisch und diejenigen, die dazu entwickelt wurden, sind teilweise auch schon 5, 10, 20 Jahre alt. Es gibt sichere Program-

miersprachen, die gewisse Basisfehler nicht haben. Wenn Sie sich z.B. irgendwelche Reports anschauen über die gängigsten Fehler von Programmiersprachen und von Programmen, hat sich das in 20 Jahren kaum geändert. Die Fehler werden immer wieder gemacht, wenn man mal eben auf die alten Technologien zurückgreift. Hier angemessen zu reagieren, stabilere Programmiersprachen für stabilere Systeme, wie z.B. diese Microkernel Technologie kollaborativ weiterzuentwickeln und auch vielleicht mit staatlicher Unterstützung weiterzuentwickeln, macht auf alle Fälle Sinn, um uns hier als IT-Wirtschaft entwickeln zu können und von Ideen, wie Internet of Frames, End-to-End dann auch gemeinsam profitieren zu können.

7.4 Dr. Rainer Baumgart, secunet Security Networks AG, Essen:

Zum Thema IT-Sicherheit ist heute Abend schon viel gesagt worden und das meiste wahrscheinlich auch nicht zum ersten Mal. Es ist ungefähr 10 Jahre her, dass wir mit einigen Vertretern der IT-Sicherheitsbranche in Tokio zusammensaßen und sinniert haben, wie man die deutsche Sicherheitswirtschaft fördern könnte. Die gleichen Argumente sind heute wieder genannt worden. Allerdings kommt das Thema heute ein bisschen mehr in der Gesellschaft an.

Wir hatten einen kleinen Marketingeffekt, der Snowden hieß und es wurde wiederholt gesagt, dass doch alle bei uns sichere Produkte und Lösungen kaufen müssten, wir aber nicht lieferfähig seien. Gekauft haben aber doch nicht alle, weil die Rahmenbedingungen wahrscheinlich doch andere sind, als man sie sich vielleicht vorstellte.

Wir haben heute bereits auch einiges darüber gehört, was uns Schwierigkeiten bereitet. Die Bundesregierung bemüht sich mit der digitalen Agenda, Deutschland zur Nr. 1 in Europa im Bereich IT zu machen. Dazu soll die IT-Sicherheit massive Beiträge leisten. Ich bin gespannt, wie sie das umsetzen wird.

Was häufig vergessen wird: wir haben ein paar gute Technologien im Land. Einige sind schon erwähnt worden. Separierung und Mikrokern stehen auf meiner Liste ganz oben. Auch mit Chipkarten haben wir langjährige Erfahrungen und sind teilweise Weltmarktführer, sowohl bei den Herstellungsprozessen als auch Betriebssystemen und allem was dazu gehört. Wir haben Verschlüsselungstechnologien und verfügen über entsprechende Kompetenz – hier besetzen wir eine international renommierte Position. In Europa können wir als Krypto-Nation mitreden. Davon gibt es insgesamt nur drei! Also sind wir europäisch vergleichsweise gut positioniert.

Andere Technologien sind Frühwarnsysteme, Biometrie, PKI, elektronische Identitäten. Letzteres Thema hat mittlerweile international ein extrem hohes Ansehen erlangt und wir vertreiben die Technik weltweit. Das wird manchmal in den Statistiken die wir heute gesehen haben nicht einbezogen. Aber hier können wir Erfolge vorweisen und sollten unser Licht nicht unter den Scheffel stellen.

In Deutschland haben wir im Grunde genommen ganz gute Voraussetzungen. Beispielsweise haben wir hohe Wertvorstellungen im Bereich Datenschutz. Das ist traditionell bei uns verankert. Wir haben hier aber auch eine offene Krypto-Politik. In anderen Ländern war Kryptographie jahrelang generell verboten. Wenn Sie mit einer Chipkarte einreisten, waren Sie praktisch schon mit einem Bein im Gefängnis. Das ist bei uns nicht der Fall und das gibt uns durchaus Freiheiten, Dinge zu entwickeln und zu tun, ohne dass sie entsprechend unter Vorbehalt stehen. Das fördert auch Kompetenzen.

Wir haben natürlich eine sehr zersplitterte, kleinteilige – heute auch schon mehrfach gesagt – IT-Sicherheitsindustrie in Deutschland und nur wenige große Player. Wir sind ebenfalls ein mittelständisches Unternehmen, ich würde secunet aber trotzdem als Marktführer bezeichnen. Mit etwas mehr als 300 Mitarbeitern sind Sie bereits Marktführer in Deutschland! Es gibt viele kleinere Unternehmen, die wir versuchen im TeleTrusT zu bündeln, um die Interessenslagen strategisch aufeinander abzustimmen und auch ein Sprachrohr in Richtung Politik zu sein. Wir reden mit dem Wirtschaftsministerium, wir reden mit dem Innenministerium und versuchen für die gesamte Branche einiges zu erreichen.
Viele Unternehmen stecken in Nischen und haben diese genutzt, um sich zu spezialisieren. Und viele warten darauf, dass ein Investor kommt und sie aufkauft. Das ist durchaus auch ein

Geschäftsmodell. Ein Geschäftsmodell von Start-ups oder zumindest vieler Start-ups. Das heißt aber auch, wenn wir – wie so oft gefordert – insbesondere Start-ups fördern, fördern wir damit eventuell auch den Ausverkauf der deutschen Sicherheitsindustrie. Das ist für mich naheliegend.

Wir befinden uns momentan vielleicht an einer Schwelle, an der man strategisch neu überlegen muss, was man künftig macht und welche angemessenen Sicherheitsniveaus man aufgrund der gestiegenen Vorfälle in dieser Wissensgesellschaft Deutschland eigentlich erreichen will? Welche Ziele will man sich setzen und welche dazugehörige staatliche Regulierung brauchen wir? Wir brauchen eine staatliche Regulierung!

In diesem Zusammenhang wird häufig das Beispiel des Sicherheitsgurtes bemüht. Ich mache das auch. Früher hatte man einen Sicherheitsgurt im Fahrzeug und keiner legte ihn an. Die Folge: 15.000 Tote im Jahr. Mit einem Film („Der siebte Sinn“) hatte man sich das Ziel gesetzt, die Zahl der Verkehrstoten zu senken. Später dann wurden die Fahrzeughersteller verpflichtet, Gurte einzubauen. Das war der Beginn der Regulierung. Aber es passierte nichts, kaum einer hat sie benutzt. Dann kam eine gesetzliche Pflicht den Gurt anzulegen. Wurde man ohne angelegten Gurt erwischt, kostete es 10 Mark Strafe. 10 Mark war auch damals nicht viel Geld, aber die Anschnallquote stieg direkt auf über 90%. Die Zahl der Verkehrstoten ging dramatisch zurück.

So gibt es wahrscheinlich noch viele andere ähnliche Beispiele in der Industrie. Wenn man nur darauf vertraut, dass die Industrie oder die Allgemeinheit sich selbst schützt, passiert wenig bis nichts.

Ein weiteres Beispiel ist das Gesundheitswesen. Wenn es keine Impfpflicht gibt, wird sich niemand impfen lassen. Dann haben wir die Seuche. Wenn wir keine Meldepflicht bei der Hühnerpest einführen, kann sich auch hier eine Seuche ausbreiten. Und wenn wir dann nicht regulierend eingreifen oder uns zurückhalten, weil wir glauben, wir zerstören den Markt oder schwächen die Branche, erreichen wir damit das Gegenteil. Wir haben mit der Sicherheitsverordnung in der Automobilindustrie Weltmarktposition erreicht, eben weil wir sichere Autos gebaut haben und verkaufen konnten. Das bedeutet auch, wenn man die Kompetenzen bündelt und auch hier IT-Technik und IT-Sicherheitstechnik verzahnen würde, könnten wir mehr erreichen. Nur haben wir das Problem, dass wir keine große IT-Technik hier in Deutschland haben.

Eine Automobilindustrie haben wir. Da hat es mit Verkehrssicherheit funktioniert, aber wir haben keine wirkliche europäische, tiefgreifende Kompetenz in der IT. Jetzt werden sich manche angegriffen fühlen, aber wir haben sie schlichtweg nicht mehr in Europa!
Die Innovationen, die neuen Technologien kommen häufig aus Kalifornien. Dort sitzen die großen Unternehmen, die sehr wohl marktbeherrschend sind und uns ihre Produkte verkaufen. Das bedeutet natürlich auch einen Spagat. Wollen wir uns mit denen verzahnen? Warum sollten sie ausgerechnet deutsche Sicherheitstechnologie einsetzen, wenn sie nicht dazu zumindest einmal genötigt werden. Anders können wir uns wohl nicht durchsetzen. Nur aus Überzeugung werden sie unsere Technik freiwillig nicht einsetzen. Dahinter stecken klare nationale Interessen.

Es gibt auch negative Beispiele, sozusagen die „Berliner Flughäfen“ in der IT. Was nicht so gut gelaufen ist, ist z.B. die Gesundheitskarte. Das sei seit 2006 abgeschlossen, wurde mir gesagt.

Wir haben aber auch andere Beispiele, die - von der Sicherheitstechnologie her betrachtet - hervorragend sind, wie der neue Personalausweis. Eigentlich ein Tool, mit dem man richtig etwas machen könnte, aber keiner macht es. Das heißt, eine staatliche Investition in hochwertige Sicherheit ist nicht unbedingt Garant dafür, dass sie auch zur Anwendung kommt. Scheinbar muss man hier Druck ausüben. Darum appelliere ich, dass wir gemeinsam

7.5 Dr. Kim Nguyen, Bundesdruckerei GmbH, Berlin

Noch einen Zusatz zu Herrn Baumgart. Was Sie nicht gesagt haben: als die Gurtpflicht kam, konnte man Pullover kaufen, wo ein Gurt aufgedruckt war. Das zeigt, dass das Thema Regulierung natürlich hilft, aber man sozusagen auch andere Dinge haben kann. Das ist ein Punkt, den ich gern noch einmal in die Diskussion reinbringen möchte. Das eine ist das Thema, was wir an der Förderungsseite, an der Regulierungsseite machen können. Ich glaube aber, dass ein ganz entscheidendes Thema noch einmal das Thema Akzeptanz ist. Ganz banal gesprochen: Wollen Leute das nutzen? Macht es Ihnen Spaß, das zu nutzen? Ist es sozusagen eine Bedrohung es zu nutzen? Wie empfinden das Leute überhaupt?

Ich denke, an der Stelle haben wir alle noch viel Aufholbedarf, denn wir leben alle in diesen regulierten Bereichen, wo die Leute das nutzen müssen. Wir wollen aber eigentlich dahin kommen, dass die Leute es machen. Dass sie es einfach benutzen und als natürlich empfinden. Das ist auch ein bisschen ein Anspruch, der sich in der Digitalen Agenda wiederfindet, wenn man dort liest Verschlüsselungsstandort Standort Nr.1. Das soll jeder machen. Das ist eine Herausforderung, die wir auch sehen müssen. Die hat aber noch einmal eine andere Dimension als das Thema Technik. Ich komme selber aus der Technik und kann dazu immer noch viel erzählen. Es interessiert aber keinen. Es ist ein Geheimnis, was ich erst nach 15 Jahren in dem Bereich irgendwann realisiert habe, dass die elliptischen Kurven super sind, aber keinen interessiert, sondern die Sachen interessieren, die funktionieren.

Er erzähle immer das Beispiel von meinen beiden Söhnen. Die sind 5 und 7 und können mit diesen ganzen Apple Geräten perfekt umgehen, weil das einfach intuitiv geht. Das ist eine Herausforderung, die wir haben, wenn wir aus diesen regulierten Bereichen rauskommen wollen. Wir müssen ein Stückweit diese Akzeptanz schaffen und das Wort Sicherheit durch das Wort Vertrauen ersetzen. Sicherheit ist gut, aber Sicherheit kann keiner messen. Vertrauen ist etwas, was jeder versteht und jeder kann sofort sagen, wem er vertraut. Dahin müssen wir kommen, dass unsere Technologien diesen Vertrauensstatus bekommen und dass die Leute das auch gern nutzen.

Das ist noch ein langer Weg, den wir vor uns haben, trotz oder vielleicht auch gerade wegen der ganzen Exzellenz, die wir haben. Das müssen wir so bündeln, und das wäre für mich noch einmal eine Herausforderung. Da finde ich es ganz schön, dass die EU - nicht alles, was aus Brüssel kommt, muss immer automatisch gleich schlecht sein - in der neuen EU-Verordnungen von Vertrauensdiensteanbietern spricht. Da sind zwei Worte enthalten, die mir wichtig sind: das Thema Vertrauen und das Thema Dienst. Dienst soll heißen, dass es mir etwas bringen soll. Das ist der Anspruch, den wir darstellen müssen. Es muss den Leuten etwas bringen und die müssen es nutzen wollen. So wie die Leute die Pullover dann doch nicht mehr gekauft haben, wo die Gurte aufgedruckt waren, sondern es gemacht haben, weil sie verstanden haben, dass es ihnen etwas bringt.

Wenn wir es schaffen, hinter diese „Kryptopullover“ zu kommen, haben wir einen großen Schritt gemacht.

7.6 Helmut Friedel, certgate GmbH, Nürnberg

Kollege Dr. Nguyen hat den entscheidenden Argumentationsweg eingeschlagen, das Thema Vertrauen. Wir können in die Technik die absolute Sicherheit nicht inhärent einbauen. Wir können schauen, welche Sicherheitsniveaus wir technisch erreichen und wo dann noch irgendwelche Sicherheitslücken sind, die wir auch kontinuierlich überwachen müssen. Wir haben uns erst einmal mit sicheren mobilen IT-Systemen in die Branchen hineinbegeben, wo hohe Sicherheitsanforderungen gestellt werden. Eine Branche ist z.B. die Energietechnik. Dort realisieren wir zusammen mit der Telekom, D-Trust und HP ein Projekt für E.on. Wir haben das Glück, mit der Bundesdruckerei (D-Trust) einen vertrauensvollen Partner zu haben, der das Trust Center darstellt und die Zertifikate für die E.on Mitarbeiter liefert. Wir sorgen dafür, dass die Zertifikate remote über Secure Messaging Verfahren direkt auf die Tokens der ca. 80.000 E.on Mitarbeiter geladen werden, mit denen dann diese sicher auf ihre IT zugreifen können. Wir haben mit diesem Verfahren, eine Technik entwickelt, die dem derzeitigen Sicherheitsstand entspricht. Ein weiteres wichtiges Thema der IT-Sicherheit sind die zum Einsatz kommenden mobilen Geräte. Hier ist im Projekt E.on unser Partner Telekom gefragt. Wir diskutieren aktuell, welche Geräte E.on mit welchem Sicherheitsniveau nutzen kann.

Ein anderes aktuelles Projekt für Mobile IT Sicherheit realisieren wir für die Bundesagentur für Arbeit in Nürnberg. Die IT der 180.000 Mitarbeiter der BA müssen einen hohen Sicherheitsstandard erfüllen, damit die sensiblen Informationen der Bürger / BA-Kunden vertrauensvoll geschützt werden.

Wir arbeiten in diesem Projekt mit der secunet zusammen, die dort das Trust Center betreibt. Wir sorgen dafür, dass in einer ersten Projektphase ca. 6.000 Zertifikate mit Schlüsseln in die mobilen Devices (Blackberry) von BA Mitarbeitern mittels unserer microSD Karten implementiert werden.

Die genannten Sicherheitstechnologien wollen wir in Kooperation mit D-Trust künftig auch kleineren Unternehmen ohne eigene PKI Infrastruktur zugänglich machen. Dabei liefert D-Trust als vertrauenswürdige Instanz die digitalen Identitäten, die anstelle von leicht manipulierbaren (Password-) Verfahren zum Einsatz kommen. Wir liefern die HW-Token in Formfaktoren, die es ermöglichen, diese digitalen Identitäten sicher zu speichern und flexibel und einfach zu nutzen.

Zwei Stichworte sind hier relevant: Vertrauen schaffen und dem Kunden klar machen, welches Sicherheitsniveau für „seine IT- Lösung“ erreichbar ist und wo die Lücken sind, die offensiv überwacht werden müssen. Da gehe ich konform mit dem, was Kollege Christoph Peylo gesagt hat: wir nutzen Technologien, wo wir ganz bewusst untersuchen, wo die Schwächen sind und die von Kollegen realisiert werden, die hoffentlich mindestens so clever sind wie die, die angreifen und die dann auch rechtzeitig erkennen, wo ein Angriff stattfindet, um dem Angriff rechtzeitig zu begegnen / stoppen.

7.7 Ammar Alkassar, Sirrix AG, Saarbrücken:

Ich versuche auch die Dinge anzusprechen, die noch nicht angesprochen worden sind. Vielleicht noch zwei Dinge im Sinne dessen, was Rainer Baumgart gesagt hat, das Ganze auch einmal positiv zu sehen. Der IT-Sicherheitsmarkt wird größer und international, auch hier bei uns in Deutschland. Das bedeutet, dass wir uns eigentlich alle freuen müssten. Es gibt mehr zu tun und es gibt auch mehr zu verteilen.
Aber trotzdem, wenn wir uns unseren Heimatmarkt anschauen, sind wir nicht wirklich gut. Wir haben es ein paar Mal gehört. Im regulierten Bereich haben wir naturgemäß eine Position gefunden, die ein stückweit vorgegeben worden ist. In den anderen Bereichen, die nicht reguliert sind, tun wir uns aber sehr schwer. Obwohl wir eigentlich sehr gute Technologien haben, bei denen wir deutlich weiter sind als viele andere in dieser Welt. Das kommt so ein bisschen auch aus unserer Kultur, aus der Affinität für Datenschutz, Affinität für Sicherheit. Aber trotzdem haben wir es nicht geschafft, diese Technologien wirklich bei uns schon dazu zu nutzen, um den Heimatmarkt zu gewinnen, geschweige denn zu exportieren.
Es gibt ein paar positive Beispiele. Wenn ich mir die Firma Ultimaco anschaue, so hat die sehr früh eine Festplattenverschlüsselung entwickelt, als viele andere noch nicht daran gedacht haben, auch in den USA nicht. Als der Boom gekommen ist, waren sie zur rechten Zeit da, hatten bereits ein Produkt und sind damit auch sehr schnell groß geworden. Dummerweise – das ist ein ganz anderes Problem -, ist die Firma dann verkauft worden ins Ausland. Ich denke, das ist in jedem Fall etwas, womit man sich auch beschäftigen muss. Aber das ist ein orthogonales Problem.
Die Frage ist, woran es liegt und was wir tun müssen, um das aufzugreifen? Ich möchte drei Punkte aufgreifen, die man sich dazu noch einmal anschauen sollte. Ich glaube auch, dass es nicht nur einen Lösungsweg gibt, sondern dass es verschiedene Akteure gibt und dass es am Ende alle Akteure ein Stück dieser Verantwortung auch selbst übernehmen müssen. Bei einem Punkt – und das betrifft auch die Regulierung – müssen wir ein bisschen selbstkritisch sein. Das eine Positive ist, dass man durch die Regulierung auch viele gefördert hat, indem man den Markt abgeschottet hat. Allerdings vielleicht auch an der einen oder anderen Stelle zu viel abgeschottet und wenig Wettbewerb zugelassen hat in der Regulierung aus einem positiven Hintergrund heraus, dass man sagte, man will nicht zu viel Regulierung in diesem Bereich zulassen, weil möglicherweise dann keiner überlebt. Das hat dazu geführt, dass in vielen Bereichen einfach die Technologien nach hinten zurückgefallen sind. Wo wenig Wettbewerb ist, entwickeln sich auch weniger marktgängige Produkte.
Das fällt in die Verantwortung des Regulierers. Die Verantwortung der Firmen selbst ist die Technik - auch das haben wir eben gehört. Ich glaube, wir haben als Hersteller zu viel aus unserem Ingenieursdrang entwickelt, Konzepte auf den Weg gebracht, die wir ganz toll fanden, die aber möglicherweise der Markt nicht brauchte, nicht bereit war, dafür zu bezahlen, also zu wenig wirklich die Produkte marktgängig entwickelt. Und das ist ein prinzipieller Ansatz, wie man das angeht.
Wir haben vor ein paar Tagen noch einmal darüber diskutiert, warum es ein Apple so gut schafft. Das ist auch etwas, was möglicherweise nicht direkt vom Markt gekommen ist, sondern vorgegeben worden ist von jemandem, der gesagt hat, dass das das Richtige ist und dass man das jetzt kaufen muss. Das hat da funktioniert, weil sozusagen das, was er vorgegeben hat, letztendlich auch wirklich marktgängig ist und dem Ingenieursdenken entsprungen ist.
Der dritte Punkt ist ein ganz wichtiger Punkt. Ich glaube, der Anwender ist ganz massiv gefragt. Wenn wir uns anschauen was in der Wirtschaft tatsächlich verwendet wird, müssen wir jetzt feststellen, dass wir viele Unternehmen haben, die im Wesentlichen nicht deutsche Produkte einsetzen. Wenn ich sehe, was bei Siemens verwendet wird, an Verschlüsselungspro-

dukten, an Gateways, an End Prosecuting Lösungen, so sind es die Standards, die man überall kauft.
Viele machen sich das auch etwas einfach und gehen in Standardlisten, die beschafft werden, Gardener Listen. Da haben wir sicherlich deutlich größere Nachteile, wenn beispielsweise auf eine Gardner Liste, die den Verkäufen in den USA zugrunde liegt, zu kommen. Damit haben wir substanzielle Nachteile. Ich glaube, dass das auch etwas ist, wo die Anwender über ihren Schatten springen und ein bisschen Aufwand investieren müssen, um Beschaffungsstandards festzulegen, die vielleicht außerhalb dieses Normalen „wir nehmen die Listen und haken die ab“ liegt.
Am Ende macht es Sinn, wenn sich alle drei Akteure zusammensetzen und gemeinsam überlegen, wie sie diese Dinge nach vorne bringen können. Eine Möglichkeit wäre, ganz konkret über Mindeststandards zu sprechen, nicht nur in diesem regulierten Bereich. Die müssen auch nicht vorgegeben, sondern als Empfehlungen herausgegeben werden, in denen auch die Branchen selbst branchenspezifisch sagen, dass das etwas ist, worauf sie sich einlassen können, dass das etwas ist, was die deutsche Sicherheitsindustrie aufgreifen kann und entsprechend dann auch zur Umsetzung bringt.

8 Anforderungen an die IT-Sicherheitswirtschaft aus Sicht der Bedarfsträger

Robert Woithe, Toll Collect GmbH, Berlin

In meinem realen Leben verdiene ich mein Geld als Technikchef von der Toll Collect am Potsdamer Platz. Das ist das pressebeliebte kleine Maut Unternehmen für die LKW-Maut in Deutschland, verantwortlich für ca.4 Mrd. Mauteinnahmen des deutschen Staates jedes Jahr. Das entspricht ca. 1% des Bundeshaushaltes. Das leisten wir als ein mittelständisches Unternehmen.

Ich freue mich hier aber in meiner Rolle als Vertreter von Voice auftreten zu dürfen. Ich hatte Ihnen die E-Books mitgeschickt, weil ich mich mit den Folien zurückhalten sollte. Voice ist ein Zusammenschluss aus den verschiedenen CIO Initiativen. Wir haben 400 IT Entscheider bei uns. Wir haben einen Verein gründen, weil bei bestimmten Tätigkeiten des Vereins, bei denen wir keine Unterstützung aus der herstellenden Industrie bekommen, einfach selbst die Initiative ergriffen haben und dazu muss man abrechnungstechnisch korrekt arbeiten.
Ansonsten sind wir ein gemeinnütziger Verein, eigentlich eine Interessensgemeinschaft der IT-Anwender und -Entscheider, die sich ein bisschen besser organisieren wollen, weil wir die Leidtragenden in unseren Unternehmen sind, die IT- Produkte kaufen und einsetzen müssen.

Die IT-Anwender kaufen „gern“ bei den Top 10 der Gardener-Listen. Ich kaufe mit Vorliebe bei Oracle. Ich bezahle mit Vorliebe seit den letzten fünf Jahren 30% Budgetkostensteigerung bei den Wartungskosten. Warum muss ich das machen? Es ist nichts anderes da. Es gibt Oracle oder IBM als Marktführer bei den Datenbankherstellern. Das können wir gern diskutieren. Bei Voice bedanke ich mich, dass wir als Anwender in der herstellenden Industrie eine Plattform geschaffen haben, um uns als Anwender Gehör zu verschaffen.

Ich habe heute gehört, dass die Anwender mehr investieren müssen für einen Mehrwert, den ich noch nicht verstanden habe. Der Staat soll regulieren. Der Staat soll also die Anwender zwingen, mehr zu investieren. Ich habe irgendwann einmal eine Marketingschule besucht, wo ich etwas über Angebot und Nachfrage gehört habe. Also nehmen wir mal das Beispiel Apple. Da wird ein Markt kreiert. Das war kreativ, userfreundlich und leicht zu bedienen.

Übrigens kann ich meine Firewall auch zuhause besser konfigurieren als die Firewall in der Firma. Warum habe ich die schlechtere Bedienbarkeit in der Firma, obwohl hier eigentlich mehr „Musik“ spielt? Es ist nichts anderes da für Business Anwendungen, was wir IT-Anwender zum Einsatz bringen können.

Die Argumentation von vorhin war, dass wir nach der ‚who is who‘ Liste von Gardener IT einkaufen. Was kann ich denn als IT-Anwender als Komplettlösungen für heutige Herausforderungen vom Markt beziehen? Wir haben hier tolle Technologien vorgestellt bekommen. Mich als Techniker, ich bin studierter Informatiker, macht Kernel Programmierung happy. Das ist das Thema proprietäre Entwicklung und Investition. Ich bin in der Anwendungsbranche, ich bin unter Kostendruck. Ich bin in den Investitionsentscheidungen meines Unternehmens angebunden und verantwortlich. Früher war die IT ein bisschen Mainframe, ein bisschen Rechenzentrum, ein paar Terminals. Das war doch super. Mainframe Zeit war das Beste. Das war hoch sicher. Es kam ja keiner ran. Das ist aber vorbei. Ich muss mich mit den Anforderungen der Digital Natives auseinandersetzen.
„IT-Sicherheit… geh doch weg! Es schränkt doch nur ein. Alles, was ich von IT-Sicherheit halte: Ich verliere Komfort. Ich verliere Usability. Du bist zu langsam und du bist teuer.“ Das ist

das, womit ich mich als IT-Verantwortlicher auseinandersetzen darf. Das sind die Konfliktfelder, in denen wir uns bewegen. Natürlich würde ich die heute gezeigte Technologie gerne einkaufen. Aber ich kaufe keine Technologie. Ich kaufe Funktionalitäten und Gesamtlösungen.

Warum haben Sie keinen Snowden-Effekt in der deutsche Industrie für Ihre Produkte gehabt? Glauben Sie allen Ernstes, dass die IT-Manager in der deutschen Industrie darauf gewartet haben, dass Snowden irgendwo Daten klaut, dass die Anwender, welche sich schon seit Jahren darüber beschweren und meckern, dass z.B. die Firewalls zu kompliziert sind, dass es keine einheitliche Lösung gibt? Alle Angebote sind „Add ons" und müssen gewartet und gepflegt werden.

Die Kollegen vom BSI haben zu Recht herausgebracht, dass größer 2.000 Bitverschlüsselung derzeit empfohlen wird. Die 1000 ist zu knacken. Das stimmt, Rechnerpower ist hoch gegangen. Jetzt kaufen Sie einmal ein leicht zu integrierbares Pin Pad, ohne dass sich das zu einem Riesenprojekt entwickelt. Das funktioniert heute so nicht. Plug and Play funktioniert in der IT-Sicherheit bei Business Anwendungen nicht.

Der Ruf nach Regulierung: Sie haben doch auch Finanzdienstleister. Hat jemand mal von SEPA gehört? Die Umstellung europäischer Markt, europäisches Lastschriftverfahren. Seit 1.1.2014 soll SEPA europaweit laufen. Die Deutschen immer ganz vorne weg. Wieviel Länder sind denn SEPA fähig, Stand heute? Wo kann ich mit dem, was ich für viel Geld gekauft habe, einen kommerziellen Nutzen für das Unternehmen einfahren? Vereinheitlichtes Lastschriftverfahren: Ich habe auch eine SAP-Anwendung, übrigens ein deutsches Unternehmen. Glücklicherweise habe ich dieses Projekt allein gesteuert und bin pünktlich SEPA ready gewesen. Das Projektvolumen war 3 Mio., nur weil die Finanzdienstleister ihre Lastschriftverfahren geändert haben. Es soll jetzt sicherer und einheitlich sein, europaweit. Der Mehrwert derzeit für mich als Industrie ist Null.

Auf einem bestehenden elektronischen Cashflow mal einfach 3 Mio. verbraten, um weiterhin dieselbe Funktionalität zu haben, die ich bisher hatte. Das finde ich super. Das macht mich total happy als IT-Chef. Ich bin nicht der klassische IT-Chef. Ich polarisiere mal ein bisschen! Beispiel EC-Karten – in den letzten zwei Jahren habe ich vier große IT-Projekte durchziehen müssen für Terminalupdates zur Akzeptanz von EC-Karten. Ich kaufe die Pin Pads eigentlich als Produkt und ärgere mich dann über unausgereifte fehlerbehaftete Updates. Ändert sich etwas an meinen Businessanwendungen? Nein, aber trotzdem muss die ganze Prozesskette durchgetestet werden. M2M von der IT verantwortet. Und wenn die Transaktion nicht klappt - wen hängen sie auf? Nicht den, der dieses Produkt nicht in den Griff gekriegt hat, sondern den, der darüber das Geld nicht mehr abrechnen kann. Das bin ich als Anwender. Jetzt habe ich EC-Karten abgeschafft. Warum? Es lohnt sich nicht.

Das dritte Projekt, was wir neben SEPA und den Terminals für das Finanzministerium hatten, war die Einführung neuer Geldscheine. Ich habe letztes Jahr einen neuen Zehner gehabt und einen neuen Fünfer als Projekt durchgezogen. Der Fünfer war die Katastrophe. Ich habe Bankautomaten im Einsatz. Es kann doch nicht so schwer sein, dass ein Hersteller, der sagt, dass er einen Bankautomaten verkauft, auch in der Lage ist, neue Geldscheine an seinem Automaten zu akzeptieren! Es kann doch nicht so schwer sein, dass Produkte der Hersteller einfach zu installieren und zu warten sind, ohne das die Anwender der IT dafür jedes Mal große Firmenprojekte fahren müssen um danach die Funktionalität wie vorher zu bewahren. Das bedeutet, der Wunsch der deutschen IT-Sicherheitswirtschaft nach Unterstützung durch Regulierung wird von den IT-Anwender sicher nicht vorbehaltslos geteilt.

Ich möchte einmal die Apple Gemeinde sehen. IOS 8.0, da schrien einige. Das Beispiel hinkt ein bisschen. Aber dann hört man wenigstens das Schreien, sieht den Schmerz der IT-Anwender an sinkenden Umsatz-Zahlen der Hersteller und es wird etwas getan. Es ging sofort zurück und es gab ein Entschuldigungsschreiben. Aber wenn Sie ein normales IOS-Update 8.x.x haben, funktionieren alle Applikationen. Und da kommt nicht die Meldung: Lieber Anwender, bitte, wenn du dieses IOS-Update hast, teste das und jenes und gib uns Feedback und sage uns Bescheid, welche Einschränkungen Du hast, weil ich es dann individuell anpassen muss und es extra kostet.

So fühlt sich der deutsche IT-Anwender. Der kauft nicht gern ein bei IBM. Der kauft nicht gern ein bei Oracle. Wer hätte nicht gern deutsche Produkte. Wie hieß die letzte deutsche Datenbank, die ich kaufen konnte? Informix hatte ich bei mir auf der Platte. War beim letzten Kunden. Wo ist die Datenbank jetzt?

Ich rede nicht immer über Snowden, weil 80 bis 90% meiner Arbeit normales Datenmanagement ist. Personen bezogene Daten, gesetzlich reguliert, muss ich löschen. Wie lange darf ich sie aufheben? Sie haben bestimmt alle Personen bezogene Daten. Haben Sie eine automatische Löschroutine in Ihren Produkten? Nein! Jeder setzt sich hin, bestellt einen Consultant, macht ein Fachkonzept und überlegt, wie er das jetzt in seiner personenbezogenen Datenbank nachhaltig löschen kann. Das ist übrigens gesetzliche Vorgabe, Regulierung. Hat das irgendwie dazu geführt, dass sich einer hingesetzt hat und sich Gedanken macht über Löschkonzepte, die nach deutschem Gesetz jeder haben müsste? Nein. Das macht jeder für sich. Es ist nicht so, dass das Geld nicht da ist. Wenn ich so sehe: 0,1% Anteil der deutschen IT-Sicherheitswirtschaft am Sicherheitsbudget deutscher Unternehmen. Ich kenne mein IT-Budget. Das ist wesentlich mehr, was ich für Sicherheit ausgebe. Das geht schon eher auf zweistellige Prozentzahlen, deutsche Unternehmen sind da kaum auf der Lieferantenliste.

Die Frage ist: Was können Sie mir verkaufen? Technologie verkaufen Sie mir nicht. Schöne Lösungspflaster verkaufen Sie mir auch nicht. Ich brauche eine ganzheitliche Lösung, welche mich in meinen Businessprozessen unterstützt und nicht behindert. Das ist nicht so ganz einfach, und wir stehen alle im Wettbewerb. Auf der einen Seite User, auf der anderen Seite bin ich Anbieter. Und ich muss meinen Fachbereichskollegen als neuer moderner IT-Chef Dienstleistungen anbieten. Die finden das gar nicht Klasse, wenn sie Apple Funktionen alle gesperrt bekommen, weil diese nicht sicher sind.

Und was kaufe ich noch? Da bin ich bei Ihnen. Ich kaufe Vertrauen. Wenn ich Investitionsentscheidungen tätige, dann sind die jetzt nicht mehr, dass ich ein bisschen Hardware und Software kaufe, sondern dann investiere ich in einen IT-gestützten Geschäftsprozess. Das ist das, wie ich denke. Das ist das, wie ich arbeite. Sie verkaufen mir keine Technologien, sondern Sie müssen mir verkaufen, wie Sie meinen IT-Prozess sicher unterstützen. Was kostet mich das? Die Anfangskosten sind mir nicht ganz egal, aber viel schlimmer sind die laufenden Betriebskosten und die Wechselkosten. Und so lange Sie diese Sprache mit mir nicht sprechen, werden wir sehr schwer ins Gespräch kommen.

Das ist jetzt für Voice: Ich habe das mit den Kollegen abgestimmt. Wie gesagt 400 IT-Entscheider und 250 Fachanwender, d.h. davon sind ca.50 Security Leute. Warum hat man mich heute hergeschickt? Wir haben im Voice eine Cyber Security AG gegründet, wo wir uns untereinander helfen. Die Mittelständler kennen ihre Problemfelder mit der IT-Sicherheit genauso, wie große DAX Unternehmen. Wir haben alle dieselben Probleme, nur die Anzahl der Nullen vor dem Komma unterscheiden sich vom Dax-Unternehmen zum Mittelstand. Und wer nicht einfach einmal 1 Mio. für eine Studie einsetzen kann oder 100.000 € für einen Consultant,

denn das ist für ihn teilweise ein Monatsbudget, muss sich trotzdem mit den gleichen Problemen auseinandersetzen. Das muss man mit unterschiedlichen Diskussionsebenen angehen.

Ich hoffe, ich habe damit für ein bisschen Auflockerung gesorgt.

9 Sicht von Investoren mit Fokus auf Safety & Security

Dr. Oliver Melzer, AMMER PARTNERS GmbH, Hamburg

Mit AMMER PARTNERS konzentrieren wir uns bereits seit einiger Zeit auf Investitionen im Sektor Safety & Security inklusive IT-Security. Wir haben insofern in diesem Sektorumfeld und darüber hinaus über viele Jahre Erfahrungen gesammelt, sowohl in der Unterstützung und Begleitung von kleinen Unternehmen bis hin zu mittelständischen und größeren Beteiligungen.

Ich möchte Ihnen in den nächsten Minuten erläutern, warum es für einen Investor auf der einen Seite sehr interessant, aber auf der anderen Seite auch schwierig ist, in diesem Sektor aktiv zu sein und auf welche Spezifika man sich als Investor einstellen muss.

Die Zahlen wurden genannt: Interessante Wachstumsraten und -potenziale sind gegeben. Für einen Investor ist es darüber hinaus von Bedeutung, ob es weitere Einflüsse oder Trends gibt, die auch in fünf Jahren noch dieses Wachstum widerspiegeln. Auch dazu ist festzustellen, dass sehr viele Trends sich positiv auf den IT Security Sektor auswirken oder auswirken werden (wie von Vorrednern dargestellt z.B. Smart Metering, Cyber Security Themen, Internet of Things, wachsende vernetzte Infrastrukturen, etc.). So betrachtet ist der Sektor also für Investoren durchaus interessant.

Allerdings hat der Sektor einige Spezifika, die es für einen Investor in der Evaluation schwierig machen bzw. auf die man sich als Investor besonders einstellen muss. Hierzu einige Beobachtungen:

- Wie wir soeben gehört haben, ist das Unternehmen des Vorredners mit 300 Mitarbeitern bereits Marktführer. Dies spiegelt wider, dass der Sektor sehr fragmentiert und sehr mittelständisch geprägt ist. Gerade in den kleineren mittelständischen Unternehmen findet man in der Regel nur wenige Organisationsstrukturen bzw. einen Zuschnitt nur auf Einzelpersonen. Damit einhergehend fehlen manche Reportingsysteme, –prozesse und auch Transparenz, was eine Betrachtung für einen externen Investor erschwert.
- Es sind fast alle Unternehmen des Sektors technologisch und sehr oft Software oder Hardware getrieben. Dies ist für einen Investor besonders schwierig einzuordnen, weil die Produkte eine „Black Box“ sind, die ein hohes technisches Verständnis bedürfen. Bei AMMER PARTNERS haben wir durchaus weitreichende technische Expertise im Team, doch andere Investoren kommen in der Regel aus dem Finanzbereich und haben es schwer, sich in den Markt und das Unternehmen hineinzudenken.
- Hinzu kommt die Beobachtung, dass viele Unternehmen sich in einzelnen Nischen bewegen. Die typische Reaktion eines Investors darauf ist, zunächst auf sogenannte Leuchtturmkunden zu schauen. Wenn wir von einem Unternehmer hören (wie vom Vorredner beschrieben): “In Deutschland haben wir unser Produkt(e) noch nicht verkaufen können“, fehlt uns als Investor auch diese Grundlage zur Entscheidung. D.h. Leuchtturmkunden sind nicht nur für die Binnenwirtschaft wichtig, sondern auch für Investoren eines der wichtigsten Entscheidungskriterien.
- Wenn sich eine Unternehmung zudem auf ein einzelnes Produkt konzentriert („One-Product-Company“), dann ist das Risikoprofil noch intensiver zu analysieren. Kann das Unternehmen überhaupt nachhaltig den Wettbewerbsvorsprung (gegen den globalen Wettbewerb) halten und welche R&D Aufwendungen sind nötig, um im schnellen technologischen Wandel überhaupt Schritthalten zu können.

- Eine weitere Besonderheit liegt in den oft unterschiedlichen IT-Security Anforderungen der Kunden begründet: Sehr häufig sind die Unternehmen mehr im Projektgeschäft als im reinen Produktgeschäft involviert. Damit unterliegen sie naturgemäß stärkeren Auftragsschwankungen und Abgrenzungsfragen von Umsätzen und müssen in Organisationsstrukturen „atmen“ können. Dies ist für einen Investor schwieriger zu bewerten und einzuschätzen. Darüber hinaus kann es ein Zeichen sein, dass die Skalierbarkeit der Produkte ggf. eingeschränkt ist.
- Die Skalierbarkeit und vertrieblichen Herausforderungen scheinen – auch entlang der Vorredner – „sektorimmanent“ zu sein. IT-Security ist für Kunden in der Regel zunächst nur eine zusätzliche Kostenposition und der Mehrwert der Produkte muss oft „detailliert-technisch“ dargestellt werden. Dies bedeutet, dass die Vertriebsteams sehr technologisch aufgestellt sein müssen. Auch unterliegt ein B2B-orientierter Vertrieb anderen Gesetzmäßigkeiten als hochskalierbare virale B2C-Geschäftsmodelle und die Unternehmen bewegen sich in einem kleinen Binnenmarkt unter dem Druck eines großen globalen Wettbewerbs

An dieser Stelle von meiner Seite ein paar Gedanken zu der geführten Diskussion, warum es Venture Capital Investitionen in diesem Sektor so schwer haben. Ausgangspunkt für einen Venture Capital Investor ist die Portfolio-Faustregel, die sich für Venture Capital Fonds seit den 90er Jahren immer wieder bestätigt: In einem Beteiligungsportfolio sind nur ca. 10%-20% der investierten Unternehmen außerordentlich erfolgreich und erlösen die wesentliche Rendite eines Fonds.

Daraus ergibt sich folgende (etwas polarisierend und vereinfacht dargestellte) Rechnung: Ein Risikokapitalinvestor erwartet zum Beispiel 20% Rendite. Dies bedeutet nach fünf Jahren die Rückzahlung des zweieinhalbfachen eines jeden investierten Euros.

Zusammen mit der Venture Capital Faustregel heißt dies für den Fond, bereits bei der Investitionsentscheidung abzuwägen, ob das Unternehmen derart wachsen kann, so dass es in 5 Jahren die Werthaltigkeit auf das 25fache des eingezahlten Betrags steigern kann.
Daraus ergeben sich strenge Rahmenbedingungen an die Management-Teams und die Geschäftsmodelle, ob solch hohe Wachstumsanforderungen erfüllbar sein können und die im IT-Security Umfeld nur sehr schwer nachhaltig bewerkstelligt werden können (siehe Rahmenbedingungen oben).

Aus diesen Gründen haben wir uns mit AMMER PARTNERS über die Jahre stärker auf mittelständische Beteiligungen im Sektor Safety und Security konzentriert, was wir in den kommenden Jahren weiter ausbauen. Dabei verfolgen wir eine langfristig orientierte Industrie Holding Struktur. Mit den mittelständischen Beteiligungen sehen wir die Möglichkeit, viel konsequenter, schneller und marktnäher Produktinnovationen oder Technologien für den Markt katalysieren zu können – besser als über Startups mit Einzeltechnologierisiken. Damit bekommt man auch den direkten Schulterschluss zwischen Bedarfsträgern und Kunden und hat zudem auch die direkte unternehmerische Begleitung von Fördervorhaben abgedeckt, die meines Erachtens in der Vergangenheit viel zu wenig berücksichtigt wurde.

Diese Gedanken bilden zu den anderen Rednern sicherlich nochmals einen komplementären Blick auf die IT-Sicherheitswirtschaft. Bei weiterem Gesprächsbedarf oder bei Interesse an einer Mitwirkung, Einbringung in eine Security Industrie Holding können Sie sich sehr gerne bei uns melden.

10 Diskussion

Moderatoren: Ramon Mörl, itWatch GmbH, München
Christian Köhler, IABG mbH, Berlin

Teilnehmer:
Prof. Dr. Norbert Pohlmann, if(is)/TeleTrusT e.V., Gelsenkirchen/Berlin
Dr. Gerhard Schabhüser, Bundesamt für Sicherheit in der Informationstechnik, Bonn
Peter Möhring, Giesecke & Devrient GmbH, München
Eva Wiesmüller, Power2Progress, München

Herr Köhler:
Ich schlage vor, dass wir mit den Impulsvorträgen beginnen, zuerst mit Frau Wiesmüller. Frau Wiesmüller ist Unternehmerin mit langjähriger Erfahrung, nicht nur in Geschäftsmodellen, wie wir das Thema gerade hatten, und im Management sondern vor allen Dingen auch in sicherheitsrelevanten Themen, EID, Identifikation u. ä. Insofern freuen wir uns erst einmal auf Ihren Input, Frau Wiesmüller.

Frau Wiesmüller:
Vielen Dank, Herr Köhler, für meine Vorstellung. Ich freue mich sehr, heute Abend hier bei Ihnen sein zu dürfen und mit Ihnen über das Thema „Stärkung der IT-Sicherheitswirtschaft“ zu sprechen.
Vielen Dank auch an Prof. Heinz Thielmann für die Einladung, die ich sehr gerne angenommen habe. Wir haben bereits sehr spannende Vorträge heute gehört und ich schließe mich meinen Vorrednern an. Die allermeisten Punkte sind somit bereits angesprochen worden. Aber ich möchte sie trotzdem zum Teil noch einmal wiederholen.
Wie Herr Köhler mich bereits vorgestellt hat, bin ich selbst keine IT-Sicherheitsexpertin. Mein Blickwinkel liegt darin, wo Wachstumsmärkte sind und wie man diese Märkte erschließt. Wie stärkt man Unternehmen darin, in diese Wachstumsmärkte reinzukommen? Wie findet man stabiles Geschäft, wie generiert man Geschäft und wie stabilisiert man dieses Geschäft?
Wir haben heute schon sehr viel über die IT-Sicherheitswirtschaft gehört. Ich möchte das in drei, vier Punkten nochmals zusammenfassen. Erstens, es handelt sich größtenteils um kleine Unternehmen. Zweitens, deshalb sind es meist auch Unternehmen mit manchmal sehr wenig Mitarbeitern. Junge Unternehmen und Unternehmen, die einen sehr engen Fokus in ihrem Produkt- und Leistungsportfolio haben. Auch Unternehmen, die zum Teil eine sehr knappe finanzielle Ausstattung mitbringen.
Der eine oder andere hier im Raum wird sich schon angesprochen fühlen, wenn er diese Punkte hier hört. Ich tue es auch. Ich habe viele Jahre – bis vor kurzem - in der Geschäftsleitung mittelständischer Unternehmen gearbeitet. Ich kenne die Herausforderungen. Beginnen wir damit, wenn die Finanzdecke knapp ist. Das bedeutet dann auch, dass man unter diesen finanziell angespannten Bedingungen nicht ganz einfach an gutes Personal kommt für Entwicklung und für Innovationsforschung. Es geht weiter damit, dass große Ausschreibungen und Unternehmensanfragen häufig ein sehr umfängliches Leistungs- und Lösungsportfolio abverlangen und voraussetzen. Das kann man als kleines Unternehmen zum Teil nicht mehr darstellen, weil die eigene Produkt und Lösungspalette eher eingeschränkt ist. Große – vor allem öffentliche – Ausschreibugen verlaufen zudem nach Regularien, die kleine Unternehmen häufig nicht mehr abbilden können Sei es die Anzahl der geforderten Mitarbeiter, seien es Backup Strukturen und eben auch wieder die geforderte Kapitalausstattung bzw. Kapitalsicherheit, die fehlt.

In den letzten Jahren sind viele gute Produkte auf den Markt gebracht worden, aber der Markt war kein sehr dankbarer Abnehmer. Das bedeutet, dass sich die entwickelten Produkte zum Teil nicht wirklich amortisieren konnten. Ich glaube, Sie alle kennen dieses Problem.
Zusätzlich kommt hinzu, dass die Innovationsgeschwindigkeiten immer kürzer werden und sich dadurch die Time to Market deutlich reduziert. Kleine Unternehmen und vor allem die Unternehmer, die hinter diesen Unternehmen stecken, haben große Probleme, um dieses dadurch entstehende unternehmerische Risiko abzufedern.
Was ist die Lösung des Ganzen? Ich möchte heute dafür motivieren, gemeinsam die Kräfte zu bündeln und über Verbundstrukturen nachzudenken. Verbundstrukturen begegnen uns im beruflichen Alltag bereits sehr häufig. Wir sind heute hier eingeladen - wenn man es so will - von einem Verbund, von einem Verein. Viele von Ihnen sind auch Mitglieder in Netzwerken, in Clustern.
Wir kennen also alle die Vorteile dieser Verbundstrukturen. Wir tauschen Informationen über die Netzwerke. Wir arbeiten zusammen an Standards. Wir ziehen viele Vorteile durch aktives Netzwerken daraus. Aber wir müssen auch die Grenzen solcher Verbundstrukturen erkennen. Die sind dann zu finden, wenn es darum geht, Geschäft zu generieren, das unternehmerische Risiko abzufedern, Kosten zu minimieren. Das können Netzwerke oder Cluster größtenteils nicht.
Ich möchte deshalb anregen, über organisatorisch verbindlichere Verbundstrukturen wie beispielsweise der Holding nachzudenken. Der letzte Vortrag von AMMER PARTNERS hat diesen Punkt bereits gestreift. Was wäre, wenn sich kleine Unternehmen zusammenschließen in einer Holdingstruktur? Sicherlich für den Unternehmer oder Gründer eines Unternehmens, der sich seit Jahren darum bemüht und einsetzt, sein Unternehmen am Markt erfolgreich zu positionieren zunächst ein abwegiger Gedanke – ja fast ein „no-go“.
Sehr viele kleine Unternehmen sind ja auch erfolgreich am Markt unterwegs, aber die Frage ist nicht, wie erfolgreich ich bin, sondern wie erfolgreich wir alle werden können. Das hängt auch davon ab, welche Möglichkeiten ich habe und mit welcher Kapitaldecke ich ausgestattet bin. Um attraktiv zu werden für Kapitalgeber, ist es zudem notwendig und wichtig, ein größeres Leistungsportfolio vorzuweisen, verlässlich zu sein und eine Planungsgrundlage aufzuweisen, wo die Zukunft des Unternehmens hingeht. Viele kleinere Unternehmen kommen heute nicht mehr erfolgreich über diese Schwelle hinweg.
Deswegen stelle ich an Sie hier alle eine Frage: Einige von Ihnen kennen sich untereinander. Sie haben größtenteils schon zusammen Geschäfte gemacht. Sie stehen aber auch im Wettbewerb zueinander. Was wäre, wenn einige Unternehmen – Sie hier - sich in einer Holdingstruktur zusammenschließen würden, eine gemeinsame Wertschöpfungskette aufbauen? Wir haben es gehört, Single-Product Unternehmen ist einfach nicht genug. Was ist, wenn man sich ansieht, was man zusammen tun kann.
Kapitalgeber sind sicherlich wesentlich interessierter daran, einen Unternehmensverbund zu fördern, was letztlich allen Beteiligten zugutekommen würde.
Viele von Ihnen werden sich dann vielleicht fragen, ob sie dann ihre Eigenständigkeit aufgeben müssen. Das Image des im Schweiße ihres Angesichts gegründeten Unternehmens versinkt vielleicht zugunsten einer Struktur? Man kann nicht mehr alle unternehmerischen Entscheidungen allein treffen?
Sie haben Recht. Das ist dann manchmal wirklich so. Aber der Gewinn, den man durch eine solche Struktur für sich selbst und das gesamte Unternehmen erzeugen kann, ist weitaus größer. Denken Sie an Synergie-Effekte, die man in einer solchen Zusammenarbeit haben kann. Es könnten ganze Bereiche aufeinander fokussiert werden. Man könnte zum Beispiel über eine Vertriebsholding nachdenken. Die Unternehmen können aber trotzdem am Markt auch weitestgehend selbstständig agieren. Aber man kann eben die Kräfte fokussieren für gewisse zentrale Dienste, sein es Controlling, Buchhaltung oder Marketing. Es gibt sehr viele Redundanzen in der Industrie und es gibt viele Unternehmen, die sich sehr ähnlich sind.

Deshalb möchte ich heute mit Ihnen konkret darüber sprechen, ob Holdingstrukturen eine Möglichkeit sind kleine Unternehmen der IT-Sicherheitsbranche zu mehr Wachstum zu bringen. Denn Unternehmenswachstum bedeutet wiederum die Stärkung dieses Wirtschaftszweigs.

Herr Köhler:
Frau Wiesmüller, vielen Dank. Wir haben die Aufgabe, erst einmal die Statements durchzugehen. Wahrscheinlich hat jedes sehr viel Feuer und Input, um direkt darüber zu diskutieren. Wir gehen trotzdem in der Agenda so vor. Wir haben nachher noch die Chance, darüber zu reden. Mir fällt sofort ein, dass auch genossenschaftliche Modelle schon einmal in den Raum geworfen worden sind. Wenn ich mir unsere Aktivitäten im Masterplan anschaue, habe ich auch immer im Kopf, wieviel Netzwerke und Aktivitäten es gibt. Ich glaube, bei vielen, und das betrifft auch die Verbandsarbeit, heißt es, am Ende muss jeder ein bisschen die Angst bewältigen etwas zu verlieren, denn unsere vielen kleinteiligen Arbeiten sind manchmal ein stückweit durch die Angst getrieben, etwas zu verpassen. Ich weiß jetzt keine Antwort darauf. Das diskutieren wir gleich.
Herr Prof. Pohlmann, man muss ihn wohl kaum vorstellen, ist Direktor im if(is) in Gelsenkirchen und auch an der Hochschule tätig, seit Jahren in den verschiedensten Gremien unterwegs, u.a. ist er Vorsitzender vom TeleTrusT.

Prof. Pohlmann:
Es ist mir ein Bedürfnis hier zusammenzufassen, was ich heute gelernt habe: Wenn man überlegt, haben wir alle gemeinsam die Idee, dass das IT-Sicherheitsniveau nicht angemessen genug ist. Das ist ein erster Konsens gewesen. Ich hatte auch das Gefühl, als wir die Zahlen gesehen haben, dass wir alle glauben, dass der IT-Sicherheitsmarkt größer ist als er gerade ausgeschöpft wird. Das war ein zweiter Konsens, den ich mitbekommen habe. Danach ging die Diskussion in andere Richtungen.
Mein Eindruck war, dass Herr Schallbruch mit der IT-Sicherheitsindustrie überhaupt nicht zufrieden ist und sagt: Ihr müsst einfacher, besser, schneller, innovativer sein. Von den Anwendern haben wir gehört, dass sie gar nicht über Technologien reden wollen, sondern über Funktionen. Die Hersteller haben natürlich nur über Technologien geredet und haben sich gegenseitig nicht gut aussehen lassen. Man hätte sagen können, wir sind alle zusammen hier, und wir wollen die Welt verändern. Das war mein Eindruck. Ein Investor hat gesagt, dass sich das alles gar nicht lohnt. Ich habe das Gefühl, dass wir alle in unterschiedliche Richtungen gucken. Für mich ist das auch mein Statement, dass wir eine gemeinsame Strategie für die IT-Sicherheit in Deutschland brauchen. Die Frage ist: Wo wollen wir eigentlich hin? Was ist denn das Sicherheitsniveau, das wir erreichen wollen? Ich würde auch gern von den Anwendern wissen, was denn die Sicherheitsfunktionen sind, die sie brauchen und was sie dafür bezahlen würden. Dann können sich die IT-Sicherheitsfirmen ausrichten und können sagen, wie sie das erreichen können, allein oder in einer Holding. Das sind dann interessante Diskussionen, in denen man fragen kann, wie das geht.
Ich glaube, wenn wir keine Strategie haben, was wir eigentlich gemeinsam wollen in Deutschland und wie wir das umsetzen können, dann diskutieren wir nächstes Jahr noch und kommen kein Stück weiter.
Dieses gemeinsame Denken, alle zusammenzubringen, und die Möglichkeiten der Start-ups gliedern sich dann automatisch ein. Wenn wir Technologien brauchen, die noch nicht da sind, kann man natürlich junge Leute motivieren, dass sie innovieren und sie dann in die Holding aufgenommen werden. Oder sie werden in andere Firmen gegliedert.
Wir sollten erst einmal die Ziele definieren, wohin wir wollen und dann sehen, wer helfen kann dies zu erreichen. Da gibt es sicherlich Aufgaben für die Anwender, und der Staat wird eine ganze Menge an Aufgaben für seinen Arbeitsplan bekommen, ebenso die Firmen.

Dann haben wir eine Chance in Deutschland das zu erreichen, was wir wollen, ein angemessenes Sicherheitsniveau mit einer Vertrauenswürdigkeit, die wir brauchen. Alles andere ist der Weg dorthin.

Herr Köhler:
Vielen Dank. Ich habe jetzt gerade im Kopf, dass der TeleTrusT gerade zum Thema IT-Strategie, Sicherheitsstrategie etwas vorgeschlagen hat. Vielleicht lohnt es sich für den einen oder anderen, einmal hineinzugucken, weil Sie zumindest einmal einen Versuch gemacht haben, auch Ziele vorzugeben. Das ist das Entscheidende, einfach eine Diskussionsbasis auf einen Punkt zu bringen und den dann auch gemeinschaftlich zu diskutieren.
Herr Dr. Schabhüser ist promovierter Mathematiker, seit über 20 Jahren im BSI tätig und kennt nicht nur die Branche in- und auswendig, sondern auch das, was vielleicht der Regulierer und die öffentliche Hand zu tun haben und leisten. Er ist im Thema Kryptographie von Anfang an zuhause. Wir freuen uns, dass Sie hier sind und hören gespannt Ihrem Statement zu.

Dr. Schabhüser:
Da muss ich meiner Rolle gerecht werden. Als Regulierer bevorzuge ich natürlich Regulierung ... Nein, das war ein Scherz. Herr Pohlmann sagte es gerade, ich bevorzuge Ziele zu definieren. Ziele zu formulieren, ist gar nicht so schwer. Die digitale Souveränität – Superziel. Man muss hinterher aber die Ziele auch realistisch formulieren. Der Zug für die IT-Branche ist in Deutschland für viele Bereiche abgefahren. Wir sind da nicht überall führend. Also, müssen wir sehen, was wir in welchen Bereichen machen können.
Es wurde heute sehr viel gejammert, dass man die Kundschaft erreichen muss und usw.
Herr Woithe sagte gerade zurecht, dass man in Lösungen denken muss, nicht nur in Regulierungen. Obwohl gerade das Unternehmen von Herrn Woithe davon lebt, weil Regulierung da war. Toll Collect ist nicht von selbst gekommen. Das große Geld ist durch Regulierung gekommen und das hat hinterher Märkte geschaffen. Das ist ein Ansatz, den wir auch mit im Auge haben müssen.
Wie ist das denn, wenn ich heute als Firma irgendetwas kaufe? Herr Woithe hat es schon beschrieben. Man will die Gesamtlösung kaufen. Dann sucht man sich meistens einen Generalausstatter und sagt, dass man IT-Funktionalität haben will. In einem Nebensatz wird gesagt, dass das auch noch sicher sein muss. Und so wird heute auch angeboten. Denn eigentlich haben die großen IT-Firmen ihre Funktionalität im Angebot und haben häufig als sehr preiswertes Add-on etwas an Sicherheit mit drin. Das ist einmal so. Ob das jetzt gut ist oder nicht, Sicherheit ist mit adressiert, ist mit im Paket und als Gesamtpaket da.
Das ist heute hinreichend deutlich herausgearbeitet worden. In Deutschland haben wir unsere tolle mittelständische, Technologie getriebene Sicherheitsindustrie. Herr Woithe hat es auch richtig beschrieben. Er will nicht mit, was weiß ich, Herrn Quelle, Herrn Harlander, Herrn Baumgart reden, wie er aus den vielen kleinen Häppchen eine anständige Lösung hinbekommt. Er will einfach sagen: macht mir ein Gesamtpaket und schnürt das zusammen. Dann ist das gut.
Das ist das, was Sie angesprochen haben. Man muss die Fähigkeiten der IT-Sicherheitsindustrie zu Gesamtlösungen bündeln, eigene Identitäten ein bisschen zurückstellen, in ein großes Paket hineinpacken und in der Konsequenz dann aber auch schlagfertiger sein.
Seit gefühlten 15 Jahren versuche ich, das in dem doch so kleinen VS-Markt ein wenig hinzubekommen. Ich bin nahezu vollständig gescheitert. 15 Versuche, pro Jahr einen und alle sind schief gegangen. Aber das kann besser werden.
Fähigkeiten und Ziele: Ich glaube aber auch, damit wir in diesen Markt einbrechen können, müssen wir in gewissen Bereichen doch so etwas wie Märkte schaffen. Das muss nicht gleich richtige Regulierung sein. Ich glaube zwar, dass wir im KRITIS-Bereich definitiv regulieren

sollen, und das wird durch das geplante IT-Sicherheitsgesetz auch angegangen. In anderen Bereichen müssen wir regulatorische Anreize schaffen.
Meine Idee ist, auf der einen Seite IT-Sicherheit auch finanziell messbar zu machen. Wer gute IT-Sicherheit macht, kommt in seiner Versicherungs-Police für Schäden besser weg. Das ist dann eine indirekte Regulierung. Ein Betreiber wird nicht unmittelbar verpflichtet, IT-Sicherheit umzusetzen, sondern wir schaffen einen Rahmen, der finanzielle Anreize schafft, Investitionen in IT-Sicherheit vorzunehmen.
Ein anderer Punkt des „Märkte schaffen" läuft bei mir immer noch unter Standardisierung. In diesem Umfeld ist das BSI sehr engagiert, indem für bestimmte Bereiche der IT in Deutschland Anforderungen formuliert werden, die sowohl Funktionalität als auch IT-Sicherheit und zugehörige Nachweisführungen adressieren. Diese Protection Profiles und technische Richtlinien werden gemeinsam mit der Kundschaft, den Herstellern u. ä. etabliert und durch die Beteiligung die Firmen werden diese natürlich in die Lage versetzt, Time to Market Vorteile auszunutzen. Sie kommen dann schon mit Lösungen auf den Markt, wenn sie gebraucht werden. Das ist ein sehr diffiziles Steuerungsnetz. Das greift überhaupt kaum regulativ in die Märkte ein. Man ist nur schneller, und das finde ich ausgesprochen schön.
Das ist etwas, was man definitiv ausbauen kann. Rund um Smart Metering ist so etwas passiert, rund um hoheitlich Dokumente samt Grenzkontrollsystem ist so etwas passiert. Dort haben wir genau diese Einsätze gefahren. Das kann man an verschiedenen Stellen ausbauen, ist durchaus aber auch arbeitsintensiv.
Das BSI ist in diesem Prozess bisher immer in einer sehr starken Rolle. Dies kann in Zukunft sicher mit mehr verteilten Aufgaben und Rollen umgesetzt werden, mit dem BSI als steuernde Instanz oben drüber. Das Doing wird mehr verteilt. Aber dieses indirekte Märkte schaffen durch eine kürzere Time to Market Phase für die beteiligte Industrie halte ich für einen sehr effektiven Weg.

Herr Köhler:
Vielen Dank, Herr Dr. Schabhüser.
Ich gehe in der Runde weiter zu Herrn Möhring. Eigentlich leitet er eine gescheiterte Holdingstruktur. Bitte nicht falsch verstehen. Herr Möhring ist für das Sicherheitsnetzwerk in München verantwortlich. Eigentlich wäre das eine gute Ausgangsbasis gewesen, nämlich auf Basis des Spitzencluster-Wettbewerbes eine Struktur aufzubauen, die sogar eine ziemlich erhebliche Finanzierungskomponente hatte. Es hat trotzdem nicht geklappt. Wir haben uns das in dem Masterplan angeguckt, bei den Bewerbungen aus Berlin. München ist vielleicht eine gesonderte Diskussion, das einmal nachzuarbeiten. Aber immerhin hat der Spitzencluster-Wettbewerb bisher noch keinen IT-Sicherheitscluster genehmigt. Auch das ist bestimmt eine spannende Frage.
Herr Möhring kommt aus dem Hause Giesecke & Devrient, ist also mit dem Thema seit langem befasst und hat jetzt seit zwei Jahren die spannend Aufgabe die südliche IT-Sicherheitswirtschaft etwas unter einen Hut zu bringen.

Herr Möhring
Schönen Dank, Herr Köhler. Guten Abend allerseits. Der Snowden Effekt, der Marketingeffekt, über den wir heute schon gehört haben, kam für unsere Spitzencluster-Bewerbung etwas zu spät. Die wäre vielleicht wirklich anders ausgegangen, wenn dieses Bewusstsein und die Dimension der Thematik den Herrschaften in den verantwortlichen Jurys usw. bewusst gewesen wäre.
Aber jetzt stehe ich trotzdem zwei Jahre später hier vor Ihnen, um über dieses Netzwerk zu berichten, die ersten Erfahrungen aufzuzeigen. Dieser Honigtopf im Sinne eines Geldtopfes, der damals die Akteure veranlasst hat, an diesem BMBF Wettbewerb mitzumachen, ist tatsächlich an uns vorbeigezogen. Dennoch hat der Impuls, an diesem Wettbewerb mitzumachen,

ausgereicht, dieses Netzwerk fortzusetzen. Die Motivation waren Dinge, die heute hier schon genannt worden sind. Time to Market ist ein großes Stichwort, die Innovations- und Produktzyklen, die immer schneller werden. Dass man das oftmals allein nicht mehr bewältigen kann, da mitzuhalten, wird einem schnell klar. Man braucht Kooperationen, man braucht Kompetenzen, um diese Entwicklungen in dieser Geschwindigkeit tatsächlich in marktfähige Produkte überleiten zu können. Das ist die Motivation, warum die Unternehmen, die Forschungseinrichtungen und auch die Anwender – ich war eigentlich sehr froh über den Vortrag vorhin, weil die Anwenderperspektive sehr relevant ist in unserer Netzwerkarbeit ist – sich im Netzwerk einbringen.
Wir haben damals ehrlich gesagt die Netzwerkaktivitäten nicht so aus der Bedrohungsperspektive heraus betrachtet, sondern eigentlich aus der Perspektive, dass die Innovationen tatsächlich durch die Informationstechnologien so rasant voranschreiten, wie auch die Vernetzung zunimmt, so dass wir die Sicherheit hierfür eigentlich als notwendigen Baustein sehen, als Plattform, um diese Dinge, die neuen Geschäftsmodelle und geschäftlichen Möglichkeiten überhaupt zu ermöglichen. Wir haben diesen positiven Ansatz also hier gesucht und verfolgt. Ich hoffe, und habe mich deswegen auch über diese Einladung heute gefreut, dass wir diese auf den Großraum München aktuell beschränkte Aktivität natürlich auch verbinden können mit Kompetenzen, die es sonst im Land gibt, weil wir uns davon wirklich einen Mehrwert einer solchen auch bundesweiten Vernetzung versprechen.

Herr Köhler:
Herr Möhring, vielen Dank. Wir haben im Prinzip in der Fragerunde hier gehört, dass das Thema Aufmerksamkeit und das Thema Bedeutung tatsächlich in den letzten Jahren deutlich zugenommen hat. Herr Dr. Baumgart meinte – ich würde das auch bestätigen -, dass wir es irgendwie noch nicht gemerkt haben. Da sind wir vielleicht in einer ähnlichen Situation. Die Holdingstruktur, vielleicht in zehn Jahren gibt es irgendwie einmal so etwas. Aber womit fangen wir denn jetzt konkret an? Ich gebe die Frage an Prof. Pohlmann weiter.

Prof. Pohlmann:
Erst einmal meine ich, das mit der gemeinsamen IT-Sicherheitsstrategie ernst. Ich glaube, dass wir gemeinsam überlegen müssen, wo wir hin wollen und dass wir in Deutschland – wir haben es gehört - eigentlich viele IT-Sicherheitstechnologien haben von unseren mittelständischen Unternehmen, die innovativ sind, die gut sind. Wir haben nur das Problem, dass wir sie nicht richtig auf die Straße bekommen. Wir haben gerade gestern noch einmal auf einer Konferenz mit Microsoft darüber diskutiert und festgestellt, dass wir schon anerkennen müssen, dass wir nicht IT-Marktführer sind, also wir müssen schauen, wie wir IT-Sicherheit in die Marktführer-IT einbinden können.
Wir fordern jetzt vom TeleTrusT Verein Ideen wie IT-Security und IT-Security Replaceabilty, also die Idee, dass die Firmen Schnittstellen zur Verfügung stellen, wo man Technologien tauschen kann, z.B. amerikanische IT-Sicherheitstechnologie gegen deutsche IT-Sicherheitstechnologie, weil die eine höhere Wirkung und Vertrauenswürdigkeit hat. Wir glauben, dass das auch von den Amerikanern verstanden wird. Sie werden bereit sein, das zu tun, weil es am Ende eine WIN-WIN Situation ist.
Die Amerikaner können damit wieder Vertrauen zurückgewinnen, weil sie sagen, okay, die Kunden können selber aussuchen. Die Anwender haben die Chance, dann auch wirklich auszusuchen. Wenn der Schutzbedarf das nicht verlangt, können sie amerikanische Technologie nehmen. Aber wenn der Schutzbedarf höher ist, können sie auch deutsche Technologie verwenden.
Für die deutsche IT-Sicherheitsbranche gibt es die Chance zu sagen, wenn ich eine IT-Sicherheitstechnologie habe, die in IT-Standardlösungen eingebunden ist – es muss integrativ einfach benutzbar sein -, dann kann ich auch internationalisieren und kann sagen, dass ich nicht nur in

Deutschland verkaufen kann, sondern auch weltweit erfolgreich sein kann. Wir glauben, dass das eine ganz gute Strategie ist. Wie schaffen wir es, gute IT-Sicherheitstechnologie, die deutlich besser gegen die größten IT-Sicherheitsprobleme wirkt, einzuführen? Die großen IT-Sicherheitsprobleme sind zurzeit: Zu viele Fehler, Schwachstellen in Software, Anti-Malware, die nicht ausreichend Malware erkennt, Passworte als Authentifikationsmechanismus und so weiter. Diese Idee macht Sinn und das möchten wir auch gern, zumindest vom TeleTrusT heraus unterstützen und vorantreiben.

Herr Köhler:
Wenn wir das langfristig jetzt hier einmal annehmen und den Zahlen einigermaßen glauben, die wir heute gesehen haben, dann ist zumindest eine Sache festzuhalten, dass der nationale Markt nicht nur klein ist sondern im Moment auch irgendwie einigermaßen bedient wird. Das heißt nicht, dass man da nicht auch noch wachsen kann. Aber der Blick geht nach außen. Das haben Sie auch gesagt.
Vielleicht, Frau Wiesmüller, an Sie die Frage, wenn die Holdingstruktur wächst, gibt es auch andere Möglichkeiten zu kooperieren? Mich beschäftigt die Frage auch seit langem, welche Möglichkeiten man hat, im Verbund tatsächlich vertrieblich besser zu werden, aus der Geschäftsentwicklungsperspektive?

Frau Wiesmüller:
Aus der Sicht der Geschäftsentwicklungsperspektive und um besser zu werden, ist natürlich ein Verbund ein bevorzugter Ansatz, warum Unternehmen miteinander kooperieren. Und die kleinste Einheit der Zusammenarbeit ist die Kooperation. Ich würde sagen, dass eine Kooperation ein sehr guter Ansatz für eine Zusammenarbeit ist, da langfristig weniger verbindlich wenngleich rechtlich geregelt. Kooperationen oder aber auch strategische Allianzen sind ja grundsätzlich auch Zusammenschlüsse, die auf vertraglicher Basis stattfinden, aber trotzdem im Vergleich zu anderen Verbundstrukturen deutlich schneller wieder aufgelöst werden können. Arbeitsgemeinschaften ArGe sind ebenfalls ein beliebter Einstieg, um eine Zusammenarbeit zu beginnen und Zusammenarbeit „zu trainieren".
Ich habe mich in meinen anfänglichen Ausführungen zur grundsätzlichen Erläuterung von Verbundstrukturen heute eher kurz gehalten. Schließlich geht es aber auch darum, darüber nachzudenken, welche Risiken mit einer möglichen Zusammenarbeit einhergehen und welche Schwierigkeiten es gibt, solche Zusammenarbeiten ins Leben zu rufen. Das wirft z. B. die Frage auf, ob Unternehmen kulturell zusammenpassen? Woran mache ich dieses fest? Wie feinfühlig findet die Kommunikation dazu statt? Es ist sicherlich nicht so, dass sich hier heute Abend gleich drei oder vier Unternehmen finden, die meine Idee toll finden und nur darauf gewartet haben, dass es losgeht. Die Situation ist die, dass neben den bekannten Hard Facts - den Unternehmenszahlen - zu diesem Thema auch viele sog. weiche Faktoren mit berücksichtigt werden müssen. Denn gemäß des alten Sprichwortes: „Prüfe, was sich ewig bindet, ob sich nicht ein besserer findet"….
So eine Zusammenarbeit muss irgendwo also auch wachsen und man muss sich eben Gedanken darüber machen, ob die Unternehmen zusammenpassen. Nicht nur von ihrem Portfolio, was selbstverständlich die Grundlage des zukünftigen Handels ist, sondern auch was die Werteausrichtung angeht, was die gemeinsame Strategie angeht. Was für weitere Ziele verfolgt das Unternehmen zusätzlich zum erforderlichen Wachstumskurs?
Dergleichen Fragestellungen kann man sehr gut in Kooperationen austesten oder in strategischen Zusammenschlüsse gemeinsam Projekte abwickeln und sich dann fortführende Gedanken machen.
Ich bin immer wieder bei dem Punkt, gemeinsam etwas zu tun, Kräfte zu bündeln. Das hat auch etwas mit Vertrauen zu tun. Ich muss mich auf eine Zusammenarbeit einlassen. Ich muss einen Teil meines eigenen Knowhows, meiner eigenen Ressourcen dem anderen zur Verfügung

stellen mit dem Ziel, dass ich das gleiche zurückbekomme und ein „gemeinsames Mehr“ entsteht.

Herr Köhler:
Vielen Dank. Herr Dr. Schabhüser, aus Ihrer tiefen technologischen Sicht vielleicht: Gibt es für Sie Märkte, die sich vielleicht für deutsche Unternehmen, für deutsche Konsortien besonders anbieten? Das ist der erste Teil der Frage und der zweite Teil: Das zieht sich heute auch so durch den ganzen Tag durch. Sie sind eigentlich als Fachbehörde im Bereich des BSI in dem Thema fachlich unterwegs. Wie ist eigentlich das Zusammenspiel optimal zwischen dem, der vielleicht im Kern zuständig ist für das, was wir hier im ersten Schritt reden, ein Bundeswirtschaftsministerium, nämlich für die IT-Sicherheitswirtschaft in der Kooperation mit der Fachbehörde und den Blickwinkel auf einen auswärtigen Markt?

Dr. Schabhüser:
Das ist schon eine etwas schwierigere Frage. Als Fachbehörde Märkte erschließen und wie? Welche Märkte sind da? Im Moment sehe ich noch immer das Label, „IT-Security made in Germany“, egal wie gut die Initiative bisher gelaufen ist, mit dem man etwas tun kann. Deswegen wird auch gern in Deutschland recherchiert, welche IT-Sicherheitsfirmen irgendeinen Beitrag leisten können. Das ist im Moment eine Chance, da derzeit eine gewisse Vertrauenskrise bei den führenden IT Nationen gegeben ist. Jetzt müssen Kooperationen oder strategische Partnerschaften geschlossen werden, um in das Portfolio der „Großen“ zu kommen. Da kann die Politik, wenn nötig, sogar ein bisschen Druck machen, weil der eine oder andere doch möchte, dass die Beziehungen wieder besser werden. In dem Kontext kann man schon mal klare Worte sprechen, um die eine oder andere Kooperation wirklich unterstützend ans Fliegen zu kriegen bzw. die Rahmenbedingungen so zu setzen, dass in den Kooperationen die Sichtbarkeit IT-Security Made in Germany hinreichend stark ist.
Da sind wir auch gern als BSI an der einen oder anderen Stelle bereit zu unterstützen. Das kann sicherlich aber auch mit Unterstützung der Ministerien erfolgen. Diesen Ansatz können wir aber nur punktuell verfolgen, nämlich dort, wo wir eine strategische Partnerschaft für einen besonderen Zielmarkt sehen.
Einerseits ist das BMWi zuständig für die Industrie, auf der einen Seite ist das BSI technischer Sicherheitserzeuger oder genauer gesagt „Einforderer“ und hinterher auch Bestätiger, dass IT-Sicherheit gegeben ist. Das funktioniert an einigen Stellen ausgesprochen gut. Ich hatte eben diese spezialgesetzlichen Regelungen herausgearbeitet, wo an den richtigen Stellen eine Forderung an die IT-Sicherheit platziert wird, um hinterher die Märkte auch zu schaffen. Eine besondere strukturierte Kooperation BMI/BSI mit BMWi sehe ich auch nicht unbedingt als notwendig an. Wenn sich BMI und BMWi zusammensetzen, entsteht noch lange keine Wirtschaft. Dafür brauchen wir noch mehr.
Derzeit sehe ich hier keine besondere Rolle des BSI als Industrieförderer; wir können jedoch an punktuellen Stellen Hilfestellung leisten. Künftig werden wir über das IT-Sicherheitsgesetz die Rolle als Berater für die Segmente oder die Sektoren, die ihre eigenen Mindeststandards schreiben sollen, erhalten. Da würde ich mir wünschen, dass das BSI hinterher das letzte Wort hat. Ob wir damit durchkommen, wissen wir noch nicht. Aber eine starke Rolle des BSI als beratende Instanz wird schon einmal dabei sein.

Herr Köhler:
Vielen Dank. Die Frage war auch gar nicht so gemeint, inwieweit BSI und BMWi gemeinsam uns den Markt öffnen. Das wäre auch nicht schlecht. Die Frage war - Herr Grabowski hat auch immer betont, dass er nicht vom Fach ist -, dass es eher um das Zusammenspiel geht und die Zuständigkeit des Bundeswirtschaftsministeriums für die IT-Sicherheitsindustrie, wo Sie durchaus als Fachberater eine Supportfunktion spielen könnten.

Herr Möhring, die Frage das Sicherheitsnetzwerk noch einmal aufgreifend auch auf dem internationalen Markt, können Sie vielleicht einerseits noch einmal darauf eingehen, was Sie ganz operativ jetzt daraus machen? Es gibt durchaus auch Programme, wo sich Verbünde bewerben können, nicht nur Horizon 2020, die haben die Struktur auch im Zweifelsfall nicht, um den nationalen Markt zu bedienen, denn dann treten wir uns wieder auf die Füße. Vielleicht können Sie darauf kurz eingehen.

Herr Möhring:
Tatsächlich ist es so, dass ein Großteil der Clustermitglieder wesentlich vom internationalen Geschäft lebt. Wir haben eine Infineon. Wir haben natürlich Siemens mit den Fachabteilungen, die da noch zugange sind. Auch unser Haus, Giesecke & Devrient, es wurde vorhin schon gesagt, ist ganz klar im internationalen Geschäft unterwegs.
Der Fokus der Clusterarbeit ist schon relativ technisch. Wir verstehen uns auch nicht als zweiter kleiner BITKOM oder einen der anderen bereits existierenden Verbände, sondern sind schon angetreten, technische Kompetenzen zu bündeln, um hier zu marktfähigen Lösungen und Produkten zu kommen.
Der internationale Aspekt dabei ist ganz normal, wenn ich für ein Android Betriebssystem eine sichere Ausführungsumgebung entwickele, dann kann man das nur noch an Telefonhersteller verkaufen, die heute nicht mehr in Deutschland sind, sondern im Wesentlichen in Asien, um diese Technologen mit deutschem Inhalt dort international zu platzieren.
Ein anderer Mehrwert, den wir über diese Netzwerkverbindung sehen, ist auch, dass sich kleine spezialisierte Firmen über das international etablierte Netzwerk von großen Konzernen – Siemens hat natürlich in Kalifornien seine Büros, Infineon auch – dort über diese international etablierten Großunternehmen mit seinen spezifischen Kompetenzen und Lösungen auch Zugang findet zu diesen Märkten.
Das sind ein typisches Modell, internationale Förderprojekte, die Sie gerade ansprechen, Horizon 2020. Dort suchen sich natürlich die Partner im Netzwerk die passenden Konsortien zu dem jeweiligen Thema. Das geschieht eigentlich recht autonom. Das Netzwerk ist nicht so groß, dass man sich nicht kennen würde. Ein Mehrwert ist natürlich, sich einmal kennenzulernen und von den Themen und den Kompetenzen zu wissen, mit denen jeder unterwegs ist. Nicht jeder weiß immer, auch aufgrund der Rasanz der technologischen Entwicklung, wer gerade mit welchen Kompetenzen und Entwicklungen unterwegs ist. Das hilft auch in dieser internationalen Sichtbarkeit.
Trotzdem gibt es auf jeden Fall noch Raum für Verbesserungen. Das ist unser Ziel für die nächsten Jahre. Da es sich um ein bayerisches Netzwerk handelt mit gewisser bayerischer Unterstützung, beispielsweise auch das recht bedeutsame Netzwerk von Niederlassungen der Bayerischen Staatsregierung, nicht die Handelskammern, die man auch hat, sondern regelrecht solche existierenden Geschäftsbüros zu nutzen, um eben diese Made in Germany Kompetenzen bekannt zu machen, die durchaus nachgefragt werden. Einen gewissen Snowden-Effekt haben einige unserer Mitglieder doch erlebt. Viele sind von der Apple Cloud weggegangen und haben nach etwas anderem gesucht, weil ihnen das nicht mehr ganz geheuer war.
Wir sind stark orientiert an den Anwendern. Ich habe es vorhin schon gesagt. Es ist in Deutschland und auch in Bayern die Industrie, der Maschinen- und Fahrzeugbau, aber auch die Energiebranche, die unsere Wirtschaft prägen, d.h. diese Differenzierung sehen wir auch in anderen innovativen Teilen der Welt.
Wir sind eigentlich der Meinung, dass wir diese Kompetenzen, die wir hier haben und die vielleicht nicht so bekannt sind, weil es nicht so medienbreit diskutiert wird, aber durchaus im Einsatz sind. Dass wir das auch in Form einer Fachkonferenz in München aufbauen und zeigen wollen. Da gibt es die Münchner Sicherheitskonferenz, die jedem ein Begriff ist und auf uns zugekommen ist und gesagt hat: Cyber Sicherheit ist mittlerweile nicht nur ein rein technologisches Thema oder ein Wirtschaftsthema, sondern auch ein gesellschaftliches Thema, und wir würden das gern hier mit einbauen. Das wäre natürlich auch ein Weg, unsere Kompetenzen,

Projekte und Firmen auch in einer solchen internationalen Fachkonferenz mit einzubringen. Ich stelle mir da ein bisschen so etwas wie den Mobile World Congress in Barcelona vor. Der fing auch einmal ganz klein als Hotelmesse in Nizza an und ist jetzt eine gigantische Veranstaltung. Warum nicht auch für Cyber Sicherheit mit diesem wirtschaftlichen Fokus? Das wäre unser Wunschziel.

Herr Köhler:
Vielen Dank. Herr Mörl hat jetzt die wunderbare Aufgabe, die letzte halbe Stunde zu moderieren und aus allem, was wir heute gehört haben, eine Strategie aus den vier Podiumsteilnehmern herauszuholen.

Prof. Carle, TU München:
Ich würde gern noch ein kurzes Statement abgeben. Mein Name ist Georg Carle, Professor für Informatik an der TU München, ich habe dort den Lehrstuhl für Netzarchitektur und Netzdienste. Ich habe mich seit etlichen Jahren damit befasst, was man über NSA Aktivitäten überhaupt so weiß, so wie frühere Whistle Blower auch schon Dinge aufgedeckt haben. Ich habe mich intensiv damit befasst, was wir gelernt haben über die häppchenweise zusätzlichen Dokumente. Ich denke, wir sind bezüglich dem Verständnis dessen, was wir da an weiterer Informationen haben, noch nicht komplett durch. Ich denke, dass wir da noch mehr Diskussionen brauchen, was das überhaupt bedeutet.
Man kann nicht einfach so weitermachen und sagen, in Deutschland haben wir ein paar hübsche Produkte und es ist blöd, dass wir den Produkten dieser dominierenden IT-Macht nicht mehr so richtig trauen können. Wir müssen schon bezüglich der Strategie, was Sie Herr Pohlmann gesagt haben, überlegen, ob das ausreicht oder wofür das ausreicht. Ich habe den Eindruck, dass das, was wir aktuell in den Händen haben, uns nur einen äußerst eingeschränkten Schutz gibt. Vielleicht haben wir hier im Raum alle akzeptiert, dass wir mit diesem stark Eingeschränkten die nächste Zeit überleben müssen und wollen deshalb nicht so misslich dreinschauen und sagen, dass es besser halt nicht geht. Vielleicht können wir es trotzdem schaffen, irgendwie eine Strategie zu machen, dass das nicht immer so bleiben muss.
Das wäre meine Hoffnung. Da hätte ich gehofft, dass wir irgendetwas Greifbares mit nach Hause nehmen können und dass meine Hoffnung nicht nur eine Seifenblase ist.

Herr Mörl:
Ich hätte jetzt auch vorgeschlagen, dass wir das Thema erden, praktisch werden und mit wirklich kurzen Statements dazu kommen, was eigentlich wäre. Wir haben eine Menge Konjunktive gehört und diese Konjunktive treiben uns, Herrn Dr. Schabhüser seit 15 Jahren und uns, itWatch, noch ein bisschen länger in der Gegend herum. Sie, Hr. Dr. Schabhüser, haben gesagt: 15 Versuche und keiner hat geklappt.
Ich würde ganz gern mit Frau Wiesmüller anfangen, ein bisschen provokanter heranzugehen. Für mich klingt das Statement, was ich von Dr. Melzer und von Ihnen gehört habe, ein bisschen so, als wenn Sie aktiv dieser oben angesprochene „Pullover mit dem aufgemalten Sicherheitsgurt“ wären, indem Sie sagen, diese Technologien, wie Facebook, wie WhatsApp - WhatsApp ist ein Laden, der für 11 Mrd. verkauft worden ist, WhatsApp hat 50 Mitarbeiter und noch nie ein Plus im Budget gehabt - sind „Venture Kapital-fähig“. Diese Technologien von Facebook und WhatsApp treten das nationale Datenschutzgesetz mit Füssen, machen das legal im Ausland und es interessiert keinen. Das sind aber exakt die Firmen, die für die Investmentbanker interessant sind. „Und ihr von der IT-Security seid maximal unsexy, bleibt daheim, spielt im Keller und bitte lasst uns als Venture Capitalisten in Ruhe, außer ihr bündelt euch, macht das aus eigener Initiative und dann kommen wir um die Ecke und dann machen wir auch etwas mit euch“. Habe ich das falsch verstanden oder haben Sie auch für uns als Kellerkinder eine kleine Lösung, wie wir das verbessern können?

Frau Wiesmüller:
Zunächst einmal vielen Dank für Ihre Zusammenfassung. In der Tat besteht Korrekturbedarf. Ich denke schon, dass es Lösungen gibt, und zwar ganz konkrete. Es beginnt mit dem ersten Schritt, dem konkreten Aufeinander-Zugehen. Den kann man niemandem aufzwingen oder herbeireden.
Der erste Schritt beginnt ganz klar beim Unternehmer bzw. beim Unternehmensverantwortlichen selbst. Dort wo Handlungsbedarf erkannt wird. Bin ich bereit dazu, an so einer Lösung mitzuarbeiten? Wenn ja, dann gibt es eine Vielzahl praktischer Möglichkeiten. Diese Plattform zum Beispiel, der MÜNCHNER KREIS. Hier wurde dieses Thema heute erneut ins Rollen gebracht. Ich denke, hier sind Sie alle im Kontakt untereinander. Es bedarf meiner Ansicht nach weiterer Zusammentreffen und Gespräche zwischen den Unternehmen, die daran Interesse haben. Die sollten sich aber zuvor darüber klarwerden, ob sie wirklich etwas gemeinsam tun möchten.
Ein potentieller Kapitalgeber kommt als solcher meiner Ansicht nach erst im zweiten Schritt ins Spiel, und zwar dann, wenn man ihm etwas anbieten kann, was interessant ist. Zunächst einmal sollten Unternehmen, die sich so etwas vorstellen können, miteinander sprechen.
Auf Basis dieser Anbahnungen muss man sich zusammensetzen und fragen: Was wäre wenn, wie, womit und wo? Es macht sicherlich auch Sinn, solche Gespräche ab einem gewissen Stadium moderiert zu führen. Dergleichen Gespräche können – wenn unterschiedliche Interessen aufeinanderstoßen - in der Tat schnell emotional und heikel werden. Aber: Wo ein wirklicher Wille, da ein Weg.

Herr Mörl:
Meine Bitte wären einfach ganz kurze Statements. Diese IT-Security Landschaft wird von vielen Seiten betrachtet. Wenn wir den Versuch machen, dass wir sagen, wenn nationale Datenschutzrichtlinien, IT-Sicherheitsvorstellungen, die wir in der Bundesrepublik über lange Jahre entwickelt haben, exportfähig sind, weil wir gut sind, weil die Welt das will und braucht, dann stellt sich doch die Frage, warum da, wo wir IT im Ausland fördern, z.B. bei der Gesellschaft für internationale Zusammenarbeit, nicht die deutsche Vorstellung von IT-Sicherheit und Datenschutz ein Teil des geförderten IT-Projektes ist. Da werden Steuergelder im Ausland ausgegeben. Warum investieren wir da nicht in nationale Technologie und exportieren die? Das gleiche Thema haben wir bei der Drittmittelförderung. Wenn wir nationale Fördermittel haben, werden trotzdem ausländische IT-Sicherheitsprodukte in diese Themen involviert. Warum ist das so?

Prof. Pohlmann:
Wir müssen uns genau überlegen, was wir eigentlich leisten können. Was ist unsere Kompetenz? Wir müssen die Realität einschätzen. Im Sinne der IT-Souveränität wird keiner der Meinung sein, dass wir Google ersetzen können. Keiner wird der Meinung sein, dass wir Betriebssysteme selber entwickeln müssen, sondern wir müssen feststellen, wo wirklich Handlungsbedarf ist, wo Geld genutzt werden kann, Masse da ist, um gestalten zu können. Man muss mit den großen Herstellern sprechen und ihnen sagen, dass ihr Betriebssystem gut ist, aber die Festplattenverschlüsselung uns nicht gefällt. Diese muss ausgetauscht werden, um Vertrauen zu erlangen. Oder wir wollen die IP-Pakete über die Router verschlüsseln oder die Verschlüsselung aus Deutschland in die Router integrieren. Und wir müssen dann Konzepte finden, wie wir diese Idee umsetzen können.
Es gibt aber auch Aspekte, wie den Datenschutz, die wir technologisch nicht einfach umsetzen können. Der Datenschutz wird von den amerikanischen Unternehmen anders interpretiert. Das ist nicht einmal eine Bösartigkeit, sondern sie haben kulturell andere Vorstellungen und verdienen viel Geld mit den persönlichen Daten ihrer Kunden. Das werden wir ihnen nicht

über eine Technologie austreiben, sondern da wird die Europäische Union festlegen müssen, ob deutsches Recht oder europäisches Recht gilt.
Wir brauchen eine Unterschiedlichkeit; in unterschiedlichen Bereichen brauchen wir unterschiedliche Mechanismen. Wir müssen das Datenschutzgesetz europaweit und bei den Amerikanern durchsetzen. Wir müssen schauen, dass wir da, wo wir verschlüsseln können, verschlüsseln, um unsere Werte zu schützen. Und wir müssen da, wo wir IT-Sicherheitstechnologien einbringen können, uns abschotten. Wir müssen darüber diskutieren, wie wir das umsetzen können, also an welchen Stellen wir die IT-Hersteller motivieren müssen, diese Idee mit uns gemeinsam umzusetzen. An welchen Stellen brauchen wir Gesetze? An welchen Stellen brauchen wir Regulierungen? Und das muss gemeinsam diskutiert werden mit den Anwendern, der Politik, den IT-Sicherheitsherstellern aber auch mit der IT-Sicherheitsforschung zusammen.
Ich glaube, hier muss man eng zusammenspielen. Das kann man nicht klein-klein machen, sondern man muss ein Puzzle zusammenbauen und sich fragen, was wir uns leisten können. Was wollen wir uns leisten? Was müssen wir uns leisten? Das sollten wir gemeinsam entscheiden und dann wissen die Anwender, was sie zu kaufen haben. Dann weiß der Staat, was er zu beschaffen hat. Dann wissen die IT-Sicherheitshersteller, was sie entwickeln müssen und dann wissen die IT-Sicherheitsforscher, wo Innovationen gebraucht werden. Dann wissen auch die Start-ups, wo Handlungsbedarf vorhanden ist. Und dann haben wir eine Strategie und können die gemeinsam zielgerichtet umsetzen. Ich glaube, dass wir uns gemeinsam dazu entschließen sollten, die Prioritäten zu setzen.

Herr Mörl:
Herr Dr. Schabhüser, wir haben heute von Herrn Schallbruch gelernt, dass die Mindeststandards gesetzt werden von den einzelnen kritischen Umgebungen. Die Frage: Welche Rolle spielt das BSI bei der Kontrolle der Umsetzung und welche Chancen sehen Sie für die nationale IT-Security Industrie bei der Umsetzung der Mindeststandards?

Dr. Schabhüser:
Da muss man ein bisschen differenziert sehen. Die Rolle des BSI ist noch nicht völlig klar. Die minimale Rolle, die ich beim BSI sehe, ist, dass wir dafür zuständig sind, ein anständiges Lagebild zu erzeugen. Das hatten Sie gerade schon einmal adressiert. Wo sind wir? Wo stehen wir? Was sind die Auswirkungen u. ä. Da sehe ich das BSI durchaus in der Pflicht, basiert auf anonymisiert gemeldeten Vorfällen einmal darzulegen, was wirklich alles passiert. Die bisherigen Analysen sind alle schön und gut. Notwendig ist schon, dass substantiell aufgearbeitet wird, was wirklich schon passiert ist und was schon an Angriffen gelaufen ist. Da ist eine ganze Menge aufzuarbeiten.
Der nächste Schritt zur Rolle des BSI ist die Sensibilisierung an den richtigen Stellen, in den branchenspezifischen Arbeitskreisen darauf hinzuarbeiten auf dieses und jenes, was für den jeweiligen Bereich sehr relevant ist, ob das angemessen durch Sicherheitsmaßnahmen bedient wird, im Sinne einer Sensibilisierung und Beratung bei der Erstellung der entsprechenden Mindeststandards.
Ich kann mir sehr gut vorstellen, dass das BSI im Nachgang eine Konformitätsprüfung begleitet. Das müssen wir nicht alles selber tun, aber einen Prozess aufsetzen, wo im konkreten Fall die Konformität zu den Mindeststandards geprüft wird kann ich mir schon vorstellen. Ich würde mir wünschen, bin mir aber nicht sicher, ob das kommen wird, dass das BSI zum Schluss sagen soll: das ist genug. Und wenn wir sagen, dass es noch nicht genug ist, dann ist es auch noch nicht genug. Aber ich bin mir nicht sicher, ob diese Rolle für das BSI kommen wird.

Herr Mörl:
Herr Möhring, noch eine Anschlussfrage und dann würde ich gern die Fragerunde an das Publikum eröffnen. Wo sehen Sie die Zuständigkeit für die Durchsetzung einer digitalen Souveränität auf Bund-, Länder- und Kommunen-Ebene verortet?

Herr Möhring:
Da habe ich leider den Vortrag von Herrn Schallbruch verpasst, der sicher schon ein Teil der Antwort war. Ich bin auch nicht der Experte für diese Zuständigkeitsfragen der digitalen Souveränität. Das beginnt schon damit, dass mir nicht 100%ig klar ist, was das genau meint. Wir haben auch gesagt, dass Firmen im Netzwerk, die durchaus auch Produkte in Nordamerika verkaufen, Sicherheitsprodukte, und sich dort auch qualifizieren, um dort als Lieferant zugelassen zu werden, Teil unserer geschäftlichen Realität ist. Nun weiß ich nicht, inwieweit das teilweise auch Effekte haben kann, wenn man sich hier ein bisschen abschottet und sich gleichzeitig die Exportmärkte verbaut. Das müsste man sich noch einmal anschauen. Ich glaube, die Hochsicherheitsanwendungen sind heute schon vom BSI speziell qualifiziert und zertifiziert, um diese hochsensiblen Souveränitätsbereiche entsprechend abzudecken. Und bei diesem Thema, da wissen Sie mehr als ich.

Herr Mörl:
Dann würde ich jetzt in die Abschlussrunde gehen und mit der Kernfrage: welche Themen, glauben Sie, sollte der MÜNCHNER KREIS in kleinen Runden und Arbeitskreisen fortführen, um zu konkreten Ergebnissen, Lösungen, Vorgehensmodellen zu kommen? Vielleicht erst eine ganz kurze Antwort vom Panel und dann die Wünsche aus dem Publikum.

Frau Wiesmüller:
Ich darf ganz offen sagen, dass ich heute hier Premiere habe beim MÜNCHNER KREIS. Insofern fällt es mir etwas schwer, zu beurteilen, welche Themen Sie schon behandelt haben. Ich möchte meine Antwort kurz und allgemein halten. Aufgrund meiner Erfahrungen aus anderen vergleichbaren Veranstaltungen möchte dafür werben, dass eine ausgewogene Mischung darüber herrscht, Technologiethemen und Businessthemen gleichermaßen zu behandeln. Ich glaube, dass das eine nicht ohne das andere funktioniert. Wir haben bei vielen Technologien mit ansehen müssen, dass sie - bis zum letzten ausgereizt - in verschiedensten Veranstaltungen diskutiert wurden. Es gab wunderbare Lösungen, aber am Markt wurden sie zum Rohrkrepierer.
Mein Statement wäre somit eine gesunde Mischung eben auch mit Businessthemen wie: Was braucht der Markt? Was wünscht sich der Anwender und wie kommen wir dazu? Mehr Marktnachfrage führt unweigerlich wiederum zur Stärkung der Wirtschaft – wobei wir dann wieder bei unserem Thema wären.

Prof. Pohlmann:
Ich hatte schon einige Male meine Priorität gesagt. Wir kommen nicht umhin, eine Strategie zu definieren, und ich bin mir nicht sicher, ob der MÜNCHNER KREIS der geeignete Platz ist, das zu machen. Wenn ich es richtig verstanden habe, gibt es eine Dialogplattform von den Bundesministerien, zu der die Stakeholder eingeladen werden sollen, um gemeinsam eine Strategie zu definieren. Man wird eine Menge an Teilthemen diskutieren müssen. Die Idee, dass Firmen sich zusammentun und zusammen stärker sind, finde ich eine interessante Idee. Warum soll man die nicht diskutieren und gucken, ob man Gesellschaftsformen hinkriegt, wo WIN-WINN möglich ist und wie man dann die Mittelständler im Bereich IT-Sicherheit zusammenkriegt. Das wäre eine spannende Aufgabe. Das könnte ich mir durchaus vorstellen. Aber ich glaube, wir müssen erst einmal die erste Diskussion führen, die Ziele entwickeln und dann gucken, wie die einzelnen Stakeholder die Teilaufgaben lösen können.

Dr. Schabhüser:
Vertieft in die Struktur des MÜNCHNER KREIS bin ich noch nicht eingedrungen, so dass ich nicht genau weiß, was der Kreis wirklich leisten kann. Ich fand die Idee von Ihnen ausgesprochen interessant, nämlich die Businessfelder, Geschäftselemente zusammenzutragen. Ich glaube, dass man das in kleineren Kreisen unter den Teilnehmern schon in den Griff kriegen kann.
Technologie sollte die zweite Rolle spielen und Geschäftsfelder eher die erste Rolle, weil wir da einfach Defizite haben. Das könnte ich mir als Kristallisationspunkt für Kooperationen vorstellen. Ich glaube nicht, dass die kleinen Kreise dann die Kooperationen bringen, aber den Appetit auf so etwas wecken können. Das ist eine Botschaft von mir.

Herr Möhring:
Ich glaube, dass man diese Dialogveranstaltungen, die der MÜNCHNER KREIS seit geraumer Zeit durchführt zu spezifischen Branchen, mit dem Thema IT-Sicherheit noch würzen kann und da idealerweise die Kompetenzen des Sicherheitsnetzwerks München mit dazu gehören. Das wäre eine Anregung, diese Dialoge in die Politik als Sprachrohr mit einzubringen, so wie sich der MÜNCHNER KREIS auch versteht. Ich glaube, dass das wichtig ist und wir da gern auch unseren Beitrag leisten wollen.

Prof. Thielmann:
Ich möchte als Mitorganisator fragen, welche Firmen bereit sind, sich in einem kleineren Kreis, wie es Herr Schabhüser auch sagt, einmal zusammenzusetzen? Ich glaube, Herr Schallbruch hat uns dazu eine Empfehlung gegeben. : „Setzt euch zusammen und kommt auf uns zu. Wir sind gern bereit zur Zusammenarbeit.“ Aber eigentlich sollten wir heute einfach einmal feststellen – wir werden auch noch über Internet abfragen - wer zu weiteren Diskussionen im kleinen Kreis bereit ist, an Ideen mitzuarbeiten. Die Handzeichen zeigen mir, dass es Sinn macht.

Dr. Baumgart:
Entschuldigung, aber wir können uns doch nicht zusammensetzen und irgendwo heimlich im Keller überlegen, wie die Welt aussieht, kommen dann raus und stellen fest, dass alles anders ist. So kann es doch nicht gehen. Wir müssen doch vom Bedarf ausgehen. Herr Prof. Pohlmann hat es gerade richtig gesagt. Was benötigen wir denn? Wir müssen überhaupt erst einmal wissen, was wir brauchen. Auf der anderen Seite ist es so, dass wenn wir einen Bedarf feststellen, es automatisch Kooperationen gibt. Solche Kooperationen hat es immer gegeben. Ich kann nur von uns sprechen. Wir kooperieren natürlich mit Partnern, sobald sich eine Geschäftsmöglichkeit ergibt. Das ist gar kein Problem. Ganz im Gegenteil, das machen wir doch gern und schauen, wie wir gemeinsam eine nationale partnerschaftliche Technologie in einem Projekt platzieren können. Wir arbeiten zum Beispiel mit der Bundesdruckerei zusammen und haben gemeinsam automatische Grenzkontrollanlagen für Deutschland aufgebaut. Auch das Unternehmen Cognitec ist an diesem Projekt beteiligt. Wir haben hochgradige, auch internationale Kompetenz damit bewiesen, in internationalen Ausschreibungen solche Projekte zu gewinnen. Partnerschaften müssen sich doch vom Markt her ergeben und können nicht erzwungen werden nach dem Motto: Wir haben uns jetzt alle lieb. Das kann nicht zum Erfolg führen.

Frau Wiesmüller:
Wenn ich ganz kurz dazu noch etwas antworten darf. Ich finde doch, dass Sie in dem Zusammenhang nicht die Unternehmensgröße repräsentieren, die den Hauptnutzen des besprochenen Ansatzes zieht. Wie wir wissen, führen Sie ein Unternehmen mit fast 300 Mitarbeitern – also eher schon ein etwas größeres mittelständisches Unternehmen mit entsprechendem Background. Viele kleinere Unternehmen haben aber diese komfortable Situation nicht, einfach

sagen zu können: „da mach ich hier mit oder da mit ….. “
Man sollte dieser Idee schon mit Leben füllen. Ich glaube, wir haben auch nicht darüber gesprochen, dass wir konspirative Gespräche dazu in irgendeinem Keller machen wollen. Ich würde zur Not auch noch andere Örtlichkeiten für Gespräche finden. Man sollte Ideen doch nicht sofort abwürgen bevor man etwas darüber gesprochen hat.

Prof. Thielmann:
Meine Damen und Herren, wir müssen jetzt leider Schluss machen. Wir führen die Abfrage seitens des MÜNCHNER KREIS durch. Aber ich denke, mit dem Thema, das Herr Dr. Baumgart beschrieben hat. Wer macht mit bei den Marktdefinitionen? Zielvorstellungen, wie auch Prof. Pohlmann gesagt hat.
Ich danke Ihnen allen, dass Sie so lange ausgehalten haben und hoffe, dass wir in irgendeiner Form einen Schritt weiterkommen.

Anhang

Liste der Referenten, Moderatoren und Diskussionsteilnehmer

Ammar Alkassar
Sirrix AG
Im Stadtwald D3 2
66123 Saarbrücken
a.alkassar@sirrix.com

Dr. Rainer Baumgart
Vorsitzender des Vorstandes
secunet Security Networks AG
Kronprinzenstr. 30
45128 Essen
rainer.baumgart@secunet.com

Prof. Dr. Michael Dowling
Universität Regensburg
LS f. Innovations- und
Technologiemanagement
93040 Regensburg
michael.dowling@wiwi.uni-regensburg.de

Prof. Dr.-Ing. Jörg Eberspächer
Technische Universität München
Arcisstr. 21
80333 München
joerg.eberspaecher@tum.de

Marc Fliehe
BITKOM e.V.
Bereichsleiter Sicherheit
Albrechtstr. 10
10117 Berlin
m.fliehe@bitkom.org

Helmut Friedel
certgate GmbH
Merianstr. 26
90409 Nürnberg
friedel@certgate.com

Dr. Dirk Grabowski
BMWi
Referatsleiter Sicherheitsindustrie
Scharnhorststr. 34-37
10115 Berlin
dirk.grabowski@bmwi.bund.de

Dr. Magnus Harlander
Geschäftsführer
genua mbH
Domagkstr. 7
85551 Kirchheim
magnus_harlander@genua.de

Christian Köhler
Leiter Vertrieb
Geschäftsberreich InfoKom
IABG mbH
Alt-Moabit 94
10559 Berlin
ckoehler@iabg.de

Dr. Oliver Melzer
Gründer und Partner
AMMER PARTNERS GMBH
Schauenburgerstrasse 27
20095 Hamburg
melzer@ammerpartners.de

Peter Möhring
Alliance Management
Giesecke & Devrient GmbH
Prinzregentenstr. 159
81677 München
peter.moehring@gi-de.com

Ramon Mörl
Geschäftsführer
itWatch GmbH
Aschauer Str. 30
81549 München
ramon.moerl@itwatch.de

Dr. Kim Nguyen
Bundesdruckerei / D-Trust
T SC
Kommandantenstraße 15
10969 Berlin
kim.nguyen@bdr.de

Dr. Christoph Peylo
Geschäftsführer
Trust2Core GmbH
Kurfürstendamm 22
(Neues Kranzlereck)
10719 Berlin
christoph.peylo@)trust2core.de

Prof. Dr. Norbert Pohlmann
Geschäftsführender Direktor
Institut für Internet-Sicherheit if(is)
Westfälische Hochschule
FB Informatik und Kommunikation
Neidenburger Str. 43
45897 Gelsenkirchen
pohlmann@internet-sicherheit.de

Dr. Gerhard Schabhüser
BSI
Godesberger Allee 185-189
53133 Bonn
gerhard.schabhueser@bsi.bund.de

MinDir
Martin Schallbruch
BMI
IT-Direktor und CIO
Alt-Moabit 101d
10559 Berlin
martin.schallbruch@bmi.bund.de

Prof. Dr. Heinz Thielmann
Geschäftsführer
Emphasys GmbH
Eichenstr. 11
90562 Heroldsberg
heinz.thielmann@t-online.de

Eva Wiesmüller
CEO
power2progress
Eversbuschstr. 251
80999 München
info@power2progress.de

Robert Woithe
Geschäftsführer Technik
Toll Collect GmbH
Linkstr. 4
10785 Berlin
robert.woithe@toll-collect.de
Toru Kumagai
Freier Journalist
Margarete-Danzi-Str. 12
80639 MünchenF 134014
Box_1@tkumagai.de