Bundesamt
für Sicherheit in der
Informationstechnik

Mit Sicherheit.

BSI Jahresbericht 2010

De-Mail-Dienste
Technische Rahmenbedingungen und Prüfinfrastruktur

Cloud Computing
Herausforderung für die Informationssicherheit

Kritische Infrastrukturen
Bedrohungen außerhalb klassischer IKT-Infrastrukturen

Mit Sicherheit.

BSI Jahresbericht 2010

IT-Sicherheit

[engl. ai'ti: – (für information technology)]
Abkürzung für Informationstechnik- bzw. Informationstechnologie-Sicherheit, bezeichnet als Oberbegriff einen Zustand, wonach IT-Systeme frei von Risiken oder Beeinträchtigungen sind. Sicherheit ist möglich, wenn Gefahren im Vorfeld erkannt und beseitigt werden. Hauptaufgabe ist es daher, Bedrohungen durch entsprechende Schutzmaßnahmen entgegenzuwirken und so eventuellen Schäden vorzubeugen.

Brockhaus

Hans-Peter Friedrich
Bundesminister des Innern

Liebe Leserinnen und Leser,

vor 20 Jahren wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) gegründet. Rückblickend war es eine zukunftsweisende Entscheidung, das BSI zu errichten.

Heute ist das Internet aus unserem Alltag nicht mehr wegzudenken. Es hat nicht nur unsere Kommunikation verändert, sondern auch neue Formen des Zusammenarbeitens und Zusammenlebens geschaffen. Internetbasierte Geschäftsmodelle sind wesentlich für Produktivitätssteigerung und Wirtschaftswachstum. Die Entwicklung ist noch nicht am Ende: Flugzeuge, medizinische Produkte, Stromzähler und vieles mehr werden zukünftig mit dem Internet verbunden sein.

Sowohl für die Bürgerinnen und Bürger als auch für die Wirtschaft und die Verwaltung ergeben sich daraus zahlreiche neue Chancen und Möglichkeiten. Der Schlüssel für eine erfolgreiche Nutzung des Cyber-Raums ist Vertrauen – Vertrauen in die Sicherheit und in die Verfügbarkeit des Internets, nicht nur in Deutschland, sondern weltweit.

Das BSI ist durch seine Kompetenz als zentraler IT-Sicherheitsdienstleister innerhalb und auch außerhalb der Bundesverwaltung zu einem wichtigen Partner und damit zu einem Vertrauensgeber geworden. Wir haben in den letzten Jahren die Befugnisse des BSI gestärkt und das BSI auch zu einem wichtigen Ansprechpartner national und international tätiger Unternehmen gemacht.

International anerkannt als Kompetenzträger für IT-Sicherheit, wird das BSI in den nächsten Jahren das Innovationstempo des Internets weiter mitgehen müssen. Aufklärung über die Gefahren des Internets und das schnelle Reagieren auf entdeckte Schwachstellen werden eine noch intensivere Vernetzung des BSI zu anderen Behörden, in die Wirtschaft und im internationalen Bereich notwendig machen.

Ich wünsche Ihnen bei der Lektüre des Berichts viel Freude und viele Denkanstöße für eine sichere Nutzung des Cyber-Raums.

Berlin, im Juli 2011

Hans-Peter Friedrich

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Liebe Leserinnen und Leser,

das BSI ist dem Teenager-Alter entwachsen. Mit nunmehr 20 Jahren sind wir zwar eine verhältnismäßig junge Behörde, wie bei kaum einer anderen öffentlichen Institution unterliegt unsere Thematik IT-Sicherheit aber einer Dynamik, die unser Aufgabenspektrum seit der Gründung konstant erweitert hat.

Das Jahr 2010 war keine Ausnahme: Mit der Umsetzung des BSI-Gesetzes haben wir Neuland betreten. Lange Zeit hatte das BSI zwar eine Vielzahl von Aufgaben, jedoch kaum Befugnisse. Mit der neuen gesetzlichen Grundlage sind wir für die Zukunft als Abwehrbehörde nun besser aufgestellt. Das ist wichtig, denn auch für Sicherheitsexperten wird die Arbeit zunehmend zu einem Wettlauf, den sie sich mit den mittlerweile hoch professionellen Angreifern liefern.

Zuversichtlich macht uns die sich stetig verbessernde Kooperation zwischen IT-Herstellern, Providern und Sicherheitsexperten. Sie alle haben erkannt, dass gemeinschaftliches Handeln einen Gewinn für alle Beteiligten bedeutet. Und so sind immer wieder Erfolge für die IT-Sicherheit auf nationaler und internationaler Ebene zu verzeichnen. Nicht nur das Internet lässt Grenzen verschwinden, auch Bedrohungen lassen die Handelnden enger zusammenstehen, und das öffentliche Bewusstsein wird geschärft. Stuxnet war im Jahr 2010 das wohl einprägsamste Beispiel. Die Schadsoftware machte sehr deutlich, dass Angriffe inzwischen auch gezielt auf spezielle Unternehmens- und Prozesssteuerungssoftware ausgerichtet werden. Von einem „Cyberwar“ war weltweit die Rede. Diese Entwicklung wird auch im politischen Umfeld aufgenommen, und entsprechende Maßnahmen wurden bereits öffentlich angekündigt. So hat das Nationale Cyber-Abwehrzentrum unter der Federführung des BSI am 1. April 2011 seine Arbeit aufgenommen.

Weitere Ereignisse waren in vielerlei Hinsicht spannend: Die Einführung des neuen Personalausweises (nPA) am 1. November 2010 markierte den vorläufigen Höhepunkt eines technisch und organisatorisch ambitionierten IT-Projekts, in welches das BSI von Beginn an eingebunden war und zu dessen Erfolg es maßgeblich beigetragen hat. Am 3. Mai 2011 ist das De-Mail Gesetz in Kraft getreten, welches den Weg für die Einrichtung einer sicheren Kommunikationsinfrastruktur für Bürger, Unternehmen und Verwaltung ebnet.

Doch auf Erfolgen darf man sich nicht ausruhen, man muss sie ständig hinterfragen. Meine Mitarbeiter und ich tun genau dies mit dem Ziel, die vernetzte Welt für uns alle sicherer zu gestalten. Ich freue mich, Ihnen mit dem Jahresbericht 2010 einen Einblick in die Arbeit des BSI geben zu können und wünsche Ihnen eine interessante Lektüre.

Bonn, im Juli 2011

Michael Hange

Seite 13
Ganzheitliche Cyber-Sicherheit

Seite 18
De-Mail-Dienste: Technische Rahmenbedingungen und Prüfinfrastruktur

Seite 26
Cloud Computing – Herausforderung für die Informationssicherheit

Weichen stellen – Zukunft planen

IT-Sicherheit gestalten

Sicherheit für die Cyberwelt

Seite 44
BSI macht sicher mobil

Seite 48
Der neue Personalausweis

Seite 60
Karriere und öffentlicher Dienst

Kommunizieren – mobil und geschützt

Sichere elektronische Identitäten

Herausforderungen gemeinsam angehen

20 Jahre BSI

Weichen stellen – Zukunft planen

„Wir können unsere Rolle viel wirksamer wahrnehmen als früher.“

Das BSIG in der Umsetzung

Interview mit Horst Samsel, Abteilungsleiter Zentrale Aufgaben und Leiter der „Projektgruppe BSIG neu“, und Fabian Hodouschek, Referent und Mitglied der „Projektgruppe BSIG neu“

Am 20. August 2009 trat das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, kurz auch BSI-Gesetz (BSIG), in Kraft. Mit dem Gesetz wurde das Spektrum der Aufgaben und Befugnisse des BSI deutlich erweitert. Wir werfen einen Blick darauf, welche Veränderungen sich für das BSI ergeben haben und wie die Umsetzung der rechtlichen Rahmenbedingungen in der Praxis realisiert wurde. Als Abteilungsleiter Zentrale Aufgaben war Horst Samsel Leiter der „Projektgruppe BSIG neu“ und mit der Implementierung der gesetzlichen Anforderungen im BSI betraut. Fabian Hodouschek hat als Mitglied dieser Projektgruppe maßgeblich an der Umsetzung mitgewirkt.

Herr Samsel, das neue BSIG markiert einen Wendepunkt für die Informationssicherheit. Setzt sich dieser Eindruck auch in der täglichen Arbeit im BSI fort?

Samsel: Auf der Grundlage des bisherigen Gesetzes konnte das BSI bei der Cybersicherheit und der Netzverteidigung nur sehr vorsichtig agieren. Basis unseres Handelns waren beispielsweise einzelne Dienstvereinbarungen, die in den einzelnen Behörden abgeschlossen wurden. Mit dem neuen BSI-Gesetz wurden unsere Möglichkeiten deutlich erweitert, Gefahren für die Kommunikationstechnik des Bundes abzuwehren und dementsprechende technische Schutzmaßnahmen zu treffen. Beispielsweise haben wir das Schadprogramm-Erkennungsystem, kurz SES, und das Schadprogramm-Präventionssystem, abgekürzt SPS, etabliert. Indem wir diese Systeme auf Basis der gesetzlichen Grundlage einsetzen, können wir den Schutz der Regierungsnetze effektiver bewerkstelligen. Im Vergleich zu früher kann das BSI jetzt mit Hilfe der gesetzlichen Befugnisse selbständiger handeln und damit auf veränderte Bedrohungen besser reagieren.

Werden die Aufgaben des BSI auch seitens der Politik noch stärker wahrgenommen?

Samsel: Unsere Arbeit wird jetzt deutlich mehr von der Politik wahrgenommen. Beispielsweise

müssen wir nach § 5 Abs. 10 BSIG dem Bundestags-Innenausschuss jährlich Bericht zu den Tätigkeiten des BSI nach § 5 BSIG (Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes) erstatten. Hierbei geht es um konkrete Erkenntnisse bezogen auf die Bedrohungssituation und Angriffsszenarien. Im übertragenen Sinn stand das BSI bis 2009 an den Schnittstellen zu den Netzen des Bundes gewissermaßen mit verbunden Augen und gefesselten Händen da. Jetzt haben wir die Möglichkeit, tatsächlich dort tätig zu sein. Auch dadurch rücken die mit IT und Internet verbundenen Risiken stärker in den Fokus der Politik.

„Im Vergleich zu früher kann das BSI mit Hilfe der gesetzlichen Befugnisse selbstständiger handeln und damit auf veränderte Bedrohungen besser reagieren.“

Horst Samsel

Gemäß § 4 BSIG ist das BSI zentrale Meldestelle für die Sicherheit in der Informationstechnik. Was bedeutet das in der Praxis?

Samsel: In diesem Punkt erfolgte die Umsetzung der gesetzlichen Grundlage in praktische Arbeitsabläufe am schnellsten. Laut Gesetz haben die Behörden des Bundes bezüglich IT-Sicherheitsvorfällen eine Unterrichtungspflicht gegenüber dem BSI. Bereits zum Jahreswechsel 2009/2010 konnten wir eine entsprechende Verwaltungsvorschrift vorlegen, in der diese Meldepflichten erläutert sind. Es geht in erster Linie darum, dass das BSI Schaden von den Behörden fernhält, indem wir Gefahren für die Kommunikationstechnik des Bundes abwehren. Ohne unsere Schutzmaßnahmen, beispielsweise gegen die Spamflut auf die Regierungsnetze, hätte jeder Bundesbedienstete im Schnitt 20.000 E-Mails pro Monat zu bearbeiten. Bis zu 99 Prozent der E-Mails, die die Bundesverwaltung erreichen, sind Spam.

Das Gesetz verlangt ausdrücklich, datenschutzrechtliche Belange zu berücksichtigen. Wie schlägt sich das in der Umsetzung nieder?

Samsel: Die Grundlage für den Einsatz der Schutzsysteme bildet das Datenerhebungs- und -verwendungskonzept, das zwischen den Fachreferaten im BSI, dem Justiziariat und der Datenschutzbeauftragten des BSI erörtert und vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit geprüft wurde. Das Schadprogramm-Erkennungssystem überprüft automatisiert den E-Mail-Verkehr an der Schnittstelle zur Kommunikationstechnik des Bundes. Die Kriterien, wer wann in dieses System reinschauen darf, sind sehr genau geregelt. Das SES ist übereinstimmend mit den gesetzlichen Anforderungen so aufgebaut, dass die Fälle, in denen tatsächlich ein Mensch Kenntnis vom Inhalt einer Kommunikation erhalten muss, so gering wie möglich gehalten werden. Solche Fälle müssen exakt protokolliert und von einem Bediensteten des BSI mit der Befähigung zum Richteramt angeordnet werden. Über entsprechende Vorschriften und Sicherheitsvorkehrungen, die Systeme und Mitarbeiter betreffen, ist ein Höchstmaß an Regularien umgesetzt, um unberechtigte Zugriffe auszuschließen.

Gegen § 5 BSIG wurde Mitte 2010 Verfassungsbeschwerde eingereicht. Wie beurteilen Sie das?

Samsel: Im Gesetzgebungsverfahren wurden die Frage etwaiger Grundrechtseingriffe intensiv beraten, sodass die geltende Vorschrift des § 5 ausgewogen ist. Für die Anwendungsbereiche des BSIG, in denen das Fernmeldegeheimnis oder das Recht auf informationelle Selbstbestimmung betroffen sein könnten, hat man Regelungen entwickelt, um Eingriffe auf das absolut notwendige Maß zu beschränken. Dem Grundsatz der Verhältnismäßigkeit ist hier Rechnung getragen worden. Es wird nicht sorglos mit den Daten umgegangen.

„Der Bedarf an Personenzertifizierungen steigt an, was teilweise auch aus anderen Gesetzen resultiert."

Fabian Hodouschek

§ 5 Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes

(1) Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes

1. Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist,
2. die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist.

Das BSIG stattet das BSI mit der Kompetenz aus, Wirtschaft und Bürger vor Sicherheitslücken in Produkten und Diensten zu warnen.

Hodouschek: Auch bei der Umsetzung des § 7, der die Thematik der Warnungen betrifft, sind wir sehr zügig voran gekommen. Wir haben einen detaillierten Prozess definiert, was zu geschehen hat, bevor eine Warnung vor einer öffentlichkeitsrelevanten IT-Sicherheitslücke ausgesprochen wird. Dies beinhaltet grundsätzlich auch die Einbeziehung des Herstellers eines betroffenen Produkts.

Wie reagieren die Hersteller auf Warnungen des BSI, die ihre Produkte betreffen?

Hodouschek: Wir haben 2010 in einigen Fällen Warnungen aussprechen müssen, die auch von den Medien prominent aufgegriffen wurden. Seitens der betroffenen Hersteller wurde dies natürlich kritisch gesehen, bislang wurden aber in keinem Fall rechtliche Schritte dagegen eingeleitet. Da die Hersteller vorab informiert werden, bestand noch kein Fall, wo eine Warnung des BSI den Hersteller unvorbereitet getroffen hat.

Samsel: An der Reaktion der Hersteller sieht man, wie wichtig die Befugnis aus § 7 für das BSI ist. Wir können jetzt unsere Rolle viel wirksamer wahrnehmen als früher. Wir wurden zwar auch vorher seitens der Hersteller ernst genommen, die Zusammenarbeit von deren Seite ist jedoch deutlich besser geworden. Wir führen das darauf zurück, dass das BSI sozusagen Zähne bekommen hat. Hersteller kommen deutlich früher auf uns zu und suchen die Kooperation. Ein Beispiel war Stuxnet: Hier wurde keine Pauschalwarnung ausgesprochen, sondern das Vorgehen sehr eng und verantwortungsvoll mit dem Hersteller abgestimmt.

Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende Aufgaben wahr: [...] Beratung und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen; § 3 Absatz 1 Satz 2 Nummer 14.

Zum Schutz der Regierungsnetze darf das BSI einheitliche und strenge Sicherheitsstandards für die Bundesbehörden definieren und sogar geeignete Produkte entwickeln lassen.

Samsel: So beschreibt es § 8 des BSIG. Gleichzeitig weist dieser dem BSI die Befugnis zu, IT-Sicherheitsprodukte für den Bund bereitzustellen. Durch das zeitgleich anlaufende IT-Investitionsprogramm des Bundes konnten IT-Sicherheitsprodukte wie SINA, SiMKo oder SecuVOICE in der Bundesverwaltung ausgerollt werden. So war es möglich, IT-Sicherheit viel schneller und auch zielgerichteter in die Fläche zu bringen, als wenn wir die Entwicklung lediglich begleitet bzw. Zulassungen oder Zertifizierungen ausgesprochen hätten und die Behörden selbst für die Umsetzung zuständig gewesen wären.

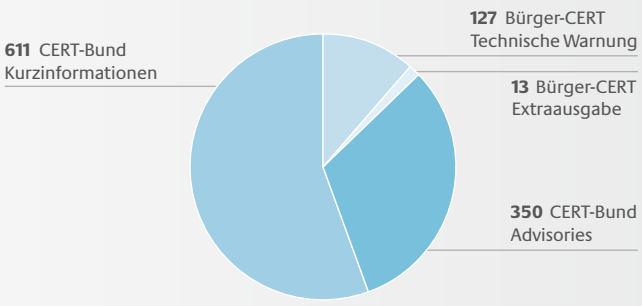
Derzeit setzen 180 deutsche Behördenkunden SINA-Systeme ein. 23 Behörden verwenden derzeit die SINA Virtual Workstation. SiMKo kommt bei über 30 Behörden zum Einsatz.

2010 haben wir sehr engagiert mit dem Beschaffungsamt des Bundesministeriums des Innern zusammengearbeitet und konnten einige Rahmenverträge abschließen. Daraus können die Bundesbehörden unmittelbar ihren Bedarf an Produkten mit IT-Sicherheitseigenschaften abrufen, und wir können damit die Anforderungen für die IT-Sicherheit vorgeben. Rahmenverträge sollen künftig weiter ausgebaut werden.

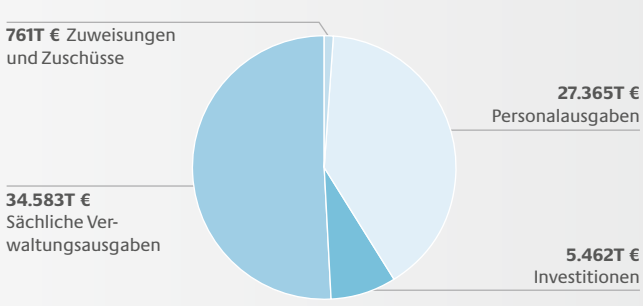
Weckt das nicht auf Seiten der Hersteller allerlei Begehrlichkeiten?

Hodouschek: Im Grunde ist das eine Bedarfsbündelung, die sich auch auf den Markt auswirkt. Wir wollen letztlich eine Bedarfsdeckung für die Bundesverwaltung im Hinblick auf Produkte mit den angemessenen Sicherheitseigenschaften gewährleisten. Begehrlichkeiten der Hersteller gibt es sicherlich – diese spielen bei der Auswahl der Produkte aber keine Rolle.

Warnungen des CERT-Bund in 2010



Haushaltsvolumen des BSI 2010: 68.171T €



Wie werden diese Vorgaben innerhalb der Bundesverwaltung aufgenommen?

Samsel: Besser als früher: IT-Sicherheit ist für viele Behörden tendenziell eher eine lästige Geschichte, weil sie einerseits in dem Ruf steht, die Funktionalität und die Performance zu beeinträchtigen und zudem zahlreiche Vorgaben zu beachten sind. Der Abruf von IT-Sicherheitsprodukten aus einem Rahmenvertrag, bei denen die Standards des BSI berücksichtigt sind, ist einfacher, als die Haushalts- und Arbeitsmittel selbst zu beschaffen. Damit wird IT-Sicherheit bequemer. Die Vorbehalte bezüglich Funktionalität und Performance sind zwar nicht verschwunden, aber es können weitere negative Rahmenbedingungen beseitigt. Auf diese Weise lässt sich die Akzeptanz erhöhen.

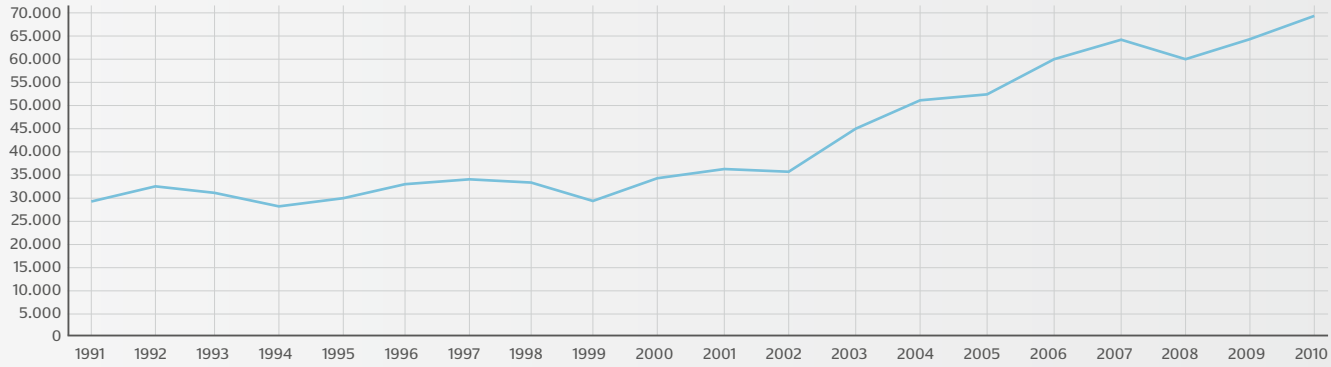
Seit Inkrafttreten des BSIG darf das BSI auch Personen zertifizieren. Wie funktioniert hier die Umsetzung?

Hodouschek: Die Umsetzung der Personenzertifizierung stellt kein großes Problem dar, weil das BSI bereits seit längerem im Bereich der Zertifizierung tätig ist und auch schon Personen beurteilt hat. Die Prozesse sind vergleichbar. Der Bedarf an Personenzertifizierungen steigt an, was teilweise auch aus anderen Gesetzen resultiert, nach deren Vorgabe eine BSI-Zertifizierung erforderlich ist. Diese Fälle nehmen zu und die Verfahren laufen. In der Zertifizierungspraxis ist das für uns nichts wesentlich Neues. Ein ständiger Lernprozess hingegen ist, wie die Zertifizierungen extern aufgenommen werden. Die bisherigen Erfahrungen sind jedoch positiv.

Erfordern die erweiterten Befugnisse auch strukturelle Änderungen innerhalb der Organisation des BSI?

Samsel: Veränderte Aufgaben und neue Befugnisse schlagen sich natürlich auch organisatorisch nieder. Weitergehende Aufgaben lassen die externen Schnittstellen stärker sichtbar werden. Speziell die neuen Befugnisse aus § 5 oder § 8, die man in der Organisation des BSI bislang nicht klar verortet hatte. Dies werden wir bei der Neuorganisation des BSI, mit der wir uns gerade befassen, berücksichtigen. In anderen Bereichen, die es bereits vor der Novellierung des Gesetzes gab – wie etwa das CERT-Bund oder Akkreditierung und Zertifizierung – wird es weniger Neuerungen geben.

Entwicklung des Haushaltsvolumen (in T€)



Ganzheitliche Cyber-Sicherheit

Dr. Hartmut Isselhorst, Abteilungsleiter Cyber-Sicherheit

Das Internet ist heute unverzichtbar. Sämtliche Bevölkerungskreise von Jung bis Alt nutzen das Internet für Informationsrecherchen, für E-Commerce und Homebanking, für E-Government, für Online-Spiele und soziale Netzwerke. Auch Verwaltung, Wirtschaft und Forschung haben im Internet ihre Präsenzen und bieten Leistungen an, nutzen es aber auch als Kommunikationsplattform und für mobiles Arbeiten.

Massenangriffe und gezielter Missbrauch

Die Omnipräsenz des Internets hat aber auch eine Kehrseite. Die Abhängigkeit von seiner Funktionsfähigkeit ist enorm gewachsen, viele Prozessketten würden ohne das Internet zusammenbrechen. Mit dem Erfolg wuchs außerdem das Interesse im Bereich Kriminalität sowie ausländischer staatlicher Stellen, das Internet zukünftig

„Es gilt, für die Zukunft die Herausforderung ‚Cyber-Sicherheit für Deutschland' anzunehmen."

Dr. Hartmut Isselhorst

vielleicht auch im Bereich Terrorismus als Plattform für Angriffe zu nutzen. Zugute kommt diesen Angreifern, dass sie aufgrund der Komplexität der Software sowie durch ihre großen Ressourcen in der Lage sind, Fehler und Schwachstellen zu finden und in Kombination mit den alltäglichen Diensten des Internets für Angriffe zu missbrauchen.

So werden

- Webseiten mit Schadprogrammen präpariert, sodass das einfache Surfen auf diesen Seiten dazu führt, die Kontrolle über den eigenen Rechner zu verlieren (Drive-by-Downloads),
- massenhaft oder auch nur gezielt an wenige Adressaten E-Mails versendet, denen manipulierte Dateien (Office-Dateien, PDF-Dateien, Bilddateien etc.) anhängen, die wiederum über Softwarefehler zum Kontrollverlust über den eigenen Rechner führen (Trojanische Pferde),
- massenhaft PCs im globalen Internet attackiert und deren Kontrolle übernommen und zentral ferngesteuert (Botnetze),
- mit Botnetzen milliardenfach unerwünschte E-Mails (Spam) versendet, die viele Server nutzlos belasten und
- mit Botnetzen auch gezielt Server von Firmen und Behörden völlig überlastet, sodass der Dienst nicht mehr verfügbar ist (Distributed Denial of Service-Angriffe – DDoS).

In Folge dieser Massen- beziehungsweise gezielten Angriffe, beides Bestandteile sogenannter Cyber-Attacken, können digitale Identitäten entwendet und anschließend missbraucht werden, vertrauliche Informationen ausgespäht oder auch IT-gestützte Prozesse sabotiert werden.

All diesen neuen Gefährdungen sieht sich die Bundesverwaltung natürlich auch ausgesetzt. Mit der Novelle des BSIG hat der Gesetzgeber dem BSI nunmehr die Möglichkeit gegeben, den Schutz der Bundesverwaltung durch zentrale Maßnahmen zu realisieren.

Maßnahmen zum Schutz der Bundesverwaltung

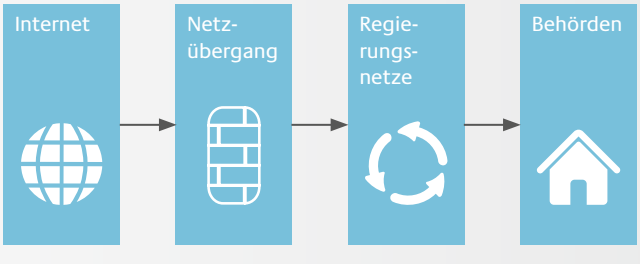
Die Cyber-Sicherheitsstrategie des BSI zum Schutz der Bundesverwaltung setzt dabei auf zwei Leitsätze:

- Cyber-Attacken möglichst früh erkennen und abwehren sowie
- Cyber-Attacken eine gestaffelte Phalanx von Schutzmaßnahmen entgegensetzen.

Der vom BSI präferierte ganzheitliche Cyber-Sicherheitsansatz setzt dies durch vier abgestufte Abwehrbereiche um:

- das Internet selbst
- Netzübergänge vom Internet in Regierungsnetze
- Regierungsnetze selbst
- lokale Netze und Arbeitsplatzrechner.

„Vier-Wall-Strategie"



Cyber-Abwehrbereich Internet

Die Cyber-Sicherheitsaktivitäten des BSI im Themenbereich Internet lassen sich in vier Teilbereiche aufteilen. Im Teilbereich „Lage“ arbeitet das BSI-CERT mit anderen nationalen und internationalen CERTs zusammen, um IT-Vorfälle zu erkennen, zu bewerten und zu beheben. Das dazugehörige Lagezentrum beobachtet hierfür die nationale und internationale IT-Lage und leitet ggf. die notwendigen Krisenreaktionsmechanismen in die Wege. Bei Bedarf werden nach BSIG § 7 öffentliche Warnungen vor Schwachstellen und Schadprogrammen ausgesprochen. Dabei arbeiten das BSI-CERT und das Lagezentrum unmittelbar mit Betreibern Kritischer IT-Infrastrukturen in Deutschland zusammen. Um im IT-Krisenfall angemessen reagieren zu können, werden zusätzlich regelmäßig IT-Krisenübungen durchgeführt.

Im Teilbereich „Internetinfrastruktur“ arbeitet das BSI mit den Betreibern des Internets, dem eco-Verband und den nationalen Internetprovidern zusammen, um die Grundstrukturen und Internetdienste sicherheitstechnisch zu verbessern. Hier sei exemplarisch die Initiative zur Einführung des sicheren DNS-Dienstes (DNSsec) genannt. Mit den Global Playern auf Produktseite kooperiert das BSI, um sicherheitstechnische Produktanalysen durchzuführen und im Vorfeld des Produkteinsatzes sicherheitsrelevante Verbesserungen zu initiieren.

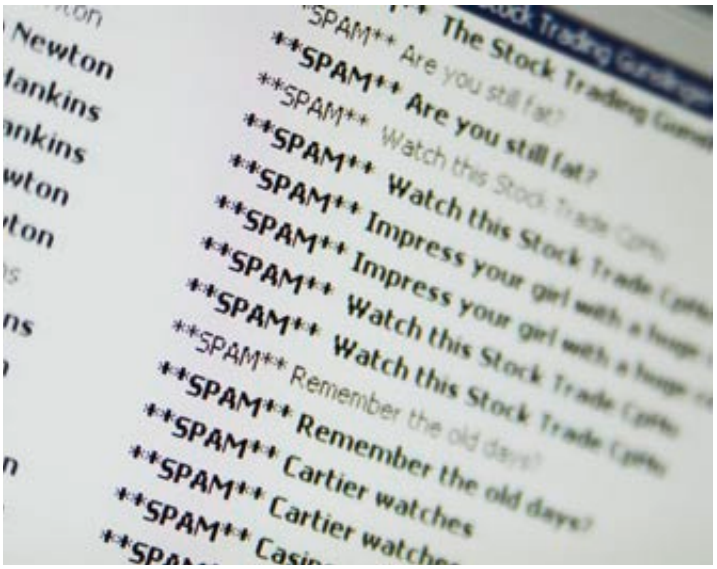
Im Teilbereich „Bürger“ unterstützt das BSI die deutschen Privatanwender des Internets, ihre Rechner besser abzusichern. Denn gerade ungesicherte Privat-PCs stellen im gekaperten Zustand (Botnetz) die virtuelle Armee im Sabotage-Kampf der Cyber-Attacken dar. Das BSI stellt über die Webseite „BSI-fuer-Buerger“ notwendige Informationen und Tools zur Verfügung und warnt über das Bürger-CERT vor aktuellen Gefährdungen. Weiterhin begleitet das BSI die Bereitstellung von sicheren Basistechnologien für die sichere Nutzung des Internets, wie es zum Beispiel der neue Personalausweis für sichere digitale Identitäten und das DE-Mail-Konzept für sichere E-Mail-Kommunikation sind. Und sollte trotz aller Bemühungen ein Privat-PC gekapert worden sein und als „Bot“ kriminell zweckentfremdet werden, so hilft die vom BSI initiierte und begleitete Anti-Botnetz-Initiative des eco - Verband der deutschen Internetwirtschaft e.V., in der die Internetprovider ihren betroffenen Kunden Hilfestellung leisten.

Im vierten Teilbereich „Bundesverwaltung im Internet“ sind insbesondere zwei Aktivitäten für den Schutz der Internetnutzung der Bundesverwaltung zu nennen:

- Mit den Internetprovidern des Regierungsnetzes wurden vertraglich Sicherheitsmechanismen vereinbart, die im Fall eines DDoS-Angriffs greifen, um den Angriff abzuwehren bzw. mindestens abzumindern.
- Da auch die Webserver der Bundesverwaltung selbst angegriffen werden, werden ausgewählte Webserver des Bundes einer permanenten Kontrolle unterzogen, um schnellstmöglich Schwachstellen oder Schadprogramme zu detektieren und zu eliminieren.

Cyber-Abwehrbereich Netzübergang Internet-Regierungsnetz

An der Schnittstelle des Regierungsnetzes zum Internet verantwortet das BSI die klassischen Cyber-Sicherheitsmaßnahmen wie den Spam-Filter, der über 95 Prozent der eingehenden E-Mails als Spam aussondert, den kaskadierten Virenfilter, der weitverbreitete Schadprogramme erkennt und eliminiert, sowie die Firewall, die klassische Hacking-Angriffe verhindert.



Über 95 Prozent der eingehenden E-Mails werden vom Spam-Filter an der Schnittstelle des Regierungsnetzes ausgesondert

Aufgrund der Befugnisse im novellierten BSI-Gesetz kann das BSI an dieser Schnittstelle zusätzlich höherwertige Schutzmaßnahmen realisieren:

» Das Schadprogramm-Erkennungs-System SES: Mit diesem innovativen System ist es dem BSI gelungen, im Jahr 2010 über 1600 gezielte Spionageangriffe mittels Trojanischer Pferde zu identifizieren und abzuwehren.
» Das Schadprogramm-Präventions-System SPS: Damit konnte das BSI im Jahr 2010 über 300.000 Zugriffsversuche auf höchst gefährliche Webseiten verhindern.

Cyber-Abwehrbereich Regierungsnetz

Das sicherheitstechnisch vom BSI verantwortete Regierungsnetz zwischen Berlin und Bonn ist sowohl bezüglich Verfügbarkeit als auch Vertraulichkeit gehärtet. Dazu zählt die durchgängig redundante Auslegung des Netzes und die redundante Anbindung ans Internet. Als wesentlicher Vorteil hat sich herausgestellt, dass das Regierungsnetz nur zwei hochverfügbare Übergänge ins Internet hat. Damit ist es möglich, diese Übergänge unter sicherheitstechnischer Kontrolle zu halten und dort gezielt die oben genannten Sicherheitsmaßnahmen zu realisieren.

Als weiteres Sicherheitsmerkmal ist die Trennung von Sprach- und Datenübertragung zu nennen, um bei einem eventuellen Ausfall eines Übertragungswegs noch eine andere Kommunikationsmöglichkeit zu haben. Zum Schutz der Vertraulichkeit ist die gesamte Kommunikation im Regierungsnetz verschlüsselt. Dazu werden vom BSI entwickelte, für den staatlichen Verschlusssachenbereich zugelassene Kryptosysteme eingesetzt. Abgerundet wird die Sicherheit des Regierungsnetzes durch die permanente redundante Überwachung durch den Betreiber wie auch durch das Lagezentrum im BSI. Zusätzlich finden regelmäßig IT-Sicherheitsrevisionen und Penetrationstests statt.

Cyber-Abwehrbereich Lokale Netze und Arbeitsplatz-Rechner

Zur Absicherung der lokalen Netze und Arbeitsplatz-PCs in den Bundesbehörden stellt das BSI Empfehlungen wie die Schriftenreihe Internetsicherheit, die IT-Grundschutz-Kataloge und das Hochverfügbarkeitskompendium bereit. Darüber hinaus stehen die Warnmeldungen des BSI-CERT zur Verfügung, das auch die zentrale Meldestelle für Sicherheitsvorfälle des Bundes nach dem BSI-Gesetz ist. Sicherheitsberatung, Penetrationstests und IT-Sicherheitsrevisionen mit der Spezialausprägung des Cyber-Sicherheit-Quickchecks sind ergänzende Dienstleistungen. Abgerundet wird dies mit der Bereitstellung geeigneter Produkte (Firewalls, Viren-Schutzprogramme, Kryptoprodukte, sichere USB-Sticks) und der Konzeption und Entwicklung von Cyber-Sicherheitsprodukten wie Anomalie-Detektoren, Datenträgerschleusen, sichere Surfumgebungen auf Basis virtueller Systeme und sichere Lösung für Mobilkommunikation und mobiles Arbeiten.

Ausblick:

Nachdem das BSI in den letzten zwei Jahren gute Erfahrungen für die Bundesverwaltung gewonnen und Cyber-Sicherheit erfolgreich umgesetzt hat, gilt es, auch für die Zukunft, die Herausforderung „Cyber-Sicherheit für Deutschland“ anzunehmen. In dieser Dimension wird das BSI neue Cyber-Abwehrbereiche erschließen und bestehende Bereiche ausweiten müssen.

Im Cyber-Abwehrbereich „Internet“ werden die potenziellen Angriffe auf die Internetinfrastruktur bewertet, beobachtet und abgewehrt werden müssen. Dazu zählen insbesondere Angriffe auf die DNS-Strukturen, Angriffe mittels manipulativen Routings und hochkapazitäre DDoS-Angriffe auf nationale Internetstrukturen.

Große Bedeutung wird der Cyber-Kooperationsbereich haben. „Cyber-Sicherheit für Deutschland“ kann nur durch die intensive Kooperation aller Akteure erreicht werden. Dazu zählen:

» Zusammenarbeit der im Bereich Cyber-Sicherheit aktiven Bundesbehörden: 2011 wird das Nationale Cyber-Abwehrzentrum unter Federführung des BSI etabliert.

Das BSI setzt Cyber-Sicherheit erfolgreich um

Um die Cyber-Sicherheit in der Wirtschaft zu fördern, wird das BSI im Rahmen der Hilfe zur Selbsthilfe die Wirtschaft unterstützen. Derzeit sind drei Bereiche geplant:

- Best Practices: Gemeinsam mit der Wirtschaft wird das BSI die Best Practices für Cyber-Sicherheit, differenziert nach dem Schutz vor Cyber-Sabotage und Cyber-Spionage, erarbeiten. Um die Ergebnisse und Erfahrungen zur Verfügung zu stellen, ist ein Webportal zur Cyber-Sicherheit geplant.
- Schulungszentrum: Im Aufbau begriffen ist ein Schulungszentrum, in dem IT-Administratoren für die Abwehr von Cyber-Angriffen geschult werden sollen. Es gibt erste Überlegungen, dieses Schulungszentrum auch für die Wirtschaft zu öffnen.
- Zertifizierung von Cyber-Sicherheitsberatern und -Dienstleistern: Zukünftig werden fachkundige Berater und Dienstleister in größerer Zahl benötigt. Hierzu kann das BSI auf Grundlage des novellierten BSI-Gesetzes geeignete Anbieter prüfen und zertifizieren.

- Zusammenarbeit mit den Internetprovidern: Das BSI wird die begonnene Kooperation intensivieren und mit den Internetprovidern nach Möglichkeiten suchen, einerseits die Privatanwender-PCs zu sichern, andererseits aber auch für den Cyber-Sabotagefall nationalen Ausmaßes Handlungsoptionen zu eröffnen.
- Zusammenarbeit mit Herstellern von Cyber-Sicherheitsprodukten und Systemhäusern: In Kooperation mit den Herstellern wird das BSI geeignete Cyber-Sicherheitslösungen erarbeiten, Dienstleistungen initiieren und geeignete Anbieter motivieren.
- Zusammenarbeit mit der Wirtschaft: Um notwendige kooperative Prozesse der nationalen Cyber-Abwehr einzuüben, wird Ende 2011 eine Bund-Länder-übergreifende Übung unter Beteiligung der Betreiber Kritischer Infrastrukturen in der Wirtschaft durchgeführt (LÜKEX 2011).
- Internationale Zusammenarbeit: Cyber-Aggressoren (Cyber-Kriminelle, Cyber-Spione, Cyber-Terroristen) sind ein internationales Phänomen. Als Antwort ist eine intensive internationale Kooperation notwendig, um Erfahrungen, Erkenntnisse und Best Practices im Vorfeld auszutauschen sowie um im akuten Angriffsfall konzertiert verteidigen zu können.

Neue Herausforderungen stehen bevor

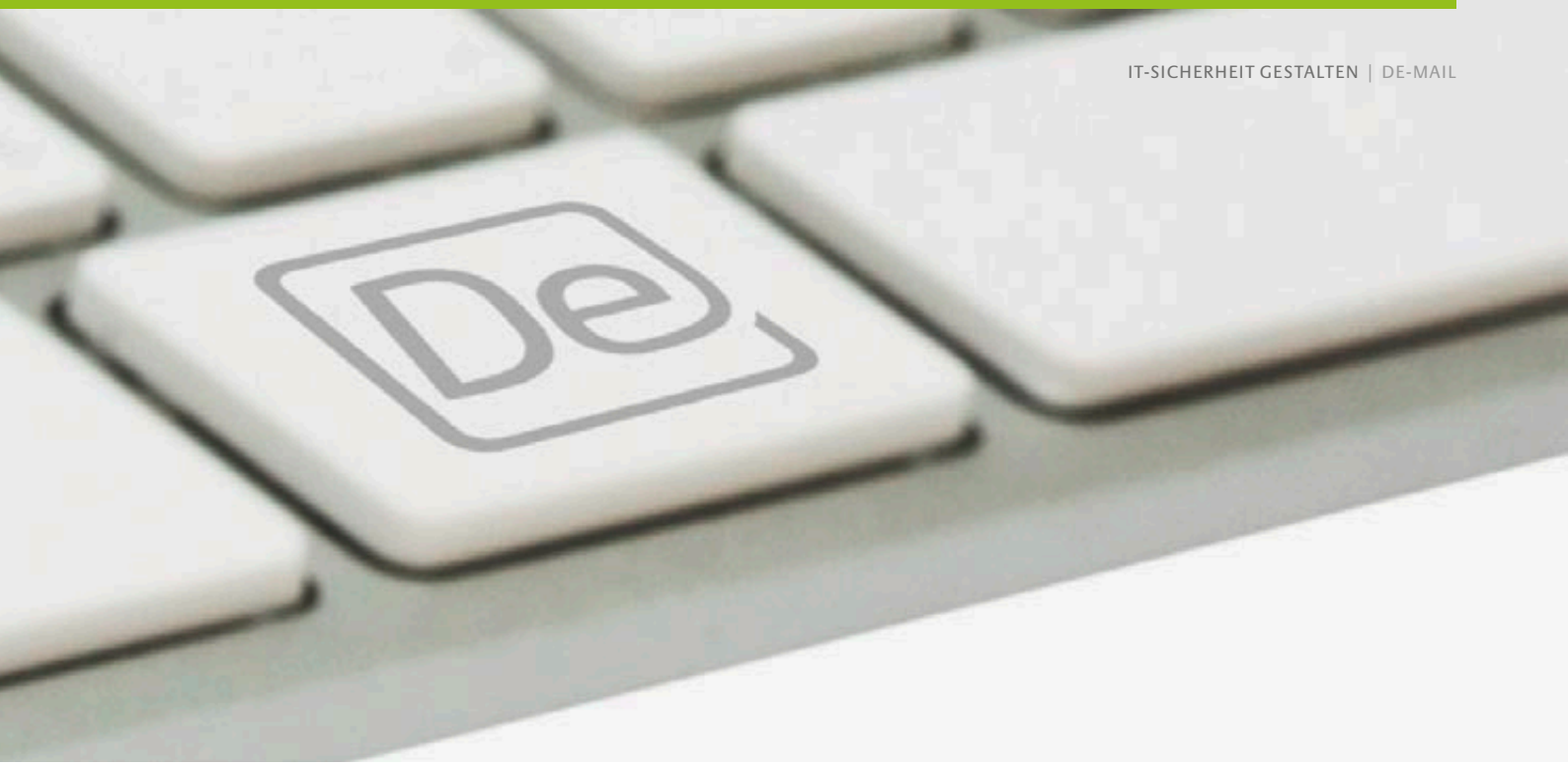
Jedoch ist die nächste Herausforderung schon erkennbar. Heute ist das Internet eine Plattform, die überwiegend durch PCs und Smartphones genutzt wird. Morgen ist das Internet ubiquitär, es wird in neue Bereiche Einzug halten: Kraftfahrzeuge und Flugzeuge werden mit dem Internet verbunden, medizinische Geräte in Arztpraxen und Krankenhäusern werden für Wartungszwecke einen Internetzugang benötigen, Stromzähler und Steuerungstechnik werden Internetzugang haben. Fehlfunktionen können hier große Schäden bis hin zu Gefahren für Leib und Leben verursachen. Schließlich nimmt die Abhängigkeit von einem funktionierenden Internet auch durch das Thema Cloud Computing weiter zu. Cyber-Sicherheit 2.0 wird dann ebenfalls nur ganzheitlich und kooperativ erreicht werden können.

IT-Sicherheit gestalten

De-Mail-Dienste: Technische Rahmenbedingungen und Prüfinfrastruktur

Dr. Astrid Schumacher, Projektleiterin De-Mail im BSI

Mit De-Mail wird das verbindliche und vertrauliche Versenden von Dokumenten und Nachrichten über das Internet möglich. De-Mail erhöht die Sicherheit der elektronischen Kommunikation. Dadurch erhält der De-Mail-Kontoinhaber ein Maximum an Sicherheit bei einem Minimum an Aufwand.



Das De-Mail Projekt – eine erfolgreiche Kooperation

De-Mail

So einfach wie E-Mail, so sicher wie Papierpost.

Durchgeführt wird das Projekt De-Mail federführend vom Bundesministerium des Innern. Das BSI ist für die technische Umsetzung verantwortlich, was sich insbesondere in der Entwicklung der Technischen Richtlinie De-Mail mit ihren einzelnen Modulen für die unterschiedlichen obligatorischen und optionalen Dienste niederschlägt.

Das Projekt De-Mail ist Bestandteil des Modernisierungsprogramms „Vernetzte und transparente Verwaltung" der Bundesregierung. Es steht in Übereinstimmung mit der Nationalen E-Government-Strategie. Zu den langjährigen Unterstützern zählen Verbände wie der BITKOM und die Arbeitsgruppe 3 „Innovative IT-Angebote des Staates", die anlässlich des Nationalen IT-Gipfels gegründet wurde. Zahlreiche KMUs, Banken und Versicherungen, für die die Realisierung einer vertraulichen und verbindlichen elektronischen Kommunikation in ihrem Geschäftsfeld von großem Interesse ist, hatten sich bereits am Pilotprojekt beteiligt. Aufgrund der positiven Rückmeldungen der Testnutzer und der hohen Nachfrage von Unternehmen und Behörden betreiben die an der Pilotierung beteiligten Provider seither ihre De-Mail-Systeme weiter. Zudem führen die Branchenprojekte durch, in denen die Beteiligten die Integration von De-Mail in ihre internen IT-Systeme und die zugrunde liegenden Geschäftsprozesse kennenlernen und einüben können.

Sicher ist sicher: De-Mail ermöglicht das verbindliche und vertrauliche Versenden von Dokumenten und Nachrichten über das Internet

Verschlüsselt – Authentisch – Nachweisbar

Die wesentlichen Sicherheitsziele Vertraulichkeit, Integrität und Authentizität der De-Mail-Kommunikation werden durch die im De-Mail-Gesetz vorgeschriebenen Maßnahmen gewährleistet.

Rechtliche Voraussetzung für die Akkreditierung und damit die Zulassung als De-Mail-Provider durch das BSI als zuständige Behörde ist das „Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften“, das am 3. Mai 2011 in Kraft getreten ist. Die Einführung von De-Mail kann nach Inkrafttreten des Gesetzes unmittelbar erfolgen. Mit De-Mail können die Identitäten der Kommunikationspartner sowie die Zustellung der De-Mails nachgewiesen werden. Die Inhalte einer De-Mail können auf ihrem Weg durch das Internet nicht mitgelesen oder gar verändert werden.

Der De-Mail-Diensteanbieter muss jedem Nutzer eine sichere Anmeldung bei seinem De-Mail-Konto ermöglichen, d.h. unter Nutzung zweier voneinander unabhängiger Sicherungsmittel wie Besitz (ein Token wie z. B. der neue Personalausweis oder ein Handy) und Wissen (ein Passwort oder z. B. eine PIN). De-Mails sind auf dem Transport verschlüsselt und können daher nicht von Dritten abgefangen und manipuliert werden. Wer darüber hinaus eine Ende-zu-Ende-Verschlüsselung wünscht, kann jederzeit die mit De-Mail übermittelten Inhalte selbst verschlüsseln. De-Mail vereinfacht dies, indem die Provider verpflichtet sind, die notwendigen öffentlichen Schlüssel auf Wunsch des Nutzers in einem Verzeichnisdienst zu veröffentlichen. Die Nachrichteninhalte werden bereits bei der normalen De-Mail-Kommunikation standardmäßig mit einem Hash integritätsgesichert. Bei allen Versand- und Eingangsbestätigungen werden die Nachrichten durch den Provider zusätzlich mit einer qualifizierten elektronischen Signatur versehen. Wer darüber hinaus jede Nachricht selbst qualifiziert signieren will, kann dies mit eigenen Komponenten beliebig ergänzen. Spam wird wirksam verhindert, weil Absender von De-Mails über die sichere Erstidentifizierung eindeutig bekannt sind. Hierfür kann auch der neue elektronische Personalausweis verwendet werden.

Die Technische Richtlinie De-Mail

Technische Richtlinien sind ein bewährtes Mittel, um Anwendern und Herstellern ein standardisiertes Format für die technischen Vorgaben an die Hand zu geben. Anwender werden so in die Lage versetzt, geprüfte Produkte für ihren Anwendungsbereich auszuwählen. Hersteller können ihre Produkte nach den hier getroffenen Empfehlungen spezifizieren und diese auf Konformität zu den vorgegebenen Spezifikationen prüfen lassen.

De-Mail-Anbieter müssen hohe Anforderungen u. a. an Sicherheit, Funktionalität und Interoperabilität erfüllen, die in der Technischen Richtlinie 01201 De-Mail näher spezifiziert sind. Beim BSI lag das Hauptaugenmerk 2010 darauf, die entsprechenden technischen Rahmenbedingungen sowie die Prüfinfrastruktur in den einzelnen Modulen der Technischen Richtlinie weiter zu konkretisieren und in diesem Rahmen auch das Gesetzgebungsverfahren zu begleiten. Auch 2010 erfolgte dies wiederum unter Einbindung der bereits involvierten künftigen De-Mail-Provider. Das BSI veröffentlicht die Kriterien auf seinen Webseiten bereits von Projektbeginn an. Die jeweils gültige Fassung der maßgeblichen Technischen Richtlinie ist online verfügbar. Zusätzliche Informationen können direkt beim BSI unter de-mail@bsi.bund.de angefragt werden.

Die BSI TR 01201 De-Mail stellt insgesamt das Rahmenwerk für die Nachweise in den Bereichen Funktionalität, Interoperabilität und Sicherheit dar. Sie beschreibt außerdem die Anforderungen, die De-Mail-Dienste erfüllen müssen, sowie die Anforderungen zur Prüfung dieser Eigenschaften (Prüfspezifikationen). Die TR ist entsprechend der im De-Mail-Verbund möglichen unterschiedlichen Dienste modular aufgebaut.

Folgende Module sind für die einzelnen Dienste beschrieben:
- IT-Basisinfrastruktur
- Accountmanagement
- Postfach- und Versanddienst
- Identitätsbestätigungsdienst
- Dokumentenablage
- (Übergeordnete) Sicherheit

Für jeden Dienst sind die relevanten Prüfbereiche Funktionalität, Interoperabilität (für Basisinfrastruktur, Postfach- und Versanddienst und Identifizierungsdienst) und Sicherheit enthalten.

Anforderungen der Akkreditierung

Hauptregelungsgegenstand des De-Mail-Gesetzes sind die Voraussetzungen der Akkreditierung und die dafür zu erbringenden Nachweise. So müssen die künftigen De-Mail-Diensteanbieter in genau definierter Weise belegen, dass sie alle technisch-organisatorischen Anforderungen erfüllen, um die unterschiedlichen Dienste zu erbringen. Dazu gehören bestimmte Sicherheitsdienstleistungen für den De-Mail-Kontoinhaber, wie z. B. das Prüfen auf Schadprogramme wie Viren oder Trojaner, das automatisch bei jeder versendeten Nachricht durchgeführt wird. Genau definierte und umfangreiche Sicherheitsmechanismen bilden den Kern der Sicherheitsanforderungen, die der Diensteanbieter zum Schutz der De-Mail-Daten und der Kommunikation selbst erbringen muss. Zum Pflichtprogramm gehören etwa obligatorische Penetrationstests sowie eine IS-Revision. Der Provider muss ein Informationssicherheitsmanagementsystem etablieren, in dessen Rahmen die dem Grundschutz entsprechenden Maßnahmen regelmäßig überprüft werden, um den definierten Sicherheitszielen unter Berücksichtigung der Bedrohungen nachhaltig Rechnung zu tragen.

Als Nachweise für die Bereiche Funktionalität, Interoperabilität und Sicherheit gelten Testate von IT-Sicherheitsdienstleistern, die vom BSI zertifiziert sein müssen. Verfahrensbeschreibungen des BSI legen die fachlichen und personellen Voraussetzungen fest, die für eine Zertifizierung erfüllt werden müssen.

Prüfstellen und Auditoren für De-Mail

Um die notwendigen Prüfungen bei den De-Mail-Diensteanbietern vornehmen zu dürfen, haben sich für den Geltungsbereich De-Mail mehrere Auditoren zertifizieren sowie Prüfstellen beim BSI anerkennen lassen.

De-Mail-Auditoren können Prüfungen auf der Grundlage von ISO 27001 auf Basis von IT-Grundschutz erweitert um die De-Mail-spezifischen Anforderungen gemäß der TR De-Mail durchführen. Dies betrifft insbesondere die übergeordneten, d. h. für alle De-Mail-Dienste geltenden Sicherheitsanforderungen.

De-Mail-Prüfstellen können Prüfungen für die Bereiche Funktionalität und Interoperabilität gemäß der TR De-Mail durchführen.

Eine aktuelle Liste der zertifizierten De-Mail-Auditoren sowie anerkannter Prüfstellen mit deren Anerkennungsbereichen findet sich auf der BSI-Webseite www.bsi.bund.de » Zertifizierung und Anerkennung » Konformitätsbewertungen oder » De-Mail.

Die Prüfberichte sowohl der Auditoren als auch der Prüfstellen müssen vom Provider, der De-Mail-Diensteanbieter werden möchte, dem zertifizierten De-Mail-IT-Sicherheitsdienstleister vorgelegt werden, damit dieser die für die Akkreditierung notwendigen Testate ausstellen kann.

Erfolgsfaktor IT-Sicherheit gestalten

Günther Ennen, Leiter IT-Sicherheitsberatung im BSI

Informations- und Kommunikationstechnik (IKT) sind unverzichtbare Kernelemente nahezu aller Geschäftsprozesse – sowohl im Bereich von Behörden als auch in Wirtschaft und Wissenschaft. Der Wettlauf technischer Systeme hinsichtlich der Leistung und der Speichervolumen bestimmt den Wettbewerb am Markt. Anbieter und Nutzer moderner Informationstechnik (IT) werden von neuen Möglichkeiten der IT an die Grenzen des Machbaren getrieben. Die Folge: Zeitkritische Prozesse mit oftmals sensitiven Informationen bestimmen in zunehmend komplexen Netzstrukturen über die Zusammenarbeit von Personen oder Organisationen, und das weltweit und unabhängig vom Standort der Beteiligten. Als IT-Sicherheit – oder allgemein Informationssicherheit – wird der Prozess bezeichnet, der den Bedarf an Schutz von Informationen erfragt, der sich mit der Verlässlichkeit von Technik auseinandersetzt, der Maßnahmen zur Absicherung empfiehlt und somit insgesamt zu einem verlässlichen IT-Betrieb beiträgt.

Sicherheitsanforderungen an den IT-Betrieb

Zuverlässiger IT-Betrieb wird allgemein durch folgende Anforderungen skizziert: Technik und Anwendungen arbeiten störungsfrei (Verfügbarkeit), die Systeme und Daten sind in fehlerfreiem Zustand (Integrität), die Informationen sind vor Missbrauch geschützt (Vertraulichkeit). Diesen Ansprüchen an den verlässlichen IT-Betrieb stehen Risiken gegenüber, die aufgrund von Quantität, Qualität und Komplexität der beteiligten Objekte nur teilweise bekannt sind. Die Gefahren sind mannigfaltig: Sie reichen von nicht beabsichtigtem menschlichen Fehlverhalten über technische Ausfälle und Vorkommnisse höherer Gewalt bis hin zu bewussten, groß angelegten kriminellen Angriffen. Hinzu kommt: Die Gefahren können von jedem Ort unter Nutzung vorhandener Netzwerke ausgehen. Diese Risikosituation belegt, dass IT-Sicherheit kein isolierter Prozess ist. Die Anforderungen und Schutzmaßnahmen müssen im Zusammenhang mit anderen Unternehmenszielen (z. B. Funktionalität, Effizienz, Flexibilität, Compliance und Nachhaltigkeit) analysiert und realisiert werden müssen.

„IT-Sicherheit ist kein isolierter Prozess, und die Anforderungen müssen im Zusammenhang mit anderen Unternehmenszielen analysiert und realisiert werden.“

Günther Ennen

IT-Sicherheit gilt als Wert an sich. Ein aktives Bewusstsein dafür setzt allerdings häufig erst nach dem Auftreten von Sicherheitsvorfällen ein. Der Aufwand zum Beheben der dadurch verursachten Schäden – beispielsweise für das Bereinigen von Systemen und Datenbeständen beim Befall durch Schadprogramme – lässt sich nur schwer abschätzen. Sicherheitsvorfälle können jedoch auch zu klar bezifferbaren finanziellen Verlusten führen: Neben entgangenen Gewinnen werden zunehmend Verträge über IT-Dienstleistungen mit Service-Level-Agreements (SLAs) vereinbart, die neben der Haftung auch Vertragsstrafen bei Nichtleistung oder Produktionsausfall beinhalten.

Informationssicherheitsmanagement (ISMS): Gestalten und Steuern von IT-Sicherheit

Der Betrieb von IT ist nahezu ausnahmslos an Regelungen und Gesetze gebunden. Diese erfordern Kontrollmechanismen – sei es in Form periodischer Berichtspflicht, dokumentierter Nachweise über den geordneten IT-Betrieb oder der detaillierten Darlegung des gesamten Risikomanagements. Diese Mechanismen sind jedoch nur eine Teilaufgabe eines umfassenden Informationssicherheitsmanagementsystems (ISMS). Der vielzitierte Satz des US-amerikanischen Experten für Computersicherheit, Bruce Schneier, bringt es auf den Punkt: „IT-Sicherheit ist kein Produkt, sondern ein Prozess.“ Sie muss also stetig weiterentwickelt und angepasst werden. Damit unterliegt IT-Sicherheit einer Dynamik und ist immer auch eine Funktion der Zeit. Die einzelnen Elemente, die die IT-Sicherheit im Zusammenwirken beschreiben, unterliegen einem steten Wandel. Mitarbeiter kommen und gehen, Technologien werden ständig aktualisiert, werden weiterentwickelt oder durchleben Entwicklungssprünge. Dem ISMS kommt daher besondere Bedeutung zu. Auf der Landkarte der IT-Sicherheit besetzt es ein breites Feld an Zuständigkeiten und Aktivitäten. Das ISMS initiiert, steuert und verantwortet im Auftrag des Vorstandes, der Geschäftsführung bzw. der Behördenleitung den IT-Sicherheitsprozess.

Der erste und häufig schwierigste Schritt ist, die Anwender von der Notwendigkeit der IT-Sicherheit zu überzeugen. Die Annäherung an die professionelle Auseinandersetzung mit der IT-Sicherheit wird häufig von Vorurteilen geprägt: IT-Sicherheit kostet Geld, Performanz und Zeit. Die Wirtschaftlichkeit wird damit in hohem Maße infrage gestellt. Hinzu kommt, dass der unmittelbare Erfolg von IT-Sicherheit weder sichtbar noch spürbar ist. Das ISMS bewegt sich damit immer im Spannungsfeld des betriebswirtschaftlichen Maximin-Prinzips: Risiken maximal reduzieren bei minimalem Einsatz von finanziellen und personellen Ressourcen. Geschäftsprozesse sind in Hinblick auf Verfügbarkeit, Integrität und Vertraulichkeit so abzusichern und zu stabilisieren, dass signifikante Beeinträchtigungen gar nicht erst auftreten bzw. in einem tolerablen Risikorahmen bleiben. Um die Verlässlichkeit und Vertraulichkeit des IT-Betriebs zu gewährleisten, werden folgende Handlungsdimensionen empfohlen:

- **Handlungsdimension Personal:** Personalauswahl, Dokumentation von Erwartungen, Vorgaben und Anweisungen und deren regelmäßige Aktualisierung.

- **Handlungsdimension Organisation:** Dokumentation von Verantwortlichkeiten und Abläufen vom Prozess-Design bis hin zur Kontrolle der Zielerreichung. Das „Need-to-know-Prinzip“ legt die Zugriffsverfahren und den Nachweis von Zugriffen fest.
- **Handlungsdimension Technik:** Realisierung von starken Verfahren für Zugriffssicherung, Identifikation, Authentisierung und Protokollierung. Verschlüsselungsmechanismen, die dem Schutzbedarf der Information entsprechen.
- **Handlungsdimension Infrastruktur:** Auswahl geeigneter Räume für IT-Betrieb, Besprechungen und Archive, Kontrolle und Überwachung des Zugangs.

Im Sinne der Kontinuität der Geschäftsprozesse offenbart dieser Handlungsrahmen ein Spannungsfeld zwischen Funktionalität, Effektivität, Effizienz, Flexibilität, Compliance und Nachhaltigkeit.

- Effizienz orientiert sich an einem optimalen Kostenniveau bei angemessenem Kosten- und Nutzenverhältnis.
- Flexibilität ist Grundlage für nachhaltige Wettbewerbsfähigkeit und orientiert sich am steten Wandel technologischer Entwicklungen.
- Compliance wird durch Regelwerke und Rechtsrahmen bestimmt, die den ordnungsgemäßen Betrieb sicherstellen.
- Nachhaltigkeit fokussiert die Überlebensfähigkeit der Organisation durch Risikominimierung bei maximaler Kontinuität der Geschäftsprozesse.

Die Gestaltung von IT-Sicherheit ist kein Selbstzweck. Die Definition von Sicherheitszielen, die Analyse der Risiken und die Kenntnis rechtlicher Anforderungen begrenzen den Handlungsrahmen, der in der Gesamtheit die Angemessenheit von IT- Sicherheit darstellt.

Mit Normen und Zertifizierungen auf dem Weg zur IT-Sicherheit

Im Laufe der Jahre haben sich zahlreiche Normen, Standards und Best Practices entwickelt, die hierbei unterstützen können. Insbesondere Zertifizierungen und Normen sind Prüfstandards, an denen sich der aktuelle Status der IT-Sicherheit im eigenen Zuständigkeitsbereich messen lässt. Erfahrungen zeigen, dass die Orientierung an etablierten Prozessmodellen sinnvoll ist. Zu den Referenzmodellen gehören die bekanntesten Vertreter des IT-Grundschutzes sowie die Prozessmodelle von CobiT (Control Objectives for Information and Related Technology) und ITIL (IT Infrastructure Library). Dabei hat sich der PDCA-Zirkel (Planungs-, Realisierungs- und Kontroll-Zirkel) als Sichtweise bei der Gestaltung von IT-Services und deren Erbringung durchgesetzt. Wenn vergleichbare Qualitäten nachgewiesen werden sollen, empfiehlt es sich, Zertifizierungen nach internationalen Standards durchzuführen, beispielsweise nach ISO 27001.

Aus den Audits und Pen-Tests lassen sich Maßnahmen ableiten, die mit der Gegenüberstellung von Risikominimierung und Ressourcenaufwand priorisiert und umgesetzt werden sollten. Gleichzeitig erlauben sie der Institution eine aktuelle Einschätzung der Risiko- und Sicherheitslage aller schützenswerten Informationen. Um den Sicherheitsprozess effektiv und effizient zu halten, ist an dieser Stelle die Abstimmung aller Aktivitäten durch das IT-Sicherheitsteam mit der Unternehmensleitung zielführend, womit sich der PDCA-Zirkel schließt.

IT-Sicherheit, Wirtschaftlichkeit und Nachhaltigkeit Hand in Hand

Die Forderungen nach Funktionalität, Effektivität, Effizienz, Flexibilität, Compliance und Nachhaltigkeit skizzieren ein Spannungsfeld mit scheinbar konkurrierenden Zielsetzungen. Minimale oder sich verknappende finanzielle oder personelle Ressourcen verschärfen dies. Für die Lösung solcher Zielkonflikte bieten sich Modelle der IT-Governance an, mit denen u.a. eine Einführung und Professionalisierung des IT-Security-Managements erreicht werden kann. Die Leitung von Unternehmen beziehungsweise Behörden muss häufig durch Darstellung der Kosten und des damit verbundenen Nutzens überzeugt werden. Oft, so die Erfahrung, ist die Verfügbarkeit finanzieller Mittel für Sicherheitsprodukte oder Dienstleistungen externer Berater weniger ein Problem, als Personen des eigenen Hauses in Vollzeit oder in Teamstrukturen als Beauftragte für IT-Sicherheit freizustellen. Kosten entstehen in jedem Falle – und in der Informationssicherheit wird genau einmal bezahlt: Entweder vor oder nach dem Crash!

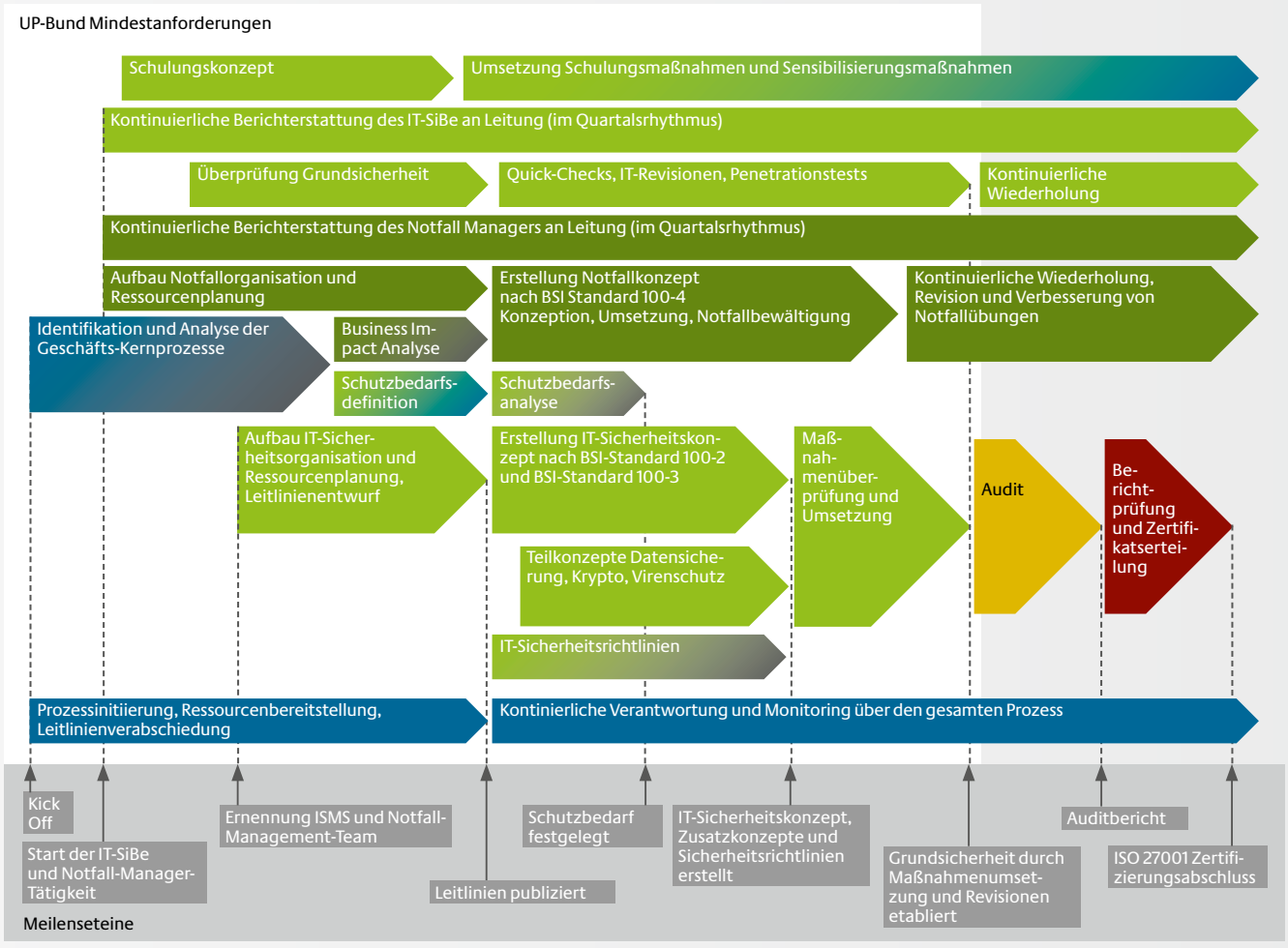
Was muss geschützt werden – wo sind die Kronjuwelen?

Die Fähigkeit, IT-Sicherheit optimal und ressourcenschonend zu gestalten, erfordert eine intensive Auseinandersetzung mit dem Schutzbedarf für Informationen, Anwendungen und IT-Systeme. Erst wenn man weiß, welches und wo die Kronjuwelen sind, kann geklärt werden, was auf alle Fälle verhindert werden und was in jedem Fall sichergestellt sein muss. Die verbindlichen Antworten müssen von der Unternehmens- beziehungsweise Behördenleitung als Eckpunkte der Risikovorsorge vorgegeben werden.

IT-Sicherheit zu gestalten ist keine unlösbare Herausforderung. Es ist weniger eine Frage der Fähigkeit, vielmehr liegt es häufig an der mangelnden Bereitschaft, sich mit den Aufgaben auseinander zu setzen.

Es muss vermittelt werden, dass der Prozess in jeder Phase und in hohem Maße gestaltet werden kann – und zwar immer nach den Maßstäben des derzeit Machbaren. Die Sicherheit der verantworteten Technik und Geschäftsprozesse hat einen Wert an sich, weil sie sich unmittelbar auf die Selbstsicherheit der verantwortlichen Personen auswirkt. Die Berichte in den Medien über Angriffe auf die IT, die Ausfälle von technischen Systemen, über unzuverlässige Kommunikationskanäle, neue Schadprogramme, raffinierte Betrugsversuche oder flüchtige Innentäter mit internem Wissen verunsichern in hohem Maß das verantwortliche Management in Unternehmen und die Leitung in der Verwaltung. Das Wissen: „Diese Vorfälle sind in meinem Zuständigkeitsbereich undenkbar!“ gibt den verantwortlichen Personen Sicherheit. Somit ist die Voraussetzung für die geordnete Betriebsführung und die erfolgreiche Amtsleitung gegeben.

Roadmap und Verantwortlichkeiten für ISMS und BCM*



* Business Continuity Management

Quelle: BSI

Sicherheit für die Cyberwelt

Cloud Computing

Herausforderung für die Informationssicherheit

Dr. Clemens Doubrava und Alex Didier Essoh,
Referenten IT-Sicherheitsmanagement und IT-Grundschutz im BSI

Das Thema Cloud Computing hat in den letzten Jahren weltweit stark an Bedeutung gewonnen und wurde zum IT-Trend des Jahres 2010 und 2011 gewählt[1]. In Deutschland rechnen die Marktforscher in den kommenden Jahren mit sehr hohen Zuwächsen bei den Ausgaben für Cloud Services. Schätzungsweise werden die Umsätze für Cloud-Dienstleistungen allein in Deutschland von 1,14 Milliarden Euro 2010 auf 8,2 Milliarden Euro im Jahr 2015 steigen. Dies entspricht einer jährlichen Umsatzsteigerung von durchschnittlich 48 Prozent[2].

Die Gründe für das zunehmende Interesse an Cloud Computing und die steigende Nutzung von Cloud-Dienstleistungen sind vielfältig. Beim Cloud Computing werden IT-Dienstleistungen wie Rechenleistung, Hintergrundspeicher, Entwicklung- und Laufzeitumgebungen, Anwendungssoftware oder sogar komplette Arbeitsumgebungen netzbasiert angeboten. Dabei ist es möglich, die angebotenen IT-Dienstleistungen je nach aktuellem Bedarf flexibel zu buchen, zu nutzen, wieder stillzulegen und sie nach tatsächlicher Nutzung abzurechnen. Auch Einsparpotenziale im Bereich der Anschaffung, des Betriebs und der Wartung der IT-Systeme werden oft genannt. Weitere Vorteile sind die Standardisierung von Geschäftsprozessen sowie die ubiquitäre Verfügbarkeit von Geschäftsanwendungen.

Chancen und Risiken von Cloud Computing

Die ursprüngliche Idee der Cloud – das heißt standardisierte Dienste, die von jedermann über das Internet genutzt werden können – wird als Public Cloud bezeichnet. Weitere Cloud-Modelle sind: Private Clouds, Community Clouds und Hybrid Clouds. Insbesondere Private Clouds erfreuen sich wegen der Möglichkeit der Kontrolle zunehmender Beliebtheit. Neben den genannten potenziellen Vorteilen gibt es auch eine Reihe von Risiken, die mit der Auslagerung von Daten und Anwendungen in eine Public Cloud verbunden sind, die bei Nutzung einer Private Cloud nicht oder nur bedingt zutreffen. Hierzu zählen:

- Die Auslagerung der IT in eine Public Cloud bedeutet, dass sich der Cloud-Kunde in eine starke Abhängigkeit von seinem Cloud-Dienstleister begibt, da er keinen direkten Zugriff mehr auf Hard- und Software hat.
- Viele unbekannte Nutzer teilen sich eine gemeinsame Infrastruktur, wodurch das Risiko steigt, dass Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) verletzt werden.
- Daten und Anwendungen werden über das Internet genutzt, so dass ein Ausfall der Internetverbindung den Zugriff unmöglich macht.
- Aufgrund der Konzentration der Ressourcen wird eine Zunahme von Distributed Denial-of-Service-Angriffen (DDoS) auf Cloud-Computing-Plattformen erwartet.

Einige der oben erwähnten Risiken wie beispielsweise DDoS sind zwar nicht Cloud-spezifisch, werden aber aufgrund der Einsatzumgebung verstärkt.

Neben technischen und organisatorischen Fragen müssen auch juristische Aspekte des Cloud Computing beachtet werden. In diesem Zusammenhang gibt es eine Reihe von Fragen zu beantworten, wie etwa: Welches nationale Recht gilt beim Auslagern der IT in die „Wolke“? Wo liegen die Daten, und sind sie vor dem Zugriff Dritter – etwa staatlicher Stellen – ausreichend geschützt? Was geschieht bei einer Insolvenz des Cloud-Anbieters?

Aktivitäten des BSI zur Erhöhung der Informationssicherheit

Obwohl weltweit die Inanspruchnahme von IT-Dienstleistungen aus der „Wolke“ steigt, zeigen fast alle Umfragen und Studien, dass es auch eine Vielzahl von Hemmnissen gibt, die einem verstärkten Einsatz entgegen stehen. Als eines der größten Hindernisse wird die Informationssicherheit betrachtet. Um dieses Thema zu adressieren und Anwender sowie Anbieter von Cloud-Diensten zu unterstützen, hat das BSI eine Reihe von Aktivitäten initiiert.

[1] BITKOM-Presseinformation vom 18. Januar 2011
[2] BITKOM-Presseinformation vom 6. Oktober 2010

Alex Didier Essoh und Dr. Clemens Doubrava, Ansprechpartner im BSI zum Thema Cloud Computing

BSI-Eckpunktepapier: Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter
Am 28. September 2010 veröffentlichte das BSI das Eckpunktepapier „Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter“ als Diskussionsentwurf. Darin wird die Cloud-basierte Verarbeitung von Informationen mit einem normalen bis hohen Schutzbedarf betrachtet – dabei folgt die Kategorisierung der Daten bezüglich ihres Schutzbedarfs den Hinweisen des BSI-Standards 100-2.

Das Eckpunktepapier bietet eine Grundlage für die Diskussion zwischen Cloud-Anbietern und -Kunden, mit dem Ziel, sinnvolle und angemessene Sicherheitsanforderungen an das Cloud Computing zu entwickeln, die einen Schutz von Daten und Systemen gewährleisten. Es behandelt vierzehn als kritisch identifizierte Bereiche (Eckpunkte) der Cloud-Computing-Sicherheit und enthält eine Reihe von Best Practices (hier Mindestsicherheitsanforderungen genannt) zur Absicherung der adressierten Bereiche. Ein weiterer Eckpunkt beschreibt Zusatzforderungen an Cloud-Computing-Anbieter aus Sicht der Bundesverwaltung. Neben Sicherheitsanforderungen aus der klassischen IT – wie Sicherheitsarchitektur, ID- und Rechtemanagement, Notfallmanagement, Monitoring und Security Incident Management – werden auch Themen behandelt, die bei der Auslagerung von Daten, Anwendungen und Prozessen in eine Public Cloud besondere Relevanz erhalten. Hierzu zählen Transparenz, Vertragsgestaltung, Datenschutz und Mandantenfähigkeit. Insbesondere ist die sichere und verlässliche Trennung der Mandanten aufgrund der gemeinsam genutzten IT-Infrastruktur essentiell und stellt einen Schlüsselaspekt der Sicherheit beim Cloud-Computing dar.

Das Eckpunktepapier wurde ausführlich diskutiert und konstruktiv kommentiert. Die Beiträge fließen in die finale Version der BSI-Mindestsicherheitsanforderungen ein.

„Cloud Computing ist ein Paradigmenwechsel in der IT hin zu mehr Services-orientierten Diensten, die über das Internet angeboten und konsumiert werden. Das ist für Kunden und Anbieter gleichermaßen wichtig und interessant. Neben den wirtschaftlichen Vorteilen der „Cloud“, etwa Skaleneffekte und Elastizität, ist Sicherheit ein ganz zentrales Thema. Sicherheit ist eine unabdingbare Voraussetzung dafür, dass Cloud Computing im Markt erfolgreich ist. Das BSI hat sich des Themas Sicherheit in der Cloud frühzeitig angenommen und führt schon seit geraumer Zeit den Dialog mit der Industrie dazu. Microsoft begrüßt die vielen Gelegenheiten zum konstruktiven kritischen Diskurs über die Sicherheit in der Cloud, die das BSI in diversen Workshops und Einzelgesprächen gegeben hat. Dies und das inzwischen veröffentlichte Eckpunktepapier zu Mindestsicherheitsanforderungen in der Cloud treibt die Diskussion um Informationssicherheit in der Cloud im positiven Sinne voran. Aus unserer Sicht gehen die Aktivitäten des BSI beim Thema Sicherheit in der Cloud in die richtige Richtung. Sicherheit in der Cloud ist Microsoft genauso wichtig wie dem BSI, und wir freuen uns auf die weitere gute Zusammenarbeit.“

Gerold Hübner, Government Security Director, Microsoft Corporation

Sicheres und vertrauenswürdiges Cloud Computing stand von Anfang an im Fokus von EuroCloud Deutschland_eco e.V.. Mit der Entwicklung eines Zertifizierungssystems für den Bereich Software as a Service, dem EuroCloud Star Audit SaaS, konnten wir einen wichtigen Schritt in diese Richtung gehen. Die enge Zusammenarbeit mit dem BSI ist dabei besonders wichtig, um eine qualitativ hochwertige Zertifizierung anbieten zu können und darüber hinaus die Möglichkeit zu haben, die Erfahrungen der Cloud-Anbieter bei der Erstellung der BSI-Mindestsicherheitsanforderungen einbringen zu können. Im gemeinsamen Dialog mit dem BSI haben wir die Gesprächsbereitschaft zur konstruktiven Ausgestaltung der Rahmenbedingungen sehr geschätzt. Cloud Computing wird sich weiterhin extrem stark entwickeln. Daher ist es wichtig, zu einem frühen Zeitpunkt die Themen Sicherheit, Datenschutz und Interoperabilität mit den notwendigen Anforderungen zu formulieren. Seitens der Cloud-Anbieter besteht eine hohe Bereitschaft, dieses Vorgehen zu unterstützen und auch darstellen zu können, dass alle notwendigen Maßnahmen zur Bereitstellung von sicheren Cloud Services umgesetzt wurden. Wir freuen uns auf die weitere Zusammenarbeit mit dem BSI bei der weiteren Gestaltung von Cloud Computing mit „Sicherheit – Made in Germany“.

Andreas Weiss, Direktor Eurocloud Deutschland_eco e.V.

Studie „Erarbeitung von Sicherheitsempfehlungen für Cloud Computing“

Neben den Mindestsicherheitsanforderungen erstellt das BSI eine Studie zur „Erarbeitung von Sicherheitsempfehlungen für Cloud Computing“. Das Dokument basiert auf öffentlich verfügbaren Informationen, einem Workshop mit Key Stakeholdern und vielen nachfolgenden direkten Gesprächen sowohl mit Cloud-Anbietern als auch Cloud Enablern zu den Sicherheitsfunktionen der jeweiligen Plattform. Zentrales Ziel der Studie ist es, einen Überblick über die internen Prozesse, Prozeduren und Grundsätze der Anbieter von Cloud-Diensten zu schaffen. Die Ergebnisse der Studie fließen in die Mindestsicherheitsanforderungen des BSI an Cloud Computing ein.

Kurzstudien zum Thema Private Cloud

Um die potenziellen Vorteile von Cloud Computing nutzen zu können und dennoch die Kontrolle über die IT-Infrastruktur zu behalten, greifen viele Anwender zur Bereitstellung der Dienste auf eigene virtualisierte Rechenzentren zurück. Auch hier müssen technische, organisatorische und infrastrukturelle Maßnahmen zum sicheren Betrieb und zur sicheren Nutzung umgesetzt werden. Vor diesem Hintergrund erstellt das BSI seit November 2010 zusammen mit Technologie-Anbietern eine Reihe von Kurzstudien mit besonderem Fokus auf Private Clouds. In den Kurzstudien soll eine detaillierte und tiefer gehende Sicherheitsanalyse von Cloud-Computing-Systemen durchgeführt werden. Primäres Ziel ist es, Sicherheitsempfehlungen für sicheres Private-Cloud-Computing zu erarbeiten. Dabei werden nur solche Private-Cloud-Implementierungen betrachtet, die als Infrastrukturpakete – also integrierte, getestete und validierte IT-Systeme, bestehend aus Server-, Netz-, Storage-, und Management-Komponenten – angeboten werden. Zunehmend werden solche integrierte beziehungsweise konvergierte Umgebungen werbewirksam als „Cloud in the box“ angeboten. Die Ergebnisse der Kurzstudien werden 2011 veröffentlicht.

Integration von Cloud Computing in den IT-Grundschutz

Die Ergebnisse der oben genannten Kurzstudien sollen in den IT-Grundschutz eingearbeitet werden. Geplant ist die Entwicklung von IT-Grundschutz-Bausteinen sowohl für die Nutzung als auch für die Bereitstellung von Cloud-Diensten. Der BSI-Standard 100-2 wird zur Integration von Cloud-Aspekten in die IT-Grundschutz-Vorgehensweise angepasst. Insbesondere die Modellierung komplexer, virtualisierter Informationsverbünde machen gegebenenfalls auch eine Anpassung des GSTOOLs nötig.

Bedrohungen außerhalb klassischer IKT-Infrastrukturen

Stefan Ritter, Referatsleiter CERT-Bund, und Hans Honecker, Referent für den Schutz Kritischer Infrastrukturen im BSI

Die Schadsoftware Stuxnet hat 2010 verdeutlicht, wie schwer inzwischen informationstechnische Bedrohungen auch außerhalb der klassischen Bürokommunikation und Datenverarbeitung wiegen.

Einsatz von Informations- und Kommunikationstechnik außerhalb klassischer IKT-Infrastrukturen

Der Einsatz von Informations- und Kommunikationstechnik ist längst nicht mehr auf klassische IKT-Infrastrukturen wie Bürokommunikationsumgebungen, Rechenzentren oder Kommunikationsnetze beschränkt. Moderne Infrastrukturen in Versorgung und Produktion, im Finanzwesen, Gesundheitswesen wie in der Wirtschaft allgemein sind von informationstechnischen Anteilen durchdrungen, die sich in vielen Grundeigenschaften immer mehr der klassischen Informationstechnik annähern oder sich gar unmittelbar auf handelsübliche Technik wie PCs, gängige Netzwerktechnik oder Standardanwendungen stützen. Dies trifft auch und gerade für die Kritischen Infrastrukturen zu, die für das Gemeinwesen und für die Wirtschaft unverzichtbare Dienstleistungen erbringen.

Trotz Abstützung auf klassische informationstechnische Bestandteile sind die eingesetzten Spezialtechnologien in ihrem Gesamtumfang von dem jeweiligen Einsatzgebiet geprägt. Bestandteile von Systemen zur Steuerung physischer Prozesse in der Produktion unterscheiden sich deutlich von Steuerungskomponenten für die Energieversorgung. Mit komplexen medizinischen Geräten haben beide kaum etwas gemein. Innerhalb der einzelnen Einsatzgebiete ist in verschiedenen Installationen zudem eine große Bandbreite der konkreten Ausprägung der physikalisch-technischen Komponenten wie auch der informationstechnischen Anteile vorhanden – und sei es nur aufgrund des Einsatzes der Produktlinien verschiedener Hersteller oder schlicht aufgrund des verschiedenen Alters der jeweiligen Anlagen.

Stuxnet – ein gezielter Angriff auf Prozesssteuerungssysteme

2010 stand das Schadprogramm Stuxnet im besonderen Fokus der Öffentlichkeit. Dabei handelt es sich um eine Schadsoftware, die mit erheblichem Aufwand programmiert wurde, um gezielt industrielle Prozesssteuerungssysteme anzugreifen. Wie Analysen von Experten ergaben, hatte Stuxnet den Auftrag, eine bestimmte Anlagenkonstellation technisch filigran zu sabotieren. Stuxnet greift mit informationstechnischen Mitteln sehr gezielt eine spezifische Prozesssteuerungstechnologie an und manipuliert dabei die Prozesse, indem es bestimmte Messgrößen abgreift und Steuerkommandos verändert, ohne dass der Betreiber der Anlage diese Veränderungen bemerken kann. Bei einem erfolgreichen Angriff könnte das bearbeitete Produkt unbrauchbar oder gar die Produktionsanlagen zerstört werden.

Bedrohung IKT-gestützter Spezialtechnologien durch gezielte Angriffe

In der öffentlichen Diskussion über Stuxnet wurde vor allem die Verwundbarkeit Kritischer Infrastrukturen mit Sorge betrachtet.

„Bei einem erfolgreichen Angriff könnte das bearbeitete Produkt unbrauchbar oder gar die Produktionsanlagen zerstört werden.“

Stefan Ritter

Stuxnet ist unter dem Strich aber weniger als konkrete Schadsoftware von Bedeutung – wichtig ist vielmehr der nun vorliegende Beleg für die Möglichkeit von Angriffen solcher Qualität. Es gibt demnach Angreifer, die weder Kosten noch Mühen scheuen, um aus ihrer Sicht sehr wichtige Ziele informationstechnisch anzugreifen und möglichst unbemerkt zu sabotieren. Auch wenn Aufwand und technische Qualität des Angriffs im Fall Stuxnet beeindrucken – weder gibt es Grund zu der Annahme, dass solche Angriffe nur vom Urheber von Stuxnet vorgetragen werden können, noch dass Stuxnet der einzige Angriff dieser Qualitätsklasse war und insbesondere bleiben wird. Letztlich bleibt die geänderte

Hans Honecker

Qualität der Bedrohung damit auch nicht auf Technologien zur Steuerung physischer Prozesse beschränkt. Vielmehr muss nun davon ausgegangen werden, dass IT-gestützte Spezialtechnologien allgemein von gezielten Angriffen bedroht sind. Die Bewertung des Risikos derart gezielter Angriffe auf Prozesssteuerungssysteme oder andere informationstechnisch gestützte Spezialtechnologien muss neu vorgenommen werden – sowohl in Kritischen Infrastrukturen als auch im allgemeinen Einsatz.

Verschärfte Bedrohung durch ungezielte Angriffe

Neben gezielten und mit hohem Aufwand vorgetragenen Angriffen stellen aber auch ungezielte Angriffe und Irrläufer von aggressiver Schadsoftware immer öfter eine Bedrohung für informationstechnisch gestützte Spezialtechnologien dar. Beispielsweise hat die Schadsoftware Conficker als sich ungezielt aggressiv verbreitender Wurm das Potenzial, schwerwiegenden Störungen mit schweren Folgeschäden auszulösen.

Umgang mit den neuen Bedrohungen

Auch außerhalb der klassischen Informationstechnik müssen schwerwiegende Störungen durch klassische IT-Angriffe und Irrläufer von Schadsoftware als Risiken mitbetrachtet werden. Wo bereits konsequent informationstechnische Sicherheit umgesetzt wird, ist dies sicher nicht neu. Wo dies nicht der Fall ist, wurde der Handlungsbedarf durch die Vorfälle im vergangenen Jahr noch einmal sehr deutlich. Insbesondere das Risiko und Schadenspotenzial gezielter, qualitativ hochwertiger und mit erheblichem Aufwand durchgeführter spezifischer Angriffe gegen IT-gestützte Spezialtechnologien sollte aber unabhängig vom bisherigen Status der informationstechnischen Sicherheit neu bewertet werden. Abhängig von den Anforderungen an die spezifische Prozessarchitektur und den eingesetzten Spezialtechnologien sind gegebenenfalls sehr spezifische Maßnahmen notwendig, um aus den neuen Bedrohungen keine Gefährdungen und damit untragbaren Risiken werden zu lassen.

Kritische Infrastrukturen

Sowohl der Staat als auch die Betreiber Kritischer Infrastrukturen berücksichtigen informationstechnische Bedrohungen von IT-gestützten Spezialtechnologien seit Langem. Die durch Stuxnet belegte Entwicklung der Bedrohung ist abstrakt in den entsprechenden Risikobetrachtungen bereits berücksichtigt. Betreiber Kritischer Infrastrukturen sind gerade für den Betrieb der Prozessinfrastrukturen gut aufgestellt und können so auf neue informationstechnische Bedrohungen schnell reagieren. Im Rahmen der gemeinsamen Maßnahmen zum Schutz Kritischer Informationsinfrastrukturen arbeiten Betreiber und Staat zudem seit Jahren eng zusammen. Im Jahr 2010 konnte diese Zusammenarbeit weiter deutlich intensiviert werden. Unter anderem wurden von den Betreibern Kritischer Infrastrukturen aus mehreren Branchen bzw. Sektoren weitere Single Points of Contact (SPoC) für den Austausch relevanter Informationen, Warnungen und Lageinformationen zwischen der jeweiligen Branche und dem Lagezentrum des BSI eingerichtet. Diese Kommunikation zwischen Staat und Betreibern hat sich im vergangenen Jahr im Rahmen verschiedener aktueller Sicherheitsvorfälle wie auch in regelmäßigen Übungen bewährt. Das 2008 gemeinsam erarbeitete Kommunikationskonzept[3] konnte damit in den vergangenen beiden Jahren in wesentlichen Punkten erfolgreich mit Leben gefüllt werden. Einerseits durch die allgemeine Zusammenarbeit, andererseits durch konkrete Maßnahmen. Dazu gehört die Etablierung operativer Kommunikationsmechanismen für die lageangepasste Prävention und die koordinierte Bewältigung von IT-Krisen. Dadurch wurde eine gute Grundlage geschaffen, um die notwendige Sicherheit auch für IT-gestützte Spezialtechnologien in Kritischen Infrastrukturen aufrecht zu erhalten. Auf diese Weise kann möglichen IT-gestützten Angriffen auch außerhalb der klassischen Anwendungsfelder von Informations- und Kommunikationstechnik gemeinsam wirkungsvoll begegnet werden.

[3] „Früherkennung und Bewältigung von IT-Krisen", erarbeitet im Rahmen des Umsetzungsplans KRITIS

Botnetzen geht es an den Kragen

Willi Herzig, Ansprechpartner Anti-Botnetz-Initiative im BSI

Das Problem der Botnetze hat in den vergangenen zwei Jahren weiterhin massiv zugenommen. Die Professionalisierung der Internetkriminalität mit wirtschaftlichen Interessen ist rasant fortgeschritten. Botnetze werden professionell international vermietet, und Kunden nutzen diese unter anderem als Mittel der Vergeltung, um Wettbewerbsvorteile zu erhalten sowie für weitere kriminelle Zwecke – wie etwa Erpressung – oder auch aus politischen und religiösen Motiven. Untersuchungen des BSI zeigen, dass Anwender oftmals nicht bemerken, dass ihr PC Teil eines Botnetzes ist, da dieser weiterhin scheinbar normal funktioniert. Die Analyse des Sicherheitsunternehmens Trendmicro, die 100 Millionen infizierte IP-Adressen weltweit untersuchte, kam zum gleichen Ergebnis. Sie zeigt, dass 80 Prozent der infizierten PCs mehr als einen Monat und 50 Prozent der betroffenen PCs sogar mehr als 300 Tage infiziert waren. Ein Grund dafür ist, dass Botsoftware sogar teilweise Antiviren-Software deaktivieren kann, um nicht entdeckt zu werden. Erkannt wird die Infektion des Rechners daher häufig erst, wenn der Anwender von seinem Provider darüber informiert wird.

Start der Anti-Botnetz-Initiative

Um einem Bürger zu helfen, dessen PC Teil eines Botnetzes ist, ist es wichtig, ihn über die Infektion seines PCs zu informieren, die damit verbundenen Gefahren zu erläutern und ihm Beratung und aktive Unterstützung bei der Beseitigung der Schadprogramme anzubieten. Das BSI unterstützt deshalb die Anti-Botnetz-Initiative des eco-Verbands der deutschen Internetwirtschaft e.V. zur Reduzierung infizierter Rechner. Diese Initiative, die am 15. September 2010 offiziell gestartet ist, schafft mehr Sicherheit für den Endnutzer und soll Botnetzen, die in beziehungsweise aus Deutschland agieren, in weiten Teilen nachhaltig den Boden entziehen.

Im Rahmen des Projekts informieren die teilnehmenden Internetserviceprovider (ISP) betroffene Kunden über eine mögliche Infektion ihres Rechners mit einem Schadprogramm. Dabei weisen sie auf die Informationen und Tools zur selbstständigen Überprüfung und Säuberung des PCs hin, die auf der Website https://www.botfrei.de zur Verfügung stehen. Hier erhält der Anwender umfangreiche Hintergrundinformationen, Sicherheitsmaßnahmen, Handlungsempfehlungen und Tools zur Identifizierung und Deinstallation von Schadprogrammen. Mit dem DE-Cleaner kann der Anwender die Infektion durch Schadprogramme selbst erkennen und beseitigen. Für hartnäckige Infektionen steht zusätzlich die DE-Cleaner Rettungssystem CD zur Verfügung, die auch dann eingesetzt werden kann, wenn die Infektion auf dem laufenden System, beispielsweise bei sogenannten Rootkits, nicht erkannt werden kann. Diese CD wurde in Zusammenarbeit mit COMPUTER BILD und Avira entwickelt und mit der Dezember-Ausgabe 2010 des Computermagazins bereits an mehrere hunderttausend Anwender verteilt.

BSI-Vizepräsident Horst Flätgen (Mitte) bei der Pressekonferenz zum Start der Anti-Botnetz-Initiative (ebenfalls im Bild: Walter Schumann, Vice President Sales, eleven GmbH (l.) und Bernd Becker, Geschäftsführer eco IT Service und Beratung GmbH

Wenn ein durch den Internetserviceprovider benachrichtigter Anwender weitere Unterstützung benötigt, wird ihm per Telefon bei der Beratungshotline des Anti-Botnetz-Beratungszentrums weitergeholfen.

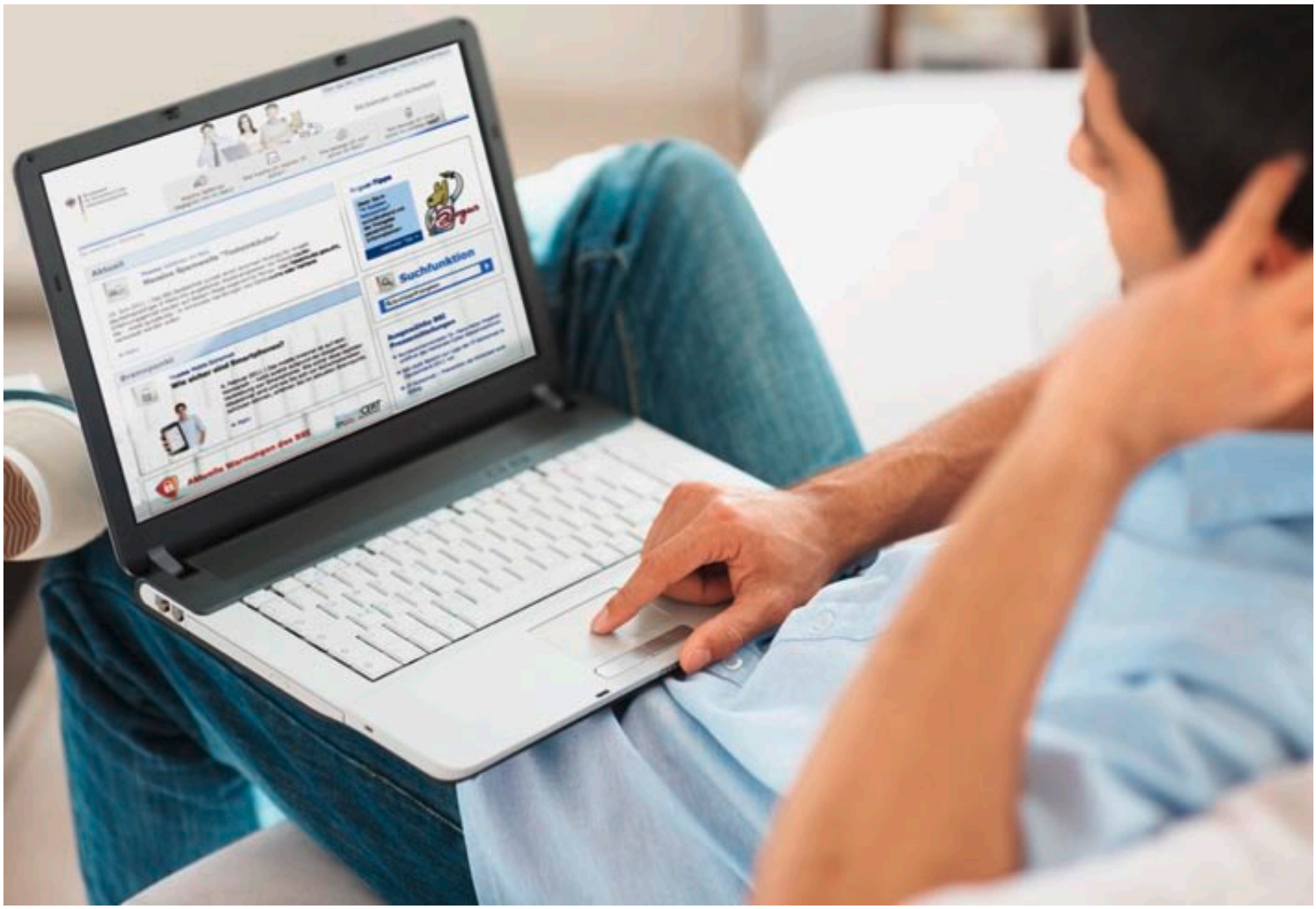
Positive Reaktionen seitens der Nutzer

Die Initiative hat seit dem Start massiven Zuspruch erhalten und es konnten weitere Partner gewonnen werden. Seit dem Projektstart am 15. September bis Ende 2010 nutzten bereits über 710.000 Besucher die Angebote der Webseite www.botfrei.de. Der DE-Cleaner wurde in diesem Zeitraum fast 370.000 mal heruntergeladen und ausgeführt.

Seit Dezember 2010 steht neben dem bisherigen DE-Cleaner von Symantec ein weiterer DE-Cleaner der Firma Kaspersky speziell für das Projekt zur Verfügung. Dieser ergänzt den bisherigen DE-Cleaner ideal, da er nach dem Herunterladen auch ohne Internetverbindung eingesetzt werden kann. Eco konnte weitere Internetserviceprovider für das Projekt gewinnen, die kurzfristig aktiv am Anti-Botnet-Beratungszentrum teilnehmen und ihre Kunden informieren werden. Das Angebot für Anwender konnte zudem erweitert werden. So steht die Webseite des Anti-Botnet-Beratungszentrums jetzt auch auf Englisch und Türkisch zur Verfügung.

„Allein in den ersten zwei Monaten konnte das Anti-Botnet-Beratungszentrum Hunderttausende Internetnutzer über die Gefahren aufklären, die von Botnetzen ausgehen. Gemeinsam mit unseren Partnern und mit Unterstützung des BSI können wir das Internet für uns alle ein Stück weit sicherer machen.“

Prof. Michael Rotert, Vorstandsvorsitzender, eco – Verband der deutschen Internetwirtschaft e.V.



Ins Internet – mit Sicherheit!

Svenja Schiffer, Referentin Öffentlichkeitsarbeit im BSI

Bürgersensibilisierung mit Hilfe des Internets

IT-Sicherheit hängt nicht allein von der Umsetzung technischer Maßnahmen ab. Auch das Verhalten der Nutzer trägt einen wesentlichen Teil zur Sicherheit eines IT-Systems bei. Nur wer angemessen über mögliche Sicherheitsrisiken und Schutzmaßnahmen informiert ist, kann entsprechend handeln. Das BSI beschäftigt sich deshalb nicht nur mit den technischen und organisatorischen Aspekten der IT-Sicherheit, sondern auch mit der Stärkung des IT-Sicherheitsbewusstseins und der IT-Sicherheitskompetenz von Privatanwendern.

Theoretisches Wissen in die Tat umsetzen

Dass bei einer Vielzahl von Internetnutzern weiterhin Aufklärungsbedarf besteht, hat 2010 eine repräsentative Umfrage des BSI zu verschiedenen Aspekten rund um das Thema IT- und Internet-Sicherheit ergeben. Ein zentrales Ergebnis dieser Umfrage: Bei einer Mehrheit der Bundesbürger klafft in Bezug auf Sicherheit im Internet eine Lücke zwischen theoretischem Wissen und faktischem Handeln. So sind Gefährdungen, die beim Surfen bestehen – wie Viren, Trojaner, Identitätsdiebstahl, Abo-Fallen, Phishing oder Spyware – bei 60 bis über 90 Prozent der Befragten bekannt.

Svenja Schiffer

Die notwendigen Schutzmaßnahmen ergreifen jedoch noch zu wenige. So ist beispielsweise der Einsatz von Virenscannern im Vergleich zur BSI-Bürgerumfrage von 2008 rückläufig. Nur noch 87 Prozent der Bürgerinnen und Bürger haben einen Virenscanner installiert, während es 2008 noch 92 Prozent waren. Ein weiteres Beispiel: 63 Prozent der Befragten sind während des Internetsurfens mit Administratorrechten an ihrem PC angemeldet. Bei einem mit Schadsoftware infizierten Rechner könnte der Angreifer somit die volle Kontrolle über den PC erlangen.

Bürger-Ansprache effizient gestalten

Um effektive Aufklärungsarbeit zu betreiben und sicherzustellen, dass die Zielgruppe auch erreicht wird, muss die Frage geklärt sein, mit welchen Kommunikationsmitteln sich Privatanwender informieren. Die Umfrage ergab dazu, dass nahezu die Hälfte der Befragten der Meinung ist, dass sich Webseiten besonders dafür eignen, über IT-Sicherheitsthemen zu informieren. Nur für ein einziges anderes Medium trafen mehr Befragte diese Aussage: PC-Fachzeitschriften. Dies bestätigt, dass das BSI mit seinen Webangebot www.bsi-fuer-buerger.de gut aufgestellt ist und die richtige Strategie verfolgt.

Die Basis seines Angebots zur Aufklärung und Sensibilisierung der Privatanwender hat das BSI bereits 2002 gelegt. Auf der CeBIT stellte das BSI seine Bürger-CD mit dem Titel „Ins Internet – mit Sicherheit!“ vor. Um den schnellen Entwicklungen im Bereich IT-Sicherheit Rechnung tragen und stets aktuelle Informationen anbieten zu können, wurde 2003 aus der CD ein Webauftritt: www.bsi-fuer-buerger.de. Auf dieser Webseite bietet das BSI allgemein-verständliche, fachlich kompetente und neutrale Informationen über Bedrohungen im Internet sowie entsprechende Schutzmaßnahmen an und gibt konkrete Hilfestellungen zu ausgewählten Themen. Darüber hinaus besteht für Privatanwender eine Kontaktmöglichkeit per E-Mail, Telefon und Fax.

2010 war es an der Zeit, BSI-für-Bürger einem Relaunch zu unterziehen. Bei der Neugestaltung ging es vor allem darum, das Design zu modernisieren, die Nutzerfreundlichkeit zu erhöhen und mehr Möglichkeiten für die Platzierung aktueller Themen zu schaffen. Eine intuitive Navigationsstruktur führt den Nutzer durch die Seite. Er findet Antworten auf die Fragen: „Welche Gefahren begegnen mir im Netz?“, „Wie mache ich meinen PC sicher?“, „Wie bewege ich mich sicher im Netz?“ und „Wie bewege ich mich sicher im mobilen Netz?“. Auf der Startseite werden dem Nutzer mit dem Brennpunkt sowie den drei neuesten Meldungen des Warn- und Informationsdienstes Bürger-CERT aktuelle Informationen geboten. In einer Themenbox greift BSI-für-Bürger Aspekte auf, die von besonderem Interesse sind bzw. aktualisiert wurden.

Das BSI bedient mit seinen Bürger-Service-Angeboten bewusst eine heterogene Zielgruppe, um mit seinen Informationen ein möglichst breites Publikum ansprechen zu können. Um Zielgruppensegmente zu erreichen, arbeitet das BSI mit Partnern zusammen, die gleichgerichtete Ziele verfolgen, aber andere Zielgruppen ansprechen. Diese Kooperationen reichen dabei von gegenseitigen Verlinkungen über die Verwendung von BSI-Informationen auf anderen Web-Angeboten bis hin zu einem konstruktiven Austausch über aktuell relevante IT-Sicherheitsthemen und darüber, wer welches Thema schwerpunktmäßig aufgreift.

Das BSI trägt mit seinen Angeboten einen wichtigen Teil zur Aufklärung und Sensibilisierung der Privatanwender bei. In Zukunft gilt es, dieses Engagement fortzuführen und auszubauen, um der steigenden Zahl der Internetnutzer gerecht zu werden.

Das BSI in Politik und Medien

Nora Basting, Pressereferentin, und
Beatrice Feyerbacher, Referentin im Leitungsstab des BSI

„Die vielseitigen Themen der IT-Sicherheit erlangen einen festen Platz in der Medienberichterstattung.“

Nora Basting

„Viele politische Projekte sind heutzutage auch IT-Projekte, in denen IT-Sicherheit eine zentrale Rolle spielt.“

Beatrice Feyerbacher

Für Journalisten und Medienschaffende ist das BSI bereits seit etlichen Jahren ein gefragter Ansprechpartner rund um das Thema IT-Sicherheit. Bei vielen Medienkontakten stehen die Kernaufgaben des BSI als IT-Sicherheitsdienstleister des Bundes im Vordergrund. Als unabhängige und neutrale Stelle gibt das BSI aber auch Tipps und Hinweise für Privatnutzer und Unternehmen. Themen wie Identitätsdiebstahl und Phishing, Passwortsicherheit und der sichere Umgang mit sozialen Netzwerken sind daher häufig Gegenstand von Medienanfragen, ebenso wie die Informationssicherheit im Unternehmensumfeld.

Im Jahr 2010 hat die Sichtbarkeit des BSI in den Medien und in der Öffentlichkeit noch einmal deutlich zugenommen. Neben der insgesamt stetig steigenden Aufmerksamkeit für die Themen IT- und Internetsicherheit ist dies vor allem auf zwei aktuelle Entwicklungen zurückzuführen. Zum einen haben 2010 Großprojekte, an denen das BSI beteiligt ist, einen erhöhten Informationsbedarf in der Öffentlichkeit hervorgerufen. Wichtigster Meilenstein war hier die Einführung des neuen Personalausweises zum 1. November 2011 – ein Thema, das nahezu alle Bundesbürger in den nächsten Jahren betreffen wird. Das BSI informierte bereits seit Jahres-

BSI-Präsident Michael Hange im Interview

anfang unter anderem im Rahmen verschiedener Pressekonferenzen, Veranstaltungen und Messeauftritte über die Sicherheitsarchitektur des neuen Personalausweises und die Möglichkeiten, den Ausweis als elektronische Identität (eID) zum „Ausweisen" im Internet zu benutzen. Daneben war das BSI auch viel gefragter Ansprechpartner für Interviews, Statements und Fernsehbeiträge. Im Vordergrund standen auch hier die Datensicherheit des neuen Ausweises sowie die Anwendungsmöglichkeiten der eID-Funktion – nicht zuletzt, weil kritische Medienberichte viel Erklärungsbedarf in der Öffentlichkeit zur Folge hatten.

Zum anderen spielt die Neuausrichtung im Rahmen des seit 2009 gültigen BSI-Gesetzes in der öffentlichen Wahrnehmung des BSI eine Rolle. Denn die neu gestaltete gesetzliche Grundlage gibt dem BSI die Möglichkeit, vor akuten Sicherheitslücken in IT-Produkten sowie vor Schadprogrammen öffentlich zu warnen. Von dieser Befugnis machte das BSI erstmals im Januar 2010 Gebrauch und veröffentlichte im Lauf des Jahres anlassbezogen eine Reihe von aktuellen Meldungen zu Sicherheitslücken in IT-Produkten wie Betriebssystemen, Browsern oder anderer Anwendungssoftware. Besteht bei Produkten mit hoher Verbreitung in der Bevölkerung die unmittelbare Gefahr, dass eine Sicherheitslücke von IT-Kriminellen ausgenutzt wird, kann das BSI auf diese Weise schnell flächendeckend informieren und Gegenmaßnahmen empfehlen. Über den Informationsdienst Bürger-CERT veröffentlicht das BSI in diesen Fällen einen entsprechenden Hinweis zusammen mit Hilfestellungen für den Bürger, wie er sich vor Angriffen schützen kann.

Im „Tagesgeschäft" der BSI-Pressestelle hatten 2010 darüber hinaus zahlreiche weitere Themen Konjunktur. Dazu gehörten beispielsweise die Sicherheit von Handys und Smartphones und die Bekämpfung von Botnetzen im Rahmen des Anti-Botnetz-Beratungszentrums, das der eco Verband der deutschen Internetwirtschaft mit Unterstützung des BSI ins Leben gerufen hat. Zu aktuellen Themen veröffentlichte das BSI so allein in 2010 über 85 Presse- und Kurzmitteilungen. Die vielseitigen Themen der IT-Sicherheit sind also auf einem guten Weg, einen festen Platz in der Medienberichterstattung zu erlangen.

Auch die Politik beschäftigt sich vermehrt mit Fragen der IT-Sicherheit. Denn viele politische Projekte sind heutzutage auch IT-Projekte, in denen IT-Sicherheit eine zentrale Rolle spielt (z. B. Einführung von Smart Meter). Darüber hinaus ist die politische Aufmerksamkeit gestiegen, da die IT den Alltag mehr und mehr durchdringt und sowohl politische als auch wirtschaftliche Handlungsfähigkeit von gut funktionierender, aber auch gut geschützter IT abhängt. Diese beiden Entwicklungen spiegeln sich insbesondere im neuen BSI-Gesetz wieder und rücken zugleich das BSI in den Fokus der Politik.

Das Jahr 2010 war durch zahlreiche Gespräche mit nationalen und internationalen Politikern geprägt. Darüber hinaus war die fachliche Expertise des BSI in verschiedenen politischen Gremien wie etwa dem Innenausschuss des Deutschen Bundestages oder der IuK-Kommission des Ältestenrates gefragt. Dabei wurden die verschiedensten BSI-Themen wie z. B. der neue Personalausweis, die Sicherheit mobiler Kommunikation oder das BSI-Gesetz – hier hat das BSI gar eine ständige Berichtspflicht gemäß § 5 Absatz 10 BSIG gegenüber dem Innenausschuss – erörtert. Mit Blick auf das BSI-Gesetz und das Nationale Cyber-Abwehrzentrum wird die politische Aufmerksamkeit dem BSI auch 2011 erhalten bleiben.

Kommunizieren – mobil und geschützt

IT-Sicherheit und mobile Arbeitsplätze – SINA VW in der Praxis

Robert Rasten, Projektleiter SINA Entwicklung, und
Oliver Zendel, Projektleiter SINA VW-Maßnahme im KP II

Ein Produkt, das in der Theorie alle Anforderungen und Vorgaben umsetzt, ist nur dann etwas wert, wenn es auch die Möglichkeit bekommt, seine Praxistauglichkeit in der täglichen Nutzung unter Beweis zu stellen. Solch eine Chance zur Demonstration der Praxistauglichkeit ergab sich mithilfe einer Maßnahme des Konjunkturprogramms II, an der 14 Bundesbehörden teilnahmen. Ziel dieser Maßnahme war es, die IT-Sicherheit bei der Nutzung von mobilen Arbeitsplätzen durch den Einsatz von durch das BSI zugelassenen Komponenten zu erhöhen. Durch die Verwendung von SINA-VW-Laptops können Behörden praktisch erfahren, dass sich flexibles, IT-gestütztes, mobiles Arbeiten und IT-Sicherheit nicht zwangsläufig widersprechen müssen. Viel mehr ergänzen sie sich bei der Verwendung von modernen Verfahren und Techniken aus der Informatik und der IT-Sicherheit hervorragend.

Umsetzung in Pilotbehörden

Für die Umsetzung der Maßnahme wurden zuerst drei Pilotbehörden ausgewählt: das Bundeskanzleramt, das THW sowie das BSI. Durch die Auswahl dieser Behörden wurde eine breite Abdeckung von unterschiedlichen Einsatzszenarien erreicht und ein Verfahren zur Umsetzung der speziellen Anforderungen in die Praxis erarbeitet. Bei den Pilotbehörden wurde die SINA VW (Sichere Inter-Netzwerk Architektur Virtual Workstation) sowohl als alleiniger Arbeitsplatzrechner sowie als zusätzlicher mobiler Arbeitsplatzrechner erfolgreich eingesetzt.

Im Betrieb als alleiniger Arbeitsplatzrechner ermöglicht die SINA VW ihren Nutzern unter Wahrung der IT-Sicherheit eine bisher noch nicht erreichte Flexibilität

bei der Wahl ihres Arbeitsplatzes. Der „Status quo“ einer bisherigen IT-Ausstattung innerhalb eines Dienstgebäudes kann mithilfe einer Docking-Station und eines fest installierten Monitors erreicht werden. Die volle Flexibilität entfaltet dieses Szenario besonders dann, wenn Mitarbeiter ihren Arbeitsplatz auf Dienstreisen oder in ihr Home Office (z. B. für die Telearbeit) komplett „mitnehmen“ und somit ihre Produktivität und Arbeitsfähigkeit maximieren können. Die SINA VW unterstützt dieses Szenario durch die zugelassenen Sicherheitsfunktionen wie VPN-Tunnel, Festplattenverschlüsselung, starke Authentifizierung mithilfe einer Smartcard sowie die Abschottung der einzelnen Arbeitsplatzsitzungen. Im zweiten erprobten Einsatzfall hält die Behörde einen SINA VW-Pool ausschließlich für die mobile Nutzung bereit. Dieses Szenario ist dann sinnvoll, wenn nicht jeder Mitarbeiter eine SINA VW bekommen soll, es also mehr Nutzer als Geräte gibt. Ziel ist es, ein Verfahren zu schaffen, bei dem ein Nutzer für eine vorgegebene Zeit eine auf seine Bedürfnisse angepasste SINA VW zugeteilt wird. Eine Herausforderung ist dabei das Personalisieren der SINA VW, sodass der Benutzer alle benötigten Daten und Funktionen zur Verfügung hat.

Verfahren zur Einführung und Integration von SINA VW

Die Erfahrungen, die bei der Umsetzung dieser Szenarien in den Pilotbehörden gewonnen wurden, sollen zukünftigen SINA VW-Nutzern zur Verfügung stehen. Getreu der Devise „Von anderen lernen, heißt Fehler vermeiden“ entstehen so Blaupausen für den Einsatz von SINA VW, die anderen Behörden bei der Einführung dieses Produktes zugutekommen. So konnte im Rahmen der Maßnahme aus den Erfahrungen bei den drei Pilotbehörden ein Verfahren zur Einführung und Integration von SINA VW erstellt werden. Das Verfahren lässt sich grob in folgende vier Phasen unterteilen:

1. Aufbau der Netzwerk- und Zugangs-Infrastrukturkomponenten
2. Anpassen des Arbeitsplatz-Betriebssystems auf die Anforderungen eines mobilen Arbeitsplatzes
3. Integration der SINA VWs in die bestehenden Betriebs-Prozesse
4. Ausrollen der Geräte an die Benutzer.

SINA VW in der Praxis

Seit Mitte 2010 arbeiten die Führungskräfte des BSI ausschließlich mit SINA VW-Notebooks. Mit diesem System wird ein hohes Maß an Flexibilität bei gleichzeitig hohem Sicherheitsniveau sowohl im stationären als auch im mobilen Einsatz gewährleistet.

Horst Flätgen, Vizepräsident,
Bundesamt für Sicherheit in der Informationstechnik

Das Bundeskanzleramt braucht für seine Beschäftigten einen sicheren Fernzugriff auf das interne Netz. Wir begrüßen es sehr, dass das BSI hierfür eine Lösung gefunden hat, die der gesamten Bundesverwaltung zur Verfügung steht.

Dr. Till Nierhoff, Referat 114, Bundeskanzleramt

Die Bundesanstalt Technisches Hilfswerk betreibt Informationstechnik, um Aufgaben bei der Planung, Durchführung und Nachbereitung von Einsätzen zu unterstützen. Derzeit setzt das THW 54 SINA VWs im Produktivbetrieb ein, die von den Benutzern durchweg positiv bewertet werden.

Angela Huschmann, Referat Z5,
Bundesanstalt Technisches Hilfswerk

Der Einsatz von BSI-zugelassenen Komponenten hat beim BKA einen hohen Stellenwert. Ein Produkt einsetzen zu können, das wie die SINA VW besondere Sicherheitsanforderungen bei hoher Funktionalität unterstützt, trägt wesentlich zur Verbesserung der IT-Nutzung „vor Ort“ bei. So lassen sich insbesondere bei mobilen Ad-hoc-Einsätzen flexibel unterschiedliche Netze für die Anbindung an die zentrale IT nutzen. Hierdurch stehen den Einsatzkräften die erforderlichen polizeilichen Anwendungen zeitnah zur Verfügung. Durch die ergänzende Ausstattung der SINA VW-Laptops mit einer Telefonsoftware und einem Headset wird die VW auch als flexibles Telefon-Endgerät (sog. Voice over IP Softwarephone) genutzt. Bei bestehender VPN-Verbindung können hierdurch sichere Voice over IP-Sprachverbindungen mit der Dienststelle geführt und die vom Bürotelefon gewohnten Funktionalitäten genutzt werden. Ein großer Schritt zur sicheren IT-Nutzung „vor Ort“.

Klaus Schiel, IT 06, Bundeskriminalamt

Ab 2011 werden deutsche Soldaten im ISAF-Einsatz in Afghanistan nach Ausstattung mit SINA VW erstmals verschiedene Sicherheitsdomänen auf einem Endgerät nutzen und als zusätzlichen Synergieeffekt die Netz- und Systemadministration optimieren können.

Oberst i.G. Armin Fleischmann, IT-AmtBw

Dabei stellte sich heraus, dass der größte Aufwand für das Anpassen des Arbeitsplatz-Betriebssystems an die Anforderungen eines mobilen Arbeitsplatzes eingeplant werden sollte. Dies ist nicht verwunderlich, da die meisten Arbeitsplatz-Betriebssysteme in der Bundesverwaltung nicht für den Einsatz als mobiles System geplant und umgesetzt wurden. Damit bei der mobilen Anbindung geringe Bandbreiten und hohe Latenzen das System nicht aus dem Tritt bringen, sind oft am jeweiligen Arbeitsplatz-Betriebssystem Anpassungen und spezielle Optimierungen notwendig. Dies sind jedoch lohnende Investitionen in die behördeneigene IT-Infrastruktur, da sie erstens den Arbeitsplatz fit für den mobilen Einsatz machen und zweitens die nicht-mobilen Arbeitsplätze in der Regel von den positiven Effekten durch die Optimierungen profitieren.

Mitte Juni 2010 war das Verfahren für die Einführung von SINA VW soweit gefestigt, dass innerhalb der Maßnahme weitere Behörden mit Geräten ausgerüstet werden konnten. In dieser zweiten Welle wurde bei elf Behörden der Grundstein für den Betrieb von SINA VW gelegt.

SINA VW im BSI

Einen besonderen Stellenwert nimmt die Pilotinstallation der SINA VW innerhalb des BSI ein. Zum einen ist es ein Zeichen von Glaubwürdigkeit, dass die Behörde, die für das System verantwortlich zeichnet, dieses auch in möglichst großer Stückzahl einsetzt. Zum anderen ermöglicht der Einsatz innerhalb des BSI wertvolle Rückschlüsse auf die weitere Entwicklungsrichtung. Über 70 Mitarbeiterinnen und Mitarbeiter des BSI verwenden bereits die SINA VW als alleinigen Arbeitsplatz für ihre tägliche Arbeit. Besonders hervorzuheben ist dabei, dass die Amtsleitung inklusive der Abteilungsleiter frühzeitig auf die ausschließliche Nutzung der SINA VW umstellte. Durch die Auswahl unterschiedlicher Benutzertypen konnte nachgewiesen werden, dass die SINA VW in allen Ebenen einer Organisation einsatzfähig ist und die jeweiligen Aufgaben mit dem notwendigen Maß an IT-Sicherheit unterstützt.

Praxistauglichkeit erwiesen

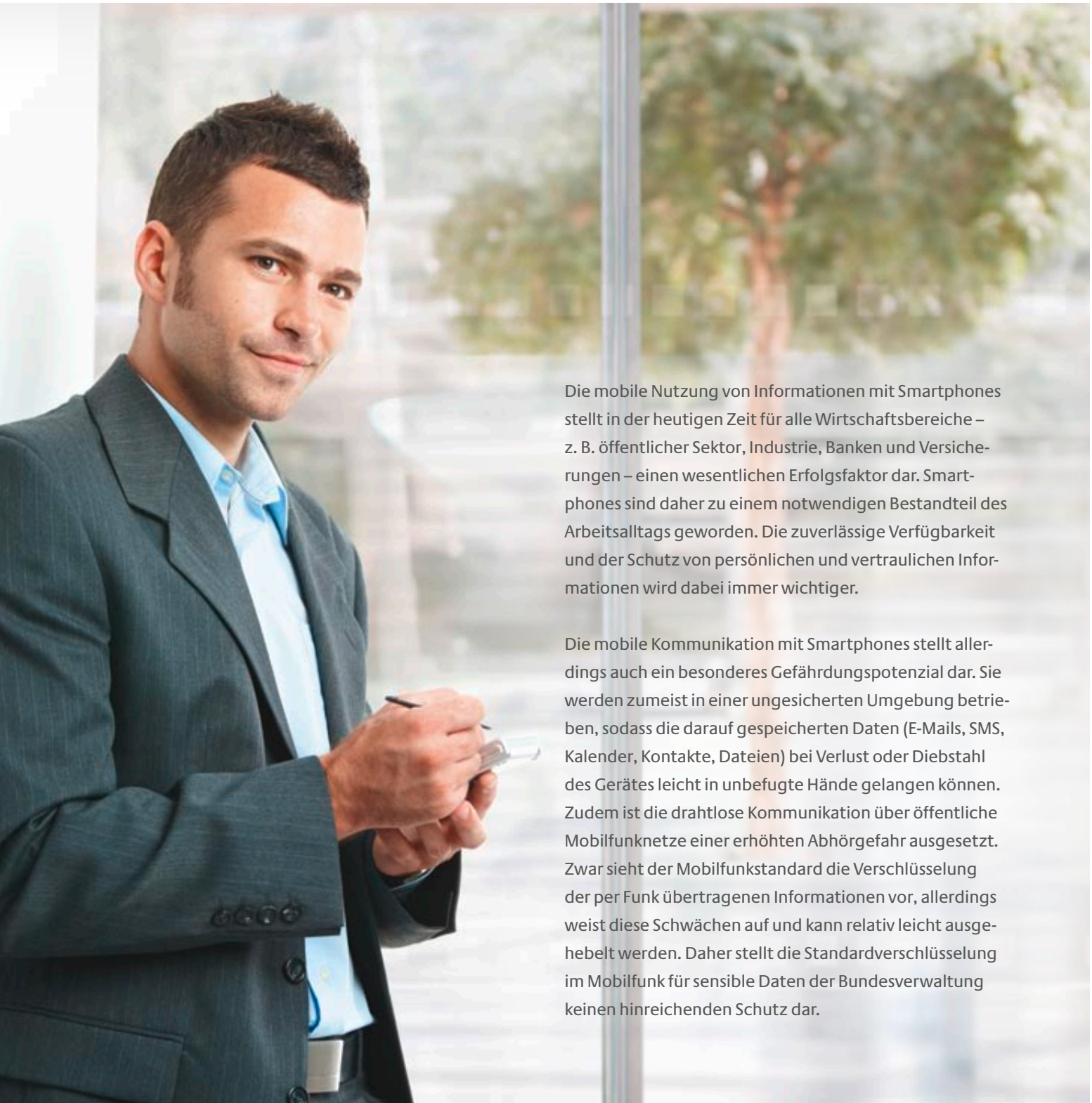
Bislang wurden 700 SINA Virtual Workstations in der Bundesverwaltung etabliert. Zusätzlich wurden Blaupausen entwickelt, die es Behörden einfacher machen, mobile Arbeitsplätze auf Basis von SINA VW in ihre IT-Infrastruktur zu integrieren. Die Maßnahme hat eindrucksvoll demonstriert, dass seit 2010 ein praxistaugliches Produkt existiert, das die Flexibilität von mobilem Arbeiten konsequent und verlässlich mit den hohen Anforderungen des Schutzes von sensiblen Informationen kombiniert. Die bei der Einführung in den unterschiedlichen Behörden gewonnenen Erkenntnisse, z. B. im Bereich Gerätemanagement, werden für die gezielte Weiterentwicklung verwendet. Aufgrund des Erfolges bei der Einführung der SINA VW in der Bundesverwaltung wurde entschieden, die Maßnahme um ein weiteres Jahr zu verlängern und der Bundesverwaltung zusätzliche SINA VW zur Verfügung zu stellen.

Auch beim mobilen Arbeiten muss ein hohes Sicherheitsniveau erreicht werden

BSI macht sicher mobil:

Lösungen für eine optimal geschützte Kommunikation mit Smartphones in der Bundesverwaltung

Joachim Opfer, Fachbereichsleiter Abhörsicherheit im BSI, und Marion Brinkkötter, Referentin im Projektteam SNS im BSI



Die mobile Nutzung von Informationen mit Smartphones stellt in der heutigen Zeit für alle Wirtschaftsbereiche – z. B. öffentlicher Sektor, Industrie, Banken und Versicherungen – einen wesentlichen Erfolgsfaktor dar. Smartphones sind daher zu einem notwendigen Bestandteil des Arbeitsalltags geworden. Die zuverlässige Verfügbarkeit und der Schutz von persönlichen und vertraulichen Informationen wird dabei immer wichtiger.

Die mobile Kommunikation mit Smartphones stellt allerdings auch ein besonderes Gefährdungspotenzial dar. Sie werden zumeist in einer ungesicherten Umgebung betrieben, sodass die darauf gespeicherten Daten (E-Mails, SMS, Kalender, Kontakte, Dateien) bei Verlust oder Diebstahl des Gerätes leicht in unbefugte Hände gelangen können. Zudem ist die drahtlose Kommunikation über öffentliche Mobilfunknetze einer erhöhten Abhörgefahr ausgesetzt. Zwar sieht der Mobilfunkstandard die Verschlüsselung der per Funk übertragenen Informationen vor, allerdings weist diese Schwächen auf und kann relativ leicht ausgehebelt werden. Daher stellt die Standardverschlüsselung im Mobilfunk für sensible Daten der Bundesverwaltung keinen hinreichenden Schutz dar.

IT-Investitionsprogramm: Mehr Produkte sorgen für mehr mobile Sicherheit

Zu Beginn des Jahres 2009 hat die Bundesregierung das IT-Investitionsprogramm im Rahmen des Pakts für Beschäftigung und Stabilität in Deutschland beschlossen. Innerhalb dieser Maßnahme wurden Produkte für die sichere mobile Sprach- und Datenkommunikation in der Bundesverwaltung beschafft, die dem Sicherheitsbedürfnis der Bundesverwaltung Rechnung tragen und den Sicherheitsanforderungen des BSI entsprechen. BMI und BSI sind für diese Maßnahme verantwortlich. Das BSI ist dabei mit der federführenden Umsetzung betraut.

SiMKo2 ermöglicht sicheren Datenaustausch mit mobilen Endgeräten

Für die sichere mobile E-Mail- und PIM[4]-Kommunikation wurde das System SiMKo2 der Firma T-Systems ausgewählt. Es verfügt als einziges Produkt auf dem Markt über eine spezifische Einsatzempfehlung für Verschlusssachen bis VS-NfD (Verschlussache – Nur für den Dienstgebrauch). SiMKo2 gewährleistet durch den Einsatz von Virtual Private Network (VPN)-Technologie einen sicheren Austausch von E-Mail und PIM-Daten zwischen mobilen Endgeräten (PDAs) und einem Unternehmensserver. Alle auf dem Endgerät abgelegten Daten werden verschlüsselt. Die Authentisierung erfolgt zertifikatsbasiert unter Nutzung der Public-Key-Infrastruktur der Bundesverwaltung (V-PKI). Unter den obersten Bundes- und Sicherheitsbehörden wurde ein Erstbedarf von insgesamt 4000 Geräten in 30 Behörden ermittelt. Im Laufe des Jahres 2010 wurde in der Folge Schritt für Schritt die vorhandene IT-Infrastruktur für den Betrieb von SiMKo2 ergänzt und angepasst. Dabei mussten die spezifischen Anforderungen und Rahmenbedingungen der Bedarfsträger berücksichtigt werden – wie z. B. Hochverfügbarkeitsanforderungen, Virtualisierung oder Austausch von Firewalls bzw. Integration vorhandener Firewalls. Um den kurzen Produktzyklen auf dem Smartphone-Markt und den Wünschen der Nutzer nach möglichst aktuellen Geräten Rechnung zu tragen, werden fortlaufend marktgängige Smartphones für den sicheren Betrieb im SiMKo2-System adaptiert. Jeder neue SiMKo2-Endgerätetyp wird dabei einer Sicherheitsevaluierung unterzogen – und die Einhaltung der Sicherheitsstandards mit einer Einsatzempfehlung des BSI attestiert. Derzeit stehen die Smartphones touch hd, snap und touch pro2 des Herstellers htc als Endgeräte mit einer BSI-Einsatzempfehlung zur Auswahl. Weitere Geräte werden entsprechend dem aktuellen Angebot des Smartphone-Marktes folgen. Auch Sprach- und SMS-Kommunikation sind mit SiMKo2 möglich – allerdings erfolgt die Übertragung zur Zeit noch ohne zusätzliche Verschlüsselung. Die Erweiterung der SiMKo-Geräte um eine Komponente für die Sprach- und SMS-Verschlüsselung, die dem BSI-Standard für die sichere netzübergreifende Sprachkommunikation (SNS) genügt, ist die nächste Herausforderung.

„Die Standardverschlüsselung im Mobilfunk stellt für die sensiblen Daten der Bundesverwaltung keinen hinreichenden Schutz dar.“

Joachim Opfer

SNS – BSI-Standard für die Sichere Netzübergreifende Sprachkommunikation

Um hoch entwickelten Lauschangriffen – z. B. mit IMSI-Catcher[5] und Rainbow-Tables – auf die mobile Sprachkommunikation und auf Kurznachrichten entgegenzuwirken, existieren diverse Ende-zu-Ende-Verschlüsselungssysteme. Durch die meist herstellerspezifische Hard- und/oder Software werden die zwischen den mobilen Endgeräten ausgetauschten Informationen vor dem Zugriff Dritter geschützt. Eine Interoperabilität zwischen Systemen verschiedener Hersteller ist dabei allerdings nicht gegeben. Vielmehr können die Nutzer solcher Kryptohandys nur zu Geräten desselben Herstellers sichere Verbindungen aufbauen. Nutzbarkeit und praktische Bedeutung dieser Systeme wurden dadurch bisher stark eingeschränkt. Abhilfe konnte ein herstellerunabhängiger Standard schaffen: Das BSI hat einen solchen Interoperabilitätsstandard in 2010 im Rahmen des IT-Investitionsprogramms und in Kooperation mit Herstellerfirmen wie Rohde & Schwarz SIT, Secusmart und T-Systems entwickelt.

Klares Ziel dieser Standardisierung der Sicheren Netzübergreifenden Sprachkommunikation (SNS): Die Funktionen „sichere Telefonie“ und „sichere Kurznachrichten (SMS)“ technisch so realisieren und zu definieren, dass:

- die Interoperabilität zwischen Herstellern gewährleistet ist,
- gleichzeitig aber herstellerspezifische Lösungen unterstützt werden,
- die Nutzung unterschiedlichster Kommunikationsverbindungen und Netze möglich ist und
- insgesamt ein Sicherheitsniveau VS-NfD erreicht wird.

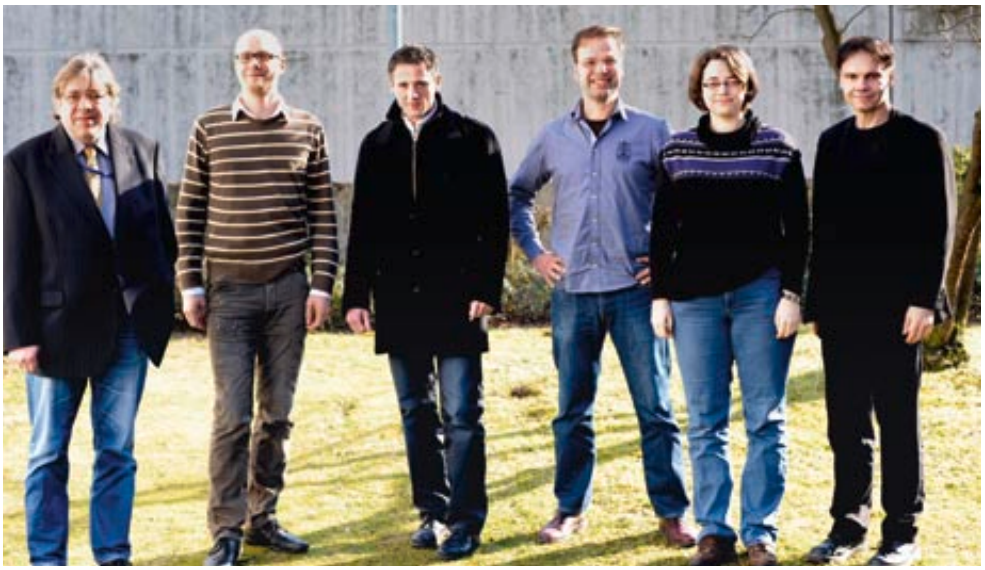
Weiterhin sollte die Bundesverwaltung mit Endgeräten ausgestattet werden, die diesen Standard unterstützen.

Rund 5.600 Geräte mit SNS-Standard bereits im Einsatz

Die erste Version des SNS-Standards wurde im März 2010 fertiggestellt und steht seitdem allen interessierten Herstellerfirmen zur Verfügung. Schon in den folgenden Monaten wurden die ersten Geräte nach SNS-Standard von Rohde & Schwarz SIT und Secusmart entwickelt und bis zum Ende des Jahres konnten bereits rund 5600 dieser neuen Geräte an die Bundesverwaltung ausgeliefert werden.

In der Entwicklung: Ab 2011 auch Festnetz SNS-fähig

Damit die Nutzer nicht ausschließlich auf Handys für die sichere Sprachkommunikation angewiesen sind, sondern SNS-Gespräche auch am Festnetztelefon des Arbeitsplatzes entgegennehmen können, befinden sich derzeit auch SNS-fähige Festnetzgegenstellen in der Entwicklung und werden noch im Jahr 2011 auf den Schreibtischen der Bundesverwaltung stehen. Das ebenfalls in der Entwicklung befindliche prototypische TETRA[6] ◄► PSTN[7] Gateway wird einen Übergang vom Telefonnetz in das neue digitale BOS[8] (Polizei)-Funknetz schaffen. Dadurch wird die sichere Telefonie zwischen TETRA-Funkgeräten und sicheren Mobiltelefonen ermöglicht.



Das SNS-Team im BSI: Dr. Frank Niedermeyer, Dr. Sören Werth, Christian Schridde, Matthias Hirsch, Marion Brinkkötter, Dr. Antonius Klingler (v.l.n.r.)

Nahtlose Integration in andere Netze

Der Standard für Sichere Netzübergreifende Sprachkommunikation wurde kanal- und netzunabhängig konzipiert. Derzeit werden für die mobile Kommunikation der Datendienst des GSM-Netzes und der ISDN-Datenkanal des Festnetzes verwendet. Beim Aufbau einer Verbindung wird von den Endgeräten ohne Einwirkung der Nutzer ein Betriebsmodus ausgehandelt. Dieser legt die technischen Randbedingungen fest, die bei dem folgenden Gespräch zum Einsatz kommen. Um in jedem Fall Interoperabilität zu gewährleisten, bietet der SNS-Standard zwei Betriebsmodi, die von allen zugelassenen Endgeräten unterstützt werden müssen:

- Betriebsmodus 1 wurde in Anlehnung an das für den TETRA-Standard entwickelte Verschlüsselungsverfahren definiert. Mit Unterstützung eines Gateways ermöglicht er die sichere Kommunikation zwischen BOS-Funkgeräten und SNS-Kryptohandys.
- Betriebsmodus 2 kommt bei Telefonaten innerhalb des PSTN-Netzes zum Einsatz und ist in der Lage, die zur Verfügung stehende Bandbreite vollständig auszunutzen. Dadurch wird eine bessere Sprachqualität erreicht.

Pluspunkt: Standard ist offen für Ergänzungen

Der Standard erlaubt es, weitere Modi zu ergänzen. Vorteil: Hersteller können so ihr eigenes Konzept erhalten und ihren Kunden z. B. weitere Optionen oder bessere Sprachqualität zur Verfügung stellen. Als Sicherheitsanker für die beiden vom Standard vorgegebenen Betriebsmodi wurde der BOS Kryptochip gewählt. Er schützt die besonders sicherheitskritischen Schlüssel und Verschlüsselungsfunktionen vor Viren und anderen Schadprogrammen. Ursprünglich wurde der Chip vom BSI für das neue digitale Netz der Behörden und Organisationen mit Sicherheitsaufgaben (BOS-Netz) entwickelt. Daher ermöglicht der Einsatz des Kryptochips die Interoperabilität mit der Ende-zu-Ende-Verschlüsselung des BOS-Netzes. Er kann von Herstellern für den Einsatz in ihren Produkten lizenziert werden. Die Aushandlung der Gesprächsschlüssel erfolgt individuell zu Beginn des Gesprächs über ein Diffie-Hellman-Protokoll. Die Authentizität der Nutzer ist PKI-basiert sichergestellt und wird bei Verbindungsaufbau geprüft. Das Zertifikat ist jeweils auf der Karte hinterlegt. Derzeit unterstützt der SNS-Standard im Bereich der Sprachkommunikation ausschließlich Telefonie, technisch Vollduplexrufe. Es wurden allerdings Vorkehrungen getroffen, um den Standard zu einem späteren Zeitpunkt auch auf klassischen Funkbetrieb, d.h. Gruppenkommunikation, erweitern zu können. Dadurch wird die nahtlose Integration in das BOS-Netz ermöglicht. Für den Austausch sicherer Kurznachrichten handeln die Endgeräte während der Sprachkommunikation Schlüssel aus – ohne Eingreifen des Nutzers und ohne Einbußen bei der Sprachqualität. Diese werden verschlüsselt abgelegt und automatisch gewechselt. Das Versenden von verschlüsselten Kurznachrichten zwischen Telefonnetz und BOS-Netz ist ebenfalls möglich.

„Der Standard für Sichere Netzübergreifende Sprachkommunikation wurde kanal- und netzunabhängig konzipiert.“

Marion Brinkkötter

[4] PIM: Personal Information Manager
[5] IMSI-Catcher simulieren eine Basisstation, sodass der Angreifer durch einen Man-In-The-Middle-Angriff Zugang zum Gespräch des Opfers erhält. Für mehr Informationen sei auf die Broschüre "Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte" (PDF) und den Sicherheitshinweis des BSI verwiesen.
[6] TETRA: Terrestrial Trunked Radio
[7] PSTN: Public Swiched Telephone Network
[8] BOS: Behörden und Organisationen mit Sicherheitsaufgaben

Sichere elektronische Identitäten

Der neue Personalausweis:

Technische Konzepte für erweiterte Funktionalität

Bernd Kowalski, Abteilungsleiter im BSI

Der neue Personalausweis

Seit November 2010 steht dem Bürger mit dem neuen Personalausweis nicht nur ein Sichtausweis im neuen Scheckkartenformat zur Verfügung. Das Ausweisdokument bietet zusätzlich verschiedene elektronische Funktionen, die auch im Internet für deutlich mehr Sicherheit sorgen. Dazu zählt zum einen der elektronische Identitätsnachweis, die sogenannte Online-Ausweisfunktion, mit der sich der Bürger zweifelsfrei online ausweisen kann. Ein in den Ausweis integrierter Radio Frequency Chip (RF-Chip) enthält dazu alle Informationen, die auch visuell von dem Dokument ablesbar sind. Mit der Unterschriftsfunktion der qualifizierten elektronischen Signatur kann der Nutzer darüber hinaus Dokumente und Willenserklärungen rechtssicher online unterschreiben. Im Unterschied zur Online-Ausweisfunktion muss er hierzu ein kostenpflichtiges Zertifikat erwerben und auf den Ausweischip laden.

Vorteil für den Bürger:
Mehr Sicherheit für die eigenen Daten
Neben der Online-Ausweis- und der Unterschriftsfunktion werden auf dem RF-Chip des neuen Personalausweises auch biometrische Daten gespeichert. Diese sorgen für eine stärkere Bindung des Ausweisinhabers an das Dokument, das ihm damit eindeutig zuzuordnen ist. Die biometrischen Daten lassen sich ausschließlich durch die zur Identitätsfeststellung berechtigten Behörden zum Beispiel im Rahmen von Polizei-, Grenz- und Zollkontrollen auslesen. Dabei kann nicht nur auf die Angaben zur Person, sondern auch auf das Lichtbild und die Fingerabdrücke, die der Bürger freiwillig erfassen lassen kann, zugegriffen werden.

„Die elektronischen Funktionen des neuen Personalausweises bieten vielfältige Möglichkeiten, den Zugang zu E-Business- oder E-Government-Dienstleistungen neu zu gestalten.“

Bernd Kowalski

Mit der Einführung des neuen Personalausweises am 1. November 2010 hat das Projekt seinen vorläufigen Höhepunkt gefunden, an dem das BSI mehrere Jahre intensiv gearbeitet hat und das es auch künftig weiter beschäftigen wird. Die ersten Ideen für den (damals noch) „digitalen Personalausweis“ wurden bereits im Jahr 2002 diskutiert. Schon in dieser Phase war das BSI an der Konzeptionierung beteiligt. Es wurden zentrale Eigenschaften des Ausweises wie starke Zugriffskontrollen und gegenseitige Authentisierung auf Basis technischer Konzepte des BSI festgelegt.

BSI sichert technische Qualität

Im Zuge der Einführung des neuen Personalausweises im Jahr 2010 hat das BSI die Sicherheitsstandards etabliert und gewährleistet die Qualität der technischen Prozesse, die die Nutzung des Ausweises im Internet ermöglichen durch Fortschreibung und Pflege dieser Standards. Der Ausweischip selbst sowie für den Ein-

Als Ergebnis der erfolgreichen Tests beginnen Unternehmen und Behörden damit, Anwendungen mit der Online-Ausweis- oder Unterschriftsfunktion anzubieten

satz verwendete Geräte und Programme werden vom BSI zertifiziert. Sie müssen hierzu IT-Sicherheitsanforderungen nach spezifischen Technischen Richtlinien und Schutzprofilen des BSI erfüllen. Dies soll neben der Datensicherheit insbesondere auch die Interoperabilität sämtlicher Komponenten sicherstellen. Die technische Prüfung erfolgt durch vom BSI anerkannte Prüfstellen.

Die Erstellung der Spezifikationen ging fließend in die Betreuung der beteiligten öffentlichen Stellen und privaten Unternehmen bei der Umsetzung über. Angefangen bei technischen Pilotierungen bis hin zum Feldtest – zum Zweck der Anbindung der Kommunen – und den Anwendungstests, die der Integration von Anwendungen der Dienstanbieter dienten.

Neue Möglichkeiten für die Gestaltung von Geschäftsprozessen

Die elektronischen Funktionen des neuen Personalausweises bieten vielfältige Möglichkeiten, den Zugang zu E-Business- oder E-Government-Dienstleistungen neu zu gestalten. In den praktischen Tests haben weit über 200 Unternehmen und Behörden in den Jahren 2009 und 2010 die neue Online-Ausweis- und Unterschriftsfunktion erprobt und versuchsweise in ihre Geschäftsprozesse integriert. Dabei galt es insbesondere, die Praxistauglichkeit, Handhabbarkeit und Akzeptanz des neuen elektronischen Identitätsnachweises zu testen. Als Ergebnis der erfolgreichen Tests und der Einführung des neuen Personalausweises beginnen Unternehmen und Behörden damit, Anwendungen mit der Online-Ausweis- oder Unterschriftsfunktion anzubieten.

Die AusweisApp – erfolgreicher Einsatz trotz schwierigem Start

Zur Nutzung der Online-Ausweisfunktion braucht der Inhaber eine Client-Software, z. B. die kostenlos bereitgestellte „AusweisApp“, sowie ein kontaktloses Kartenlesegerät, das er an seinen PC anschließt. Ausweisinhaber und auch Diensteanbieter können sich zweifelsfrei ausweisen, und die sichere Kommunikation zwischen Bürgerinnen oder Bürgern und Behörden oder Unternehmen im Internet wird erheblich vereinfacht.

Kurz nach der Bereitstellung im November 2010 hat das BSI die AusweisApp wegen einer Sicherheitslücke, die trotz umfangreicher vorbereitender Testmaßnahmen mit zahlreichen namhaften Unternehmen aufgetreten ist, kurzfristig wieder vom Netz genommen und wenig später eine überarbeitete Version der Software bereitgestellt. Die Sicherheit des nPA und der darauf geschützt abgespeicherten Daten waren durch die Sicherheitslücke nicht betroffen. Dennoch hat das BSI die mit dem Updateverfahren verbundenen Prozesse einer eingehenden Prüfung unterzogen, um seitens der Nutzer und Diensteanbieter gemeldete Probleme mit der AusweisApp schnellstmöglich auszuwerten und erforderliche Updates schnell bereitstellen zu können. Kumulierte Updates sollen künftig zudem Verbesserungen der Funktionalität, Benutzerfreundlichkeit und Performance sicherstellen.

Ein Mehr an Datensicherheit

Gerade vor dem Hintergrund der anhaltend hohen Gefährdungslage sind die elektronischen Funktionen des neuen Personalausweises ein Schritt in Richtung mehr Datensicherheit. Die auf dem Ausweischip gespeicherten Daten sind bei der Übermittlung durch sichere kryptografische Protokolle verschlüsselt. Gleiches gilt auch für den Kommunikationspartner (Behörde, Unternehmen) bei der gegenseitigen Authentisierung: Seine Daten werden ebenfalls verschlüsselt übertragen. Der Ausweisinhaber hat zu jedem Zeitpunkt doppelt abgesichert durch Besitz und Wissen die volle Nutzerkontrolle über seine Daten, solange er weder den Besitz der Ausweiskarte aufgibt, noch die PIN preisgibt.

Der nPA in der Praxis

Die DATEV eG, Nürnberg, ist ein Softwarehaus und IT-Dienstleister für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sowie deren Mandanten. Die DATEV integriert die eID-Funktion in ein Arbeitnehmer-Portal, um damit den sicheren Online-Zugriff auf zum Beispiel Lohn- und Gehaltsabrechnungen gewährleisten zu können. Für die Anmeldung an einem solchen Arbeitnehmer-Portal wird der elektronische Identifizierungsnachweis mit dem neuen Personalausweis vorausgesetzt. Begonnen wird dabei mit der Online-Bereitstellung der Gehaltsabrechnung für etwa 700 DATEV-Mitarbeiter. Die Abrechnung kann von den Teilnehmern im Internet eingesehen, heruntergeladen und ausgedruckt werden. Geplant ist, diese und weitere Cloud-Services rund um das Beschäftigungsverhältnis als generelle Dienstleistung von Steuerberatern und Arbeitgebern anzubieten.

„Über entsprechend gesicherte DATEV-IT-Dienste ist den DATEV-Mitgliedern und deren Mandanten der Umgang mit dem Prinzip ‚Besitz und Wissen‘ vertraut. Der nPA wird DATEV-myIDentity und die DATEV-SmartCard ergänzen und so u.a. Online-Dienste für Arbeitnehmer ermöglichen. Beim nPA-Konzept erscheint uns u.a. wichtig, dass sich zunächst die Anbieter per Berechtigungszertifikat beim Anwender online ausweisen müssen und angezeigt wird, welche Daten vom nPA für ein bestimmtes Nutzungsszenario gelesen werden dürfen. Das schafft Vertrauen beim Anwender und ermöglicht die Gewährleistung zentraler Datenschutzanforderungen.“

Prof. Dieter Kempf, Vorstandsvorsitzender DATEV eG

Der neue Personalausweis – ein Vorzeigeprojekt für Deutschland

Fujitsu ist das erste Unternehmen, das den neuen Personalausweis in seine eCommerce-Plattform integrierte. Seit November 2010 können nPA-Inhaber in Deutschland mit dem neuen Dokument im „Fujitsu Online Shop Deutschland“ Produkte bestellen und die Lieferung nachverfolgen. Die Online-Ausweisfunktion des nPA wird dabei direkt in den Online-Bestellprozess integriert. So lassen sich die Geschäftsfähigkeit sowie die Identität eines Käufers schnell und auf datenschutzkonforme Weise feststellen. Der Kunde profitiert von schnelleren und bequemeren Bestellprozessen.

„Der neue Personalausweis ist ein weltweit einzigartiges Projekt – und wir von Fujitsu sind stolz darauf, ein Anbieter der ersten Stunde zu sein: Im Online-Shop von Fujitsu können sich Anwender bereits jetzt mit dem neuen Ausweis registrieren. Von der Technologie profitiert aber nicht nur der Bürger – sondern sie hilft Unternehmen ebenso wie der öffentlichen Verwaltung, Geschäftsprozesse effizienter zu gestalten und so Online-Angebote einfach, sicher und damit kundenfreundlicher zu machen.“

Rolf Schwirz, CEO Fujitsu Technology Solutions.

Der neue deutsche Personalausweis im europäischen Umfeld

Dr. Andre Braunmandl, BSI Projektleiter STORK eID-LSP

Im Zeitalter elektronischer Geschäftsprozesse, großer Online-Plattformen für Handel, Auktionen, Informationsgewinnung und Freizeitgestaltung sind Datenschutz und Vertrauenswürdigkeit von Online-Angeboten sowie die Sicherheit von Online-Transaktionen von zentraler Bedeutung. Die im BSI entwickelten elektronischen Funktionen für den neuen deutschen Personalausweis leisten hier mit der sicheren und vertrauenswürdigen Funktion zur elektronischen Authentisierung (Online-Ausweis- oder eID-Funktion) einen wertvollen Beitrag.

Damit die Bundesbürger die Vorteile des neuen Personalausweises auch bei Internetangeboten aus ganz Europa nutzen können, beteiligt sich das BSI aktiv an dem von der Europäischen Union geförderten Zusammenwirken (Interoperabilität) der europäischen eID-Lösungen. Um die in den EU-Mitgliedstaaten geschaffenen Möglichkeiten zur elektronischen Authentisierung synergetisch für Europa zu nutzen, hat die Europäische Kommission mit STORK (Secure Identity Across Borders Linked) ein groß angelegtes Pilotprojekt (Large Scale Pilot, LSP) aufgelegt. Es bündelt in den Jahren 2008 bis 2011 die europäischen Aktivitäten zur interoperablen Nutzung elektronischer Identitäten. Dem durchführenden STORK-Konsortium gehörten zunächst 29 Mitglieder aus 14 Mitgliedstaaten an. Seit Beginn des Jahres 2010 ist STORK um drei weitere Mitglieder aus bisher nicht beteiligten Mitgliedstaaten erweitert worden. Das BSI war von Anfang an umfangreich an STORK beteiligt und wird die Projektergebnisse entscheidend in den fortlaufenden Ausbau der deutschen eID-Infrastruktur einfließen lassen.

Für Europa ist die Interoperabilität der nationalen eID-Lösungen ein wesentlicher Schritt zur Harmonisierung. Grenzüberschreitende eGovernment-Dienstleistungen für die EU-Bürger wie zum Beispiel im Rahmen der Dienstleistungsrichtlinie werden zu einem großen Teil erst dadurch ermöglicht. Das Instrument des Large Scale Pilot (LSP) ist hier besonders erfolgversprechend, da auf diese Weise sämtliche Schlüsselakteure der eID-Lösungen aus den verschiedenen EU-Mitgliedstaaten an einen Tisch gebracht werden.

Ein europäisch-interoperabler Ansatz

Die eID-Infrastruktur des neuen deutschen Personalausweises erfüllt erstmalig die hohen europäischen Anforderungen an Datenschutz und Sicherheit. Sie ist damit in besonderem Maße geeignet, die Vision der Europäischen Kommission einer paneuropäischen E-Government-Struktur zu ermöglichen. Das im STORK eID-LSP erarbeitete Modell zur Herstellung der Interoperabilität der europäischen eID-Systeme sieht die Verknüpfung der unterschiedlichen nationalen Systeme über nationale Knotenpunkte, sogenannte PEPS (Pan-European-Proxy-Services), vor. Das deutsche Modell berücksichtigt eine ausschließlich direkte Kommunikation zwischen Dienstanbietern und Ausweisinhabern mittels des neuen deutschen Personalausweises. Vor diesem Hintergrund ist es die Aufgabe des BSI, die Grundlagen zu schaffen, dass die Berechtigungszertifikate der europäischen Dienstanbieter sicher in den PEPS gespeichert werden und dass nur der berechtigte Dienstanbieter über das auf ihn ausgestellte Berechtigungszertifikat Zugang zu den personenbezogenen Daten des Ausweisinhabers erhalten kann. Hierzu ist auf europäischer Ebene eine sichere, vertrauenswürdig authentisierte Verbindung der Dienstanbieter zu ihren nationalen PEPS erforderlich. Gemeinsam mit Industriepartnern hat das BSI eine Lösung erarbeitet, die bis 2011 im Rahmen von STORK pilotiert wird. Damit ist eine europäisch interoperable Lösung greifbar.

Was kommt nach STORK?

Die Verbindung der nationalen eID-Systeme über PEPS löst nur einen Teil der bestehenden Interoperabilitätsproblematik. Unter dem Gesichtspunkt der Mobilität bleibt das Problem bestehen, dass die EU-Bürger bei Reisen in die anderen Mitgliedstaaten Hard- und Software mitführen müssten, um sich über ihre eID-Token authentisieren zu können. Dies ist offenkundig nicht praktikabel. Um eID als die Basistechnologie in Europa zu etablieren, auf der grenzüberschreitende Anwendungen entwickelt werden können, plant die Europäische Kommission derzeit, die Interoperabilität von eID auch nach STORK weiter zu entwickeln. Dabei sind sich alle Beteiligten einig, dass die Interoperabilität von eID ein infrastruktureller Faktor ist, der wesentlich zur Wettbewerbsfähigkeit der modernen europäischen Wirtschaft beiträgt. Das BSI wird die Entwicklungen in diesem Bereich weiter aktiv begleiten – und so als europäischer Impulsgeber wirken.

„Im Rahmen der langjährigen und engen Zusammenarbeit mit dem BSI konnte T-Systems seit Projektbeginn STORK mit dem BSI zusammenarbeiten. Dabei koordiniert T-Systems eine Gruppe von deutschen Industriepartnern. Gemeinsames Ziel im Projekt ist die Beibehaltung und das Ausrollen der hohen deutschen Sicherheitsstandards bei der ebenfalls angestrebten Harmonisierung oder - konkreter - Interoperabilität der unterschiedlichen nationalen eID-Lösungen. Basierend auf der vertrauensvollen und engen Abstimmung mit dem BSI kann Deutschland im Projekt STORK eine maßgebliche Rolle wahrnehmen, die sich speziell im von deutscher Seite geleiteten Anwendungspiloten 1 widerspiegelt. Neben den hoheitlichen Anwendungen, die national im Anwendungstest und international in den STORK-Piloten demonstriert werden, ermöglicht die engagierte Beteiligung des BSI und die intensive Zusammenarbeit mit der deutschen Industrie den Aufbau einer eID-Infrastruktur, die auch für kommerzielle Anwendungen nutzbar sein wird.“

Volker Reible, Vice President Large Scale Project Management, T-Systems International GmbH

Herausforderungen gemeinsam angehen

"In the Age of Internet, No Country is an Island."

Four questions for Neelie Kroes, Vice-President of the European Commission and Digital Agenda Commissioner

In 2010 the European Commission adopted the Digital Agenda, which is Europe's strategy for a flourishing digital economy by 2020. As trust and security are crucial to this endeavor, what are the most important measures for the EU to strengthen network and information security?

The Digital Agenda for Europe (DAE) is one of the flagship initiatives under the Europe 2020 Strategy. It reflects our vision on the efforts we need to make in the next few years to fully embrace the digital society. It clearly identifies trust and security in the online world as key contributors to a vibrant digital society and to smart, sustainable and inclusive growth. In the trust and security pillar of the DAE, we define 14 action points that aim at improving Europe's capability to prevent, detect and respond to network and information security (NIS) problems and to fight cybercrime. Some address data protection issues, awareness raising measures and child protection in a safer internet environment. Coordination at EU level and the tasks of Member States as well as areas for cooperation on a global scale are also mentioned. Among the key priorities I would highlight the cooperation of Computer Emergency Response Teams (CERTs) and fostering the multi-stakeholder dialogue between public and private sector.

Let me give you a couple of examples of what we have already accomplished. On September 30, 2010, the Commission presented to the European Parliament and the Council of Ministers a proposal for a regulation modernizing and reinforcing ENISA, the European Network and Information Security Agency. On the same day, the Commission also tabled a proposal for a directive on attacks against information systems to deal with new cyber crimes, such as large-scale cyber attacks. This was followed by the first pan-European cyber-security preparedness exercise on November 4, 2010, called "Cyber Europe 2010", which took place with the participation of all Member States and the support of ENISA and the EU Joint Research Centre.

Cyber attacks in particular are growing in sophistication and frequency. What are the Member States' and the European Union's roles and responsibilities in protecting Europe?

Addressing cyber threats and strengthening security in the digital society is a shared responsibility – of individuals as much as of private and public bodies, both at home and globally. Member States are primarily responsible for national cyber security strategies and

their implementation. However, the security of each Member State depends also on the cyber security level in other Member States. The collective aim should be to achieve a high level of NIS throughout Europe and to overcome the existing significant differences between Member States in terms of preparedness and capabilities. Let's keep in mind that we are all interconnected and that a chain is only as strong as its weakest element. In the age of Internet, no country is an island – and I am glad to see that this has been very well understood in Germany. The EU, notably through ENISA, also plays its role in this very dynamic environment. Firstly, we support Member States in their efforts to improve their cyber security capabilities. Secondly, we promote and support cooperation between Member States and the private sector on prevention, preparedness and response. Thirdly, we strive to create a level playing field for NIS in Europe to ensure that industry and businesses find their way in the diversity of security requirements and practices.

Which leads to the question, what could be the role of Germany and its cyber security authority BSI to help in this European context?

Germany is very advanced in many respects and does an excellent job in promoting European cooperation on cyber security. This is particularly true in the technical area, where the BSI's activities and projects make a valuable contribution to develop European know-how. We appreciate, for instance, the fact that the BSI has given a helping hand to new Member States to establish their governmental CERTs. In the future, I would like to encourage Germany, together with those Member States that have advanced capabilities, to share their knowledge on cyber security preparedness. In this regard, the German National Cyber Defense Centre and the German Anti-Botnet Initiative are good examples which have the potential to deliver benefits throughout the EU.

What especially interests us: what are your initiatives to promote good security practices within the Commission and across other European institutions?

I am a firm believer that we must always practice what we preach. Firstly, the European Commission is determined to adopt internally, as an organization, the best available standards and practices for security, of which NIS is a core component. Secondly, I have launched in the DAE the idea of establishing a CERT for the EU institutions. Such a CERT would be crucial in enhancing the security of the EU institutions and make it comparable to the highest standards at national and international level. In this regard Vice-President Šefčovič and I have established a high-level expert group, the "Rat der IT-Weisen", to advise the European Institutions on how to set it up. The experts delivered their report at the end of 2010. We are now engaging with other EU institutions on the way forward. My objective is that, by 2012, the community of governmental/national CERTs will have someone to call in Brussels should they detect a cyber-attack against our organizations!

Digitale Agenda – eine politische Leitinitiative für Wachstum und Wohlstand in Europas Informationsgesellschaft

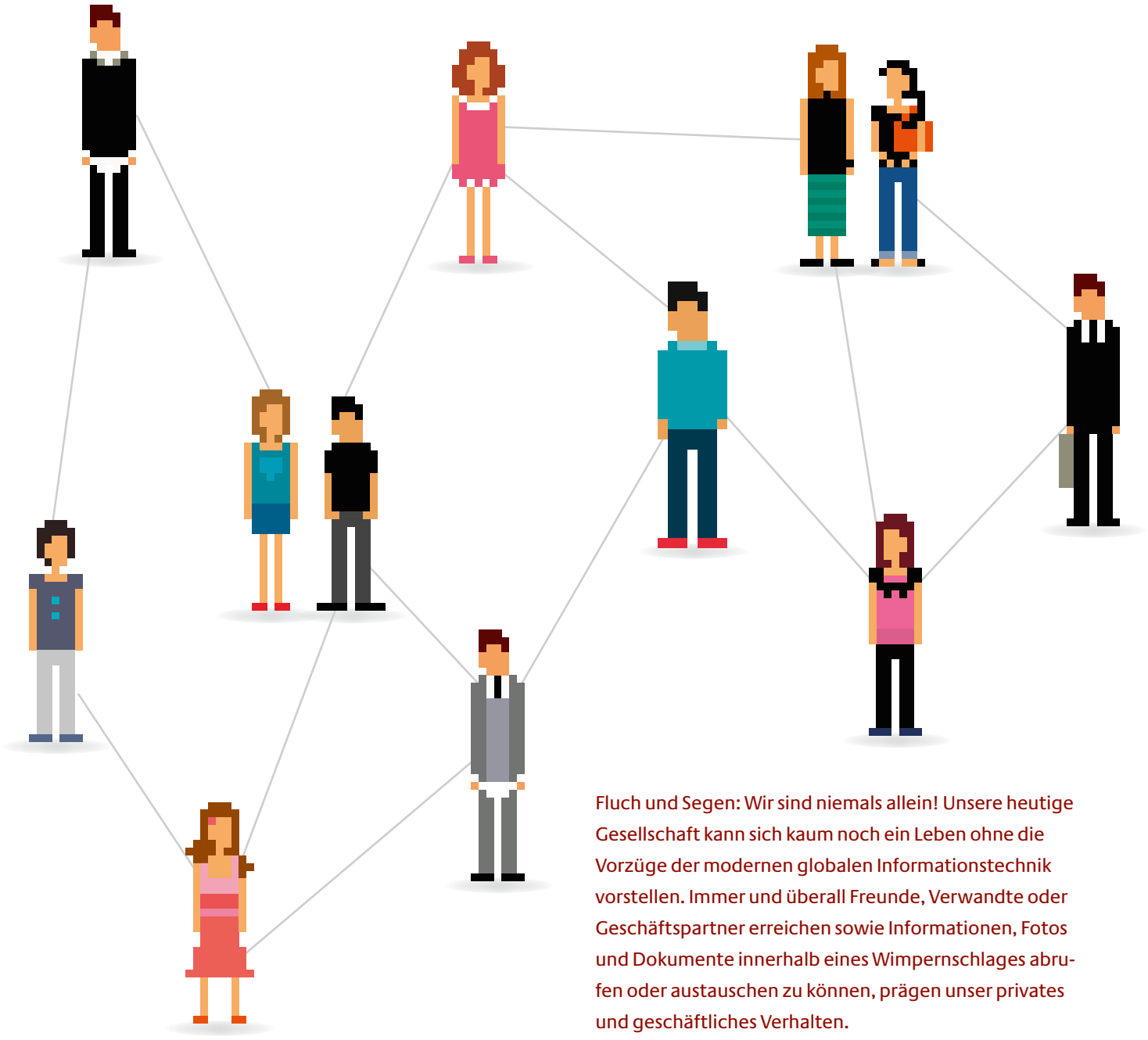
Am 19. Mai 2010 hat Neelie Kroes, die Kommissarin für die „Digitale Agenda", die gleichnamige politische Dachstrategie der Europäischen Kommission in Form einer Mitteilung veröffentlicht. Sie ist die erste von sieben Leitinitiativen der EU-Strategie Europa 2020. Sie wurde aufgestellt, um die grundlegende Rolle zu definieren, die dem Einsatz der ITK bei Wachstum und Wohlstand in Europa zukommen muss. Sie steht daher ganz im Zeichen von Wachstumschancen im digitalen Zeitalter. Die Digitale Agenda sieht sieben vorrangige Aktionsbereiche vor, die etwa 100 Folgemaßnahmen beinhalten, darunter 31 Legislativvorschläge.

Die sieben vorrangigen Aktionsbereiche bzw. Säulen sind:

1. Schaffung eines digitalen Binnenmarkts („Digital Single Market")
2. Verbesserung der IKT-Normung und Interoperabilität
3. Steigerung von Vertrauen und Sicherheit im Internet
4. Besserer Zugang der Europäer zum schnellen Internet
5. Steigerung der Spitzenforschung und Innovation im IKT-Bereich
6. Digitale Fähigkeiten und barrierefreie Online-Dienste für alle Europäer
7. Freisetzung des IKT-Potenzials zum Nutzen der Gesellschaft

Globale Informations-technik – Internationale Zusammenarbeit

Hans-Peter Jedlicka, Referent für Planung und internationale Kooperation im Bereich CERT-Bund



Fluch und Segen: Wir sind niemals allein! Unsere heutige Gesellschaft kann sich kaum noch ein Leben ohne die Vorzüge der modernen globalen Informationstechnik vorstellen. Immer und überall Freunde, Verwandte oder Geschäftspartner erreichen sowie Informationen, Fotos und Dokumente innerhalb eines Wimpernschlages abrufen oder austauschen zu können, prägen unser privates und geschäftliches Verhalten.

Niemand will inzwischen auf diese Vorteile verzichten

Diese Allgegenwart der Informationstechnik, die ständige Erreichbarkeit von lohnenden Zielen und das Vorhandensein der damit gespeicherten oder transportierten wertvollen Informationen locken auch Personen oder Gruppierungen, die eben diese Informationstechnik für eigene Zwecke missbrauchen. Es vergeht kein Tag, an dem nicht die Verbreitung eines neuen Schadprogramms oder die Entwendung von schützenswerten Daten bekannt wird, seien es Personaldaten, Kundendaten, Kreditkarteninformationen, Zugangsdaten oder Vergleichbares. Die Täter operieren aus dem Schutz der Anonymität und nutzen bewusst die Möglichkeiten der Informationstechnik, um die eigene Identität zu verschleiern und effektive Gegenmaßnahmen einschließlich einer Strafverfolgung zu erschweren.

Ständig erfolgen Kompromittierungsversuche, um die Netze der bereits infizierten und kontrollierten Systeme, die sogenannten Botnetze, weiter auszubauen. Auch seriöse Webseiten werden angegriffen und so manipuliert, dass bei deren Besuch der nichts ahnende und unvorbereitete Benutzer nicht nur die erwarteten Inhalte herunterlädt. Zusätzlich werden Schadprogramme auf seinem Computersystem installiert. Ab diesem Zeitpunkt kann das kompromittierte System von Angreifern ferngesteuert werden. Oft werden dann auch das Verhalten der Nutzer oder deren persönliche Informationen ausgespäht.

Gerade die Transparenz unseres Onlineverhaltens und die Verfügbarkeit unserer Daten, also die wesentlichen Vorteile unseres Informationszeitalters, wandeln sich aus dieser Perspektive zu handfesten Nachteilen.

Wir sind niemals allein da draußen

Diese ernüchternde Erkenntnis erfordert ein Umdenken bei allen potenziell Betroffenen, insbesondere bei denjenigen, die die Verantwortung für die Sicherheit der Informationen und der Systeme tragen. Aber auch die Nutzer müssen sensibilisiert und auf reale Bedrohungen sowie auf konkrete Schutzmöglichkeiten aufmerksam gemacht werden. Die Hersteller bemühen sich um höhere Qualitätsstandards, versuchen Fehler und Schwachstellen zu vermeiden und etablieren Prozesse, um dennoch aufgetretene Sicherheitsprobleme schnellstmöglich zu beseitigen. Die für den IT-Betrieb und die IT-Sicherheit verantwortlichen Fachstellen ringen um pragmatische Lösungen, um einerseits die Funktionalität benötigter Applikationen sowie deren Effizienz und Bedienkomfort und andererseits erforderliche Sicherheitsaspekte miteinander zu vereinen. Trotz vieler bisheriger Erfolge sind massive weitere Anstrengungen bei allen Beteiligten erforderlich, um langfristig den Status Quo beizubehalten oder die Situation sogar spürbar zu verbessern.

Nationale und internationale Kooperation

Computer Emergency Response Team (CERT®)
Die Geburtsstunde der Computer-Notfallteams geht zurück auf das Jahr 1988, als der Morris-Wurm erhebliche Teile des damals überschaubaren Internets beeinflusste und schädigte.
Um bei künftigen Vorfällen besser gewappnet zu sein, initiierte die Defense Advanced Research Projects Agency (DARPA) den Aufbau des namensgebenden CERT Coordination Center an der Carnegie Mellon University.
Synonyme Begriffe:

CSIRT	Computer Security Incident Response Team
CIRC	Computer Incident Response Capability

Ein wichtiger Aspekt für die IT-Sicherheit ist der regelmäßige Informations- und Erfahrungsaustausch sowie die gegenseitige Unterstützung innerhalb der nationalen und internationalen Organisationen, die sich der Sicherheit in der Informationstechnik widmen. Dazu zählen auf operativer Ebene vor allem die Computer-Notfallteams (engl. Computer Emergency Response Team, CERT) und Sicherheitsteams bei Herstellern, Unternehmen und Behörden. Schon seit Langem sind

die Vorteile der engen und motivierten Zusammenarbeit dieser kompetenten Stellen offensichtlich. Im Laufe der Zeit entstanden Kooperationsmodelle und Vertrauensbeziehungen, die erheblich mit dazu beitragen, die allgemeine Bedrohungssituation immer wieder zu entschärfen und neue Risiken rechtzeitig aufzudecken. Es werden Analysen durchgeführt, Lagebewertungen ausgetauscht und gemeinsam Gegenmaßnahmen erarbeitet.

Erfolgreiche deutsche Initiative

So hat sich in Deutschland beispielweise eines der weltweit dichtesten Netzwerke von Computer-Notfallteams – der sogenannte CERT-Verbund – entwickelt, dem mehrere Dutzend Teams aus dem behördlichen, industriellen und akademischen Umfeld angehören. Der regelmäßige Kontakt, der ständige Informationsaustausch sowie gemeinsame Projekte stärken den Esprit de Corps und ermöglichen es, die anfangs zumeist fragilen Vertrauensbeziehungen stetig auszubauen und zu stärken, um auch sensitive Probleme ohne Scheu diskutieren zu können. Eine Belastungsprobe für diese Gemeinschaft war im vergangenen Jahr insbesondere der Vorfall um das Schadprogramm Stuxnet, der sich letztlich als eine Chance erwies und die schnelle, effiziente Zusammenarbeit und Informationsweitergabe eindrucksvoll unter Beweis stellte.

Die Erfahrung zeigt, dass Vorfälle, auch wenn man über diese am liebsten nicht sprechen möchte, sehr schnell auch von Dritten wahrgenommen werden: Entweder werden deren Systeme direkt kompromittiert und es entstehen konkrete Schäden oder aber Angriffe werden aufgezeichnet und bei der Auswertung entdeckt. Sprachlosigkeit hilft hierbei keinem. Nur ein rascher, vertrauensvoller Informationsaustausch garantiert, eigene Sicherheitslücken vollständig zu verstehen und weitere Schäden abzuwehren. Die enge und gute Zusammenarbeit mit dem BSI und namentlich dem CERT-BUND hat es ermöglicht, diesen Informationsaustausch für wichtige nationale Netze sicherzustellen.

Dr. Klaus-Peter Kossakowski, Geschäftsführer DFN-CERT

IT-Vorfälle beachten keine Landesgrenzen

Diese äußerst positive Erfahrung im Zusammenhang mit der Aufklärung zum Schadprogramm Stuxnet bestätigte sich auch im internationalen Umfeld. Die Expertise verschiedenster Teams bereicherte das entstehende Gesamtlagebild und unterstützte die Lageeinschätzung aller Beteiligten. Unabhängig von dem besonders medienwirksamen Ereignis Stuxnet erwies sich die internationale Zusammenarbeit in den vergangenen Jahren im Rahmen der jeweils vorhandenen Ressourcen immer wieder als höchst effizient. In enger Kooperation mit den jeweiligen national zuständigen Stellen und Kontaktpunkten konnten übernommene IT-Systeme, die außerhalb der eigenen Zugriffsmöglichkeiten lokalisiert sind, identifiziert und bereinigt oder vom Netz genommen werden. Insbesondere die steigende Tendenz, mächtige, multifunktionale Botnetze, die in der Regel weltweit verteilt sind, zu missbräuchlichen Zwecken einzusetzen, sowie die zunehmende Spezialisierung und Aufgabenteilung der Täter, die ebenfalls häufig weltweit organisiert wird, erfordern gemeinsame internationale Kooperationen, um handlungsfähig zu bleiben. Beispielsweise beachten automatisierte Verbreitungsroutinen von Schadprogrammen keine Landesgrenzen oder Zonen einheitlicher Rechtssprechung. Im Gegenteil: Manche Täter nutzen bewusst die Komplexität unterschiedlicher Zuständigkeiten aus und kalkulieren mit potentiellen Reibungsverlusten bei der Aufklärung, Verfolgung und Bereinigung ihrer Angriffe.

”Over the course of years we here at CERT-FI have learned that victims of many internet threats are among the last ones to learn about the information security incidents affecting them. CSIRT's play an important role in matching information about incidents with those with a need-to-know. CERT-FI would not be able to succeed in protecting Finland without the continued help of competent and trusted international colleagues such as CERT-Bund of Germany.“

Erka Koivunen, Head of CERT-FI, Finland

Wer hilft mir?

Aus Sicht des BSI und des Computer-Notfallteams der Bundesverwaltung (CERT-Bund) war das Jahr 2010 in diesem Kontext vor allem dadurch geprägt, die Kontakte zu nationalen und internationalen Kooperationspartnern aufzufrischen, neue Kooperationen anzustoßen, bestehende Prozesse zu formalisieren sowie sogenannte „Standard Operating Procedures (SOP)“ auszuarbeiten und zu üben. So wurden neben der öffentlich wahrgenommenen Übung „CYBER EUROPE 2010“ mehrere weitere Übungen mit unterschiedlichen Teilnehmerkreisen durchgeführt, um die Beziehungen untereinander zu vertiefen und die Reaktionsprozesse zu optimieren.

„Nur das Bewusstsein, jederzeit verlässliche Partner an der eigenen Seite zu finden, erlaubt ein gemeinsames erfolgreiches Vorgehen."

Hans-Peter Jedlicka

Zum Glück sind wir nicht allein

Alle bisherigen Erfahrungen verdeutlichen die Notwendigkeit einer motivierten, auf Vertrauen basierenden Kooperation. Das Eingeständnis eines IT-Vorfalls oder gar die Weitergabe von Detailinformationen eines solchen IT-Vorfalls wird häufig von der Frage begleitet: „Will ich mit anderen darüber sprechen?" oder „Dürfen das andere überhaupt erfahren?" In vielen Fällen ermöglicht es aber erst der gelebte Informationsaustausch den zuständigen und handlungsfähigen Stellen zu agieren. Die Überwindung dieser zurückhaltenden Grundeinstellung ist daher das erklärte Ziel der Kooperationsbestrebungen des BSI. Nur das Bewusstsein, jederzeit verlässliche Partner – Schulter an Schulter – an der eigenen Seite zu finden, erlaubt ein gemeinsames erfolgreiches Vorgehen.

Erfolgsgeheimnis: Gibst Du mir, so geb ich Dir

Ein dominantes Merkmal der erfolgreichen, vom BSI unterstützten Kooperationsmodelle ist die Tatsache, dass es sich um geschlossene Gruppen von überschaubarer Größe handelt, die darauf vertrauen, dass die interne Kommunikation geschützt und respektiert wird. Die Mitglieder verfolgen in der Regel identische Ziele und teilen ein gemeinsames Verständnis füreinander. Basierend auf den Gemeinsamkeiten werden Prozesse und Verfahren entwickelt, die die Kommunikation und Reaktion in besonderen IT-Lagen bis hin zu IT-Krisen effizienter gestalten. Regelmäßige Meetings und persönliche Kontakte dienen dem bereits oft zitierten Informations- und Erfahrungsaustausch und tragen zur Vertrauensbildung bei. Dies ist insbesondere notwendig, da das Vertrauen sich nicht ohne Weiteres auf neue Partner übertragen lässt, sondern erarbeitet werden muss. Dagegen gefährdet das unkontrollierte Wachstum solcher Kooperationsmodelle deren Vertrauensbeziehungen und sollte daher vermieden werden. Von besonderer Bedeutung ist die gleichberechtigte Stellung aller Partner. Das Kernelement ist jedoch die klassische Win-Win-Situation. Jeder Partner hofft und erwartet, in seiner Notsituation Unterstützung zu finden, und muss sich daher auch darauf einstellen, Unterstützung zu gewähren.

Eine lohnende Investition

Vor diesem Hintergrund wird klar, dass der globale Aspekt der Informationstechnik auch ein enormes Potenzial für eine bilaterale und multilaterale Zusammenarbeit bietet. Eine Investition in aktive Kooperationen steigert langfristig die eigene Effektivität. Wir sind nicht allein!

Karriere und öffentlicher Dienst – die Zeichen stehen auf Chance!

In der Bundesrepublik ist für 90 Prozent der Beschäftigten zwischen 25 und 29 Jahren mit Kindern Familienfreundlichkeit bei der Arbeitgeberwahl ebenso wichtig wie das Gehalt.[8] Familienfreundlichkeit wird im BSI groß geschrieben. Durch flexible Arbeitszeitmodelle und Telearbeit können vor allem jüngere Beschäftigte Familie und Beruf optimal vereinbaren. Kind oder Karriere? – diese Frage stellt sich im BSI nicht.

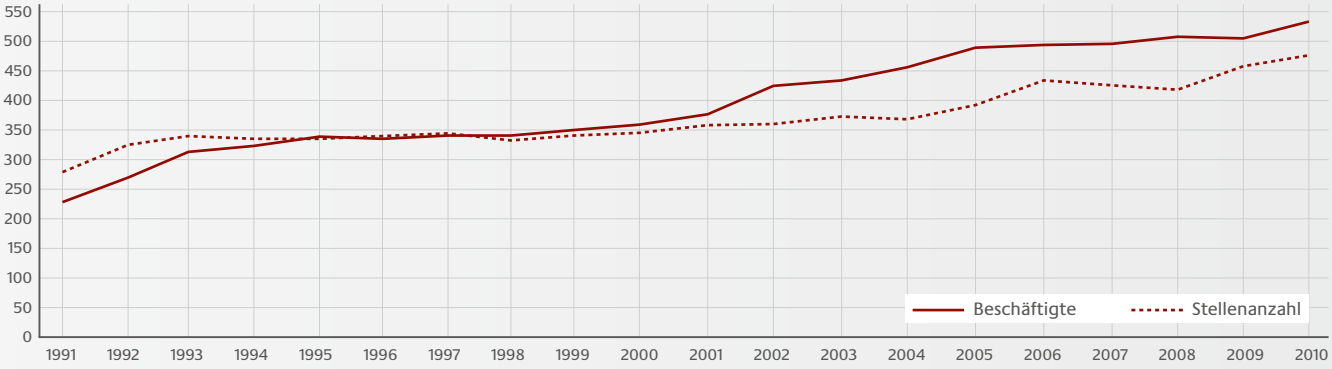
Sich neben dem Hauptberuf noch weiterzubilden, ist ein weiterer Trend, der im BSI verstärkt zu beobachten ist. Kolleginnen und Kollegen nehmen die zusätzliche Herausforderung der Weiterqualifikation an, und das BSI unterstützt dieses Engagement zum Beispiel durch eine flexible Anpassung der Arbeitszeit je nach Studienverlauf.

Außerdem wird darauf geachtet, die Höherqualifizierungen der Mitarbeiterinnen und Mitarbeiter in der strategischen Personalplanung frühzeitig zu berücksichtigen. Erfolge sind bereits zu verzeichnen: Mit ihren neu erworbenen Hochschulabschlüssen konnten sich Kolleginnen und Kollegen in Auswahlverfahren erfolgreich behaupten und eine weitere Stufe auf der Karriereleiter erklimmen. Das BSI engagiert sich, die Möglichkeiten der Personalentwicklung im öffentlichen Dienst für kompetente und engagierte Mitarbeiter voll auszuschöpfen.

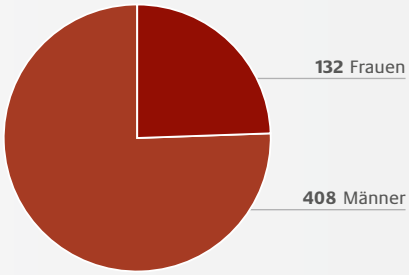
[8] Personalmarketingstudie 2010 des Bundesministeriums für Familie, Senioren, Frauen und Jugend

Entwicklung der Stellen- und Beschäftigtenzahlen im BSI

(Stellen ohne zeitlich befristete Kräfte, zum BSI abgeordnete Mitarbeiter und Auszubildende)

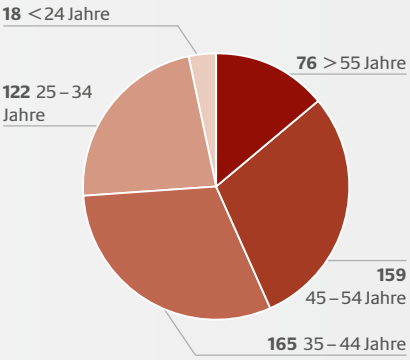


Mitarbeiter (Stand Ende 2010)



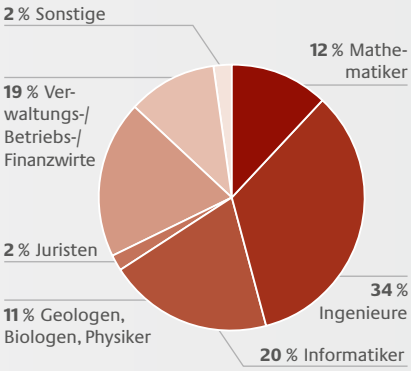
Total: 540 Mitarbeiter

Alterstruktur

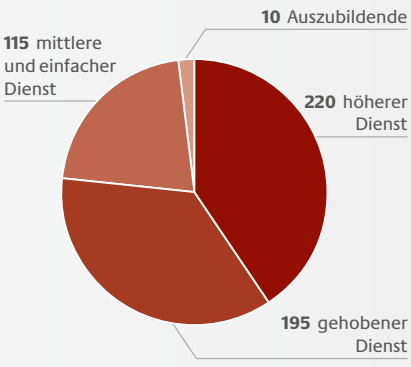


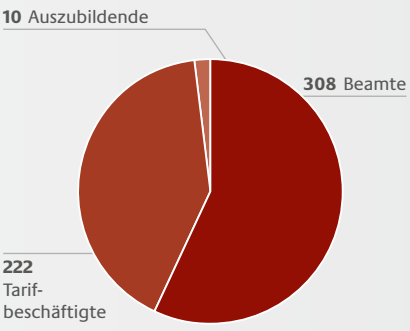
Beruflicher Hintergrund

(nur höherer und gehobener Dienst)



Laufbahnen





Das BSI ist beliebter Arbeitgeber bei IT-Absolventen

Auch im Jahr 2010 ist das BSI wieder unter Deutschlands beliebtesten Arbeitgebern im IT-Bereich. IT-Absolventen wählten das BSI zum wiederholten Mal auf Platz 12, gleich hinter namhaften Firmen wie Google, IBM, SAP und Microsoft.

Stefanie Euler,

Referat 125 „IT-Penetrationszentrum,
Abwehr von Internetangriffen“

Um meine Karrierechancen zu verbessern und in den gehobenen Dienst aufsteigen zu können, entschied ich mich nach meiner Ausbildung zur Fachinformatikerin für Systemintegration für ein berufsbegleitendes Studium an der FH Köln/FH Dortmund mit einem Abschluss als Diplom-Wirtschaftsinformatikerin. Da gerade im IT-Bereich praktische Erfahrung notwendig ist, war das Studium mit seiner Kombination aus Fern- und Präsenzunterricht für mich die optimale Weiterbildungsmöglichkeit. Meine Vollzeitstelle beim Lage- und Analysezentrum CERT-Bund im BSI konnte ich weiterhin ausüben und so Theorie und Praxis verknüpfen. Das BSI unterstützte meine Weiterbildung und ermöglichte mir eine flexible Zeiteinteilung und Urlaubsgestaltung, was vor allem in der Klausurzeit sehr wichtig war.

Kurz vor Ende des Studiums wurde ich Mutter. Nach einem Jahr Elternzeit kehrte ich ins BSI zurück und stellte kurze Zeit später die für das Studium noch ausstehende Projektarbeit sowie meine Diplomarbeit fertig. Das Thema für die Diplomarbeit fand ich zuvor bereits im Lagezentrum des BSI und konnte deshalb einen Teil der praktischen Arbeit während der Dienstzeit erledigen – eine große Erleichterung.

Durch die Möglichkeit, im BSI in Teilzeit auf meiner bisherigen Stelle bei CERT-Bund zu arbeiten, konnte ich Beruf und Familie optimal miteinander verbinden. Um meine durch das Studium gewonnenen Qualifikationen noch besser einbringen zu können, behielt ich die Stellenlage im gehobenen Dienst im Auge. Kurze Zeit später wurde eine passende Position im Referat 125 „IT-Penetrationszentrum, Abwehr von Internetangriffen“ ausgeschrieben. Trotz Zugehörigkeit zum BSI müssen Mitarbeiter, die sich verändern wollen, das normale Bewerbungsprozedere durchlaufen. Dennoch ist es natürlich ein Vorteil, potentielle Vorgesetzte und Referatskollegen schon aus früheren Projekten zu kennen. Meine Bewerbung hatte Erfolg, ich konnte im Vorstellungsgespräch überzeugen und somit unmittelbar nach Abschluss meines Studiums eine unbefristete Stelle im gehobenen Dienst antreten. Um meinen neuen Job und meine junge Familie besser miteinander vereinbaren zu können, gestattete mir das BSI, meine Teilzeit flexibel auf 80 Prozent mit anteiliger Telearbeit zu erhöhen. Die Telearbeit bietet mir vor allem zeitliche Vorteile, beispielsweise indem die Fahrten ins Büro wegfallen oder durch die relativ flexible Arbeitseinteilung. Die Zeit, die ich gewonnen habe, kann ich mit meiner Tochter verbringen.

Meine anfänglichen Sorgen, als „Teilzeitmutter“ nicht mehr als vollwertige Arbeitskraft angesehen zu werden, stellten sich glücklicherweise als unbegründet heraus. Ich konnte von Anfang an wieder in interessanten Tätigkeitsfeldern arbeiten, was mich sehr motiviert und effektiv arbeiten lässt. Auch bei Fortbildungen fördert das BSI Teilzeitkräfte und ermöglichte mir spannende Optionen wie die Teilnahme an internationalen Konferenzen und Schulungen. Nach meinen bisherigen positiven Erfahrungen im BSI bin ich optimistisch, weiterhin in interessanten Projekten arbeiten, meine Arbeitszeiten familienfreundlich gestalten und in Kürze auch mit zwei Kindern vereinen zu können.

Pilotprojekt Studienförderung

Im gehobenen Dienst fehlt es der Bundesverwaltung an IT-Fachkräften. Mit vier weiteren Behörden aus dem Geschäftsbereich des Bundesministeriums des Innern hat das BSI ein Pilotprojekt gestartet, um den IT-Nachwuchs im gehobenen Dienst zu fördern. Seit 2008 unterstützt das BSI Bachelor-Studenten mit einer Studienbeihilfe und garantiert ihnen im Anschluss an ihr Studium eine Festanstellung. Der erste geförderte Student, Sebastian Cielewicz, ist ein ehemaliger Auszubildender des BSI. Er wird im nächsten Jahr das Studium mit dem Bachelor of Computer Science an der Fachhochschule Bonn-Rhein-Sieg abschließen und dann im gehobenen Dienst im BSI arbeiten.

Sebastian Cielewicz

Wie kamen Sie darauf, sich für das Studienförderungsprogramm des BSI zu bewerben?
Cielewicz: Bevor die Bewerbungsverfahren zum Studienförderungsprogramm begannen, arbeitete ich nach meiner Ausbildung zum IT-Systemelektroniker in einem befristeten Arbeitsverhältnis im BSI. Durch meinen damaligen Ausbildungsleiter wurde ich auf dieses Programm aufmerksam. Ich fand es auf Anhieb toll und habe mich sofort beworben. Der Aspekt, nach erfolgreichem Abschluss einen festen Arbeitsplatz im BSI zu erhalten, hat mich besonders gereizt, denn meine bisherige Zeit im BSI hat mir sehr gefallen. Das Arbeitsklima stimmt einfach, die Kollegen und Kolleginnen sind sehr nett und hilfsbereit. Es gibt sehr viele interessante und herausfordernde Aufgaben.

Wie ist der Ablauf der Studienförderung?
Cielewicz: Sobald das Bewerbungsverfahren abgeschlossen und ein Bewerber ausgewählt wurde, muss sich dieser selbstständig um den Studienplatz bemühen und an der Hochschule Bonn-Rhein-Sieg immatrikulieren. Die Kosten der Semesterbeiträge werden dem Student zurückerstattet, sobald er einen Zahlungsnachweis vorgelegt hat. Außerdem muss der Student für jedes Semester den Nachweis der erreichten Credits aus den Prüfungen vorlegen. Während des Studiums unterstützt das BSI den Studenten monatlich finanziell – und zwar in Höhe des maximalen BAföG-Satzes. Wenn man in den höheren Semestern seinen Schwerpunkt wählen muss, ist es sinnvoll, dem Leiter der Studienbeihilfe die eigene Wahl in einem persönlichen Gespräch zu erläutern. Auf diese Weise können schon im Vorfeld die zukünftigen Verwendungsmöglichkeiten im BSI, zumindest grob, eingeschätzt werden. Das BSI bietet den Studenten sowohl eine Praktikumsstelle, die innerhalb des Studiums vorgesehen ist, als auch eine Stelle für die Bachelorarbeit an.

Wie ist Ihr (Zwischen-)Fazit? Wie beurteilen Sie das Programm?
Cielewicz: Mein Zwischenfazit für dieses Programm ist sehr positiv. Auf fachlicher Seite lässt es mir den nötigen Freiraum, selbst zu bestimmen, welchen Schwerpunkt ich im Studium wählen möchte. Man wird dadurch nicht in eine bestimmte Richtung gedrängt, sondern kann sich den Bereich aussuchen, der einen am meisten interessiert. Persönlich habe ich es bisher nie bereut, dem Programm anzugehören. Die Vorteile liegen klar auf der Hand: Theorie und Praxis sind hier eng miteinander verbunden. Für das Studium bringe ich durch meine Ausbildung und berufliche Tätigkeit schon gute Voraussetzungen mit. Andersherum kann ich das im Studium Gelernte im Rahmen meines Praktikums beim BSI auch gleich wieder in die Praxis einbringen und durch praktische Erfahrungen erweitern. Davon profitiert ja auch das BSI: Neueste Erkenntnisse und Entwicklungen, die im Studium vermittelt werden, fließen direkt in die Arbeit ein, und Nachwuchskräfte können frühzeitig rekrutiert werden. Ein ganz großer Vorteil für mich ist natürlich die Sicherheit, nach dem Studium einen festen und vor allem interessanten und meinen Qualifikationen entsprechenden Job im BSI zu erhalten.

Wie reagieren Ihre Studienkollegen darauf, wenn sie erfahren, dass Sie eine Studienbeihilfe erhalten und eine feste Jobperspektive haben?
Cielewicz: Diejenigen von meinen Kommilitonen, die davon wissen, finden das super – fast beneidenswert. Eine feste Jobperspektive bedeutet heutzutage sehr viel. Auch die Mitarbeiter des BSI, mit denen ich darüber gesprochen habe, halten das für eine gute Sache.

20 Jahre BSI

„20 Jahre BSI – Anerkennung und Ermutigung“

Peter Hohl, Journalist und Gründer der SecuMedia Verlags-GmbH

Am 17. Dezember 1990, dem Tag, als im Bundesanzeiger das BSI-Errichtungsgesetz verkündet wurde, saß ich vor meinem PC, um eine Meldung über das Bundesamt zu schreiben, das ab 1. Januar 1991 unter dem neuen Namen arbeiten sollte. In meinem Text kam das Wort Internet vor. Mein Textverarbeitungsprogramm hielt das bei der Rechtschreibprüfung für einen Tippfehler und schlug mir vor, das Wort Internet durch das Wort Internat zu ersetzen. Was beweist, dass staatliches Handeln durchaus einmal der Welt der Rechner und Programme um eine Nasenlänge voraus sein kann.

Nun war also das BSI geboren und nahm mit den Mitarbeitern der bisherigen Zentralstelle seine Tätigkeit als selbständige Bundesoberbehörde auf. Ich hatte die Freude, das Amt während seiner gesamten Geschichte zu begleiten. Als ich aus Anlass des BSI-Jubiläums die Jahrgangsbände der <kes> durchgeblättert habe, sind mir ein paar Dinge aufgefallen, die im Hinblick auf das Jubiläum bedenkenswert sind. Insbesondere habe ich mich gefragt:

Was sind heute wesentliche Unterschiede gegenüber der Gründungssituation, die darum vielleicht auch ein wenig wegweisend sein können? Drei Dinge sind mir besonders aufgefallen:

1. Natürlich die heutige Allgegenwart der IT und des Internets, das Pervasive Computing, wie eine der BSI-Studien betitelt ist. Eine Regierung ohne massive eigene Kompetenz in diesen lebenswichtigen Fragen wäre heute nicht mehr vorstellbar in einem zivilisierten Land.
2. Sicherheit war vor 20 Jahren vor allem Antwort auf konkrete Bedrohungen. Es gab Viren und daraufhin Antivirenprogramme, es gab Hackerangriffe und daraufhin Firewalls. Sicherheit war vor allem ein Substantiv. Das stimmt auch heute noch. Aber es ist etwas dazugekommen. Sicher als Adjektiv – als notwendige Eigenschaft eines ganz anderen Produkts oder Vorgangs. Nicht über das Design des neuen Personalausweises ist diskutiert worden, sondern über seine Sicherheit. Social Networks geraten nicht nur wegen philosophischer oder gesellschaftspolitischer Zweifel in die Kritik, sondern vor allem wegen Fragen der Datensicherheit. Niemand zweifelt daran, dass Web Applications oder Cloud Computing funktionieren. Aber wie sicher sind sie?
3. Die Intensität, mit der heute Sicherheitsfragen gestellt und Sicherheitsdiskussionen geführt werden. Denkt man an Online-Banking, an das Verfahren für die eigene Schufa-Auskunft oder den elektronischen Brief. Auffallend aufwändige und komplizierte Prozeduren. Ich habe sie ausprobiert. Und ganz offensichtlich empfinden die Leute das nicht mehr als lästige Zumutung, sondern als positives Entscheidungskriterium.

Hinter uns liegt eine stürmische Entwicklung, die bereits vor der Gründung des BSI begann: 1978 war ich zum ersten Mal auf der Hannovermesse. Mich interessierte eine einzelne Halle, die sich Centrum für Büro- und Informationstechnik nannte – abgekürzt CeBIT. Ich suchte für meinen noch zu gründenden Verlag ein Textverarbeitungssystem. Und was fand ich? Ein System, welches eine Besonderheit gegenüber den bisher bekannten Systemen hatte, und zwar einen Bildschirm. Darum hieß es Bildschirm-Textsystem, abgekürzt BITSY. Eine Festplatte hatte es nicht, das war zu jener Zeit Großrechnern vorbehalten, aber statt der bisher üblichen Musikkassetten zwei Laufwerke für Minifloppies. Später nannte man sie 5 ¼ Zoll Disketten. Kapazität: 80 Kilobyte. Auf einer war das Betriebssystem, im anderen Laufwerk steckten die Daten. Arbeitsspeicher: 19 Kilobyte. Preis bei Barzahlung: 32.000 DM.

Beeindruckt hat mich im Vorfeld der BSI-Gründung auch eine Geschichte, die ein gewisser Fred Cohen in den USA losgetreten hatte – übrigens, wie sich später herausstelle, nahezu zeitgleich mit einem Deutschen. Im

Peter Hohl mit seiner "BITSY" vor rund 30 Jahren

November 1984 erschien im SPIEGEL eine Zehn-Zeilen-Meldung: Jener Fred Cohen habe an der University of Southern California ein Programm geschrieben, das sich selbsttätig in anderen Programmen verstecken und den befallenen Rechner veranlassen konnte, Kopien dieses Programms auf den Weg zu schicken. Weil es sich also ähnlich verhielt wie ein Krankheitserreger, gab er ihm den Namen Virus.

Ich fand das ziemlich beängstigend; und da wir nicht zur Sensationspresse gehören, fühlen wir uns verantwortlich für das, was wir tun. Sprich: Wir machten es uns nicht leicht mit der Entscheidung über eine weitreichende Verbreitung der Informationen. Als aber kurz darauf ein Untergrundblatt, die „Bayerische Hackerpost“, über die neue Angriffs-Möglichkeit schrieb, war es höchste Zeit, auch die für EDV-Sicherheit Verantwortlichen zu informieren.

In den nächsten beiden Ausgaben der <kes> (Fachzeitschrift für Informationssicherheit) erschien nunmehr ein Artikel zu den neuen Ereignissen. Illustriert war der Bericht unter anderem mit einer Karikatur, die einen Rückfall in die Steinzeit prophezeite. Dass wir dann doch nicht in die Steinzeit zurückgefallen sind – und das ist meine ehrliche Überzeugung – ist sehr wesentlich dem BSI zu verdanken, das die Herausforderung angenommen hat und lange das entscheidende Informationszentrum für die Virenproblematik war, bevor sich eine funktionierende und vertrauenswürdige Antivirus-Industrie etabliert hatte. Doch nun ins Jahr 1991. Das BSI arbeitete bereits. Mein erster Besuch der neuen Behörde fand statt in einem ziemlich gut gesicherten Anwesen in Mehlem. Es ging um die Frage, wie offen die Dienststelle künftig gegenüber der Öffentlichkeit sein würde. Die Antwort war: Im Hinblick auf die allermeisten Aufgaben: sehr offen. Schon damals wurde erwogen, dem BSI ein eigenes Organ zur Verfügung zu stellen.

Erinnert sich jemand an den 20. August? An diesem Tag ist in Moskau ein Putsch von Altkommunisten im Gang. Der Präsident der Sowjetunion Michail Gorbatschow wird auf seiner Datscha in der Ukraine festgesetzt. Und vor dem Weißen Haus in der russischen Hauptstadt steigt Boris Jelzin auf einen Panzer und mobilisiert Bevölkerung und Militär gegen die Putschisten. An diesem Tag, an dem die Welt wackelt, so könnte man meinen, sind deutsche Regierungsmitglieder in höchster Alarmbereitschaft und rühren sich nicht von ihren Kommandoständen weg. Aber einem Minister ist ein anderes Ereignis so wichtig, dass er den Termin nicht absagt: Wolfgang Schäuble übergibt am 20. August dem Präsidenten des BSI ein neues Gebäude. Mit gläserner Fassade und somit ein Sinnbild für die Offenheit der künftigen Arbeit. Manchmal kann man ein Thema schön veranschaulichen, wenn man fragt: Wie sähe die Welt aus – ohne? Ohne BSI gäbe es so manches nicht: keinen Grundschutz, keine Zertifizierung, kein BSI für Bürger, es hätte viele Bücher, viele Studien, viele CDs nicht gegeben. Und wahrscheinlich auch kein europäisches Pendant.

Alles in allem: Es ist Enormes erreicht worden in diesen 20 Jahren in allen Arbeitsbereichen des BSI und auf allen Ebenen. Ich darf aus eigener Beobachtung ergänzen: Die drei Buchstaben BSI hinter einem Namen sind ein besonderer Grund, stolz zu sein. Es ist beachtlich, welches Ansehen und welchen Respekt Mitarbeiterinnen und Mitarbeiter des BSI genießen – ebenfalls auf allen Ebenen – und zwar sowohl wegen ihrer persönlichen Fachkompetenz als auch wegen des fachlichen und integren Rufs ihrer Behörde.

Der größte Erfolg, der in keiner Statistik erscheint, verdient eine ganz besondere Erwähnung: Das BSI hat in diesen 20 Jahren das Vertrauen der Bürger gewonnen. Das ist heutzutage ein kostbarer Schatz. Auch darum meine ich: Die Leistung des Amtes und seiner Menschen in den letzten 20 Jahren verdient ganz große Anerkennung – und ganz große Ermutigung für die Zukunft!

Peter Hohl ist Journalist und Gründer der SecuMedia Verlags-GmbH und als solcher Herausgeber der <kes>. Er ist Organisator der IT-Sicherheitsmesse „it-sa“ in Nürnberg und dem BSI seit seiner Gründung eng verbunden.

„Hervorragende Fachkompetenz und ein hochmotiviertes Team“

Interview mit den ehemaligen BSI-Präsidenten Dr. Otto Leiberich, Dr. Dirk Henze und Professor Dr. Udo Helmbrecht

Was waren die zeitgeschichtlichen und persönlichen Höhepunkte während Ihrer Zeit im BSI?

Dr. Otto Leiberich: Es war die Zeit des Aufbaus. Das BSI war zum 1. Januar 1991 gegründet und ich zum Präsidenten ernannt worden. Die Vorgänger-Behörde des BSI hatte ausschließlich für den staatlichen Sicherheitsbereich gearbeitet. Nun aber kamen durch das BSI-Gesetz die IT-Sicherheit der Wirtschaft und der privaten Benutzer als Aufgaben hinzu. Die Übernahme dieser Aufgabe stellte eine große Herausforderung dar.

Dr. Dirk Henze: Die Frage nach den Höhepunkten kann ich nur so beantworten, dass ich sehr zufrieden damit bin, dass es während meiner Amtszeit gelungen ist, das BSI in einem kontinuierlichen Prozess über seine traditionellen Aufgaben hinaus zu einem zentralen IT-Sicherheitsdienstleister der Bundesregierung auszubauen und dazu beizutragen, dass IT-Sicherheit zu einem festen Bestandteil unserer nationalen Sicherheitskultur geworden ist.

Prof. Dr. Udo Helmbrecht: Ich erinnere mich an die Spam-Attacke im Mai 2004, die unser Regierungsnetz lahmlegte. Es hat damals Tage gedauert, bis der IT-Betrieb wieder normal lief. Es war auch der Beginn des nachhaltigen Auf- und Ausbaus des CERT-Bund. Spannend war auch die Einführung des elektronischen Reisepasses und die damit verbundene Diskussion um die Sicherheit des RFID-Chips und den Datenschutz. Interessant war es auch, den Regierungswechsel 2005 praktisch von innen heraus mitzuerleben. Und die Novellierung des BSI-Gesetzes in 2009 war ein wichtiger Meilenstein für die zukünftige Entwicklung des BSI.

Welche Erinnerungen verbinden Sie mit Ihren „ersten 100 Tagen“?

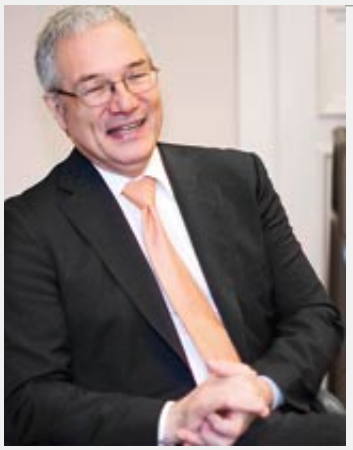
Leiberich: Die Jahre vor der Gründung des BSI waren schwer. Das „Projekt BSI“ hatte viele Feinde und stand oft genug vor dem Scheitern. Die Rückkehr zur alten Dienststelle hätte für meine engeren Mitstreiter und mich schwere persönliche Konsequenzen gehabt. Nun war das Ziel erreicht und das BSI errichtet. Die „ersten 100 Tage“ habe ich daher als eine Zeit der Befreiung von einem großen Druck in Erinnerung. Es herrschte Aufbruchsstimmung. Mit Eifer und Engagement gingen wir an die Arbeit. Uns einigte das Gefühl: „Wir werden es schaffen!“

„Ich denke, die Gründung des BSI war seiner Zeit etwas voraus.“

Dr. Dirk Henze, BSI-Präsident von 1993 bis 2002

Henze: Ich fand eine gut aufgestellte und funktionierende Verwaltung vor. Nach 23-jähriger Tätigkeit im Bundesinnenministerium war das Führen der Fachabteilungen des BSI zunächst ein Kulturschock für mich: hohe fachliche Kompetenz und großes Engagement der Mitarbeiter, aber rudimentärer vertikaler und horizontaler Informationsfluss, sehr individuelle, auch mit Vorgesetzten nicht immer abgestimmte Vorlagen.

Helmbrecht: Ich habe viel Unterstützung erfahren, was mir die Einarbeitung sehr erleichtert hat. Besonders positiv beeindruckt war ich von dem Engagement und der Identifikation der Mitarbeiter mit dem BSI. Neu war für mich der „Erlass“ und die damit verbundenen Prozesse. Das ist für jemanden, der in der Industrie groß geworden ist, gewöhnungsbedürftig.



„Besonders positiv beeindruckt war ich von dem Engagement und der Identifikation der Mitarbeiter mit dem BSI.“

Professor Dr. Udo Helmbrecht, BSI-Präsident von 2003 bis 2009

Wo sehen Sie das BSI in 20 Jahren?

Leiberich: Ich stelle nicht gerne Prognosen, meistens stellen sie sich im Nachhinein als falsch heraus. Hier aber bin ich mir sicher: Die Zukunft der Informationstechnik wird davon abhängen, ob es gelingt, die Computerkriminalität in Schach zu halten. Und dabei wird das BSI an vorderster Front mitkämpfen. Entsprechend wird seine Bedeutung zunehmen. Außerdem verfügt das BSI inzwischen über eine hervorragende Fachkompetenz. Ich konnte mich durch Fachgespräche mit den jungen Kollegen davon überzeugen, sodass mir um seine Zukunft nicht bange ist.

Henze: Sowohl Winston Churchill als auch Niels Bohr wird das Zitat „Prognosen sind schwierig, vor allem, wenn sie die Zukunft betreffen“ zugeschrieben. Sie sind ein hervorragendes Arbeitsfeld für Scharlatane, denn ihre Aussagen sind zumeist weder beweisbar noch widerlegbar. Meine Vermutung geht dahin, dass auf Dauer präventive und operative Aufgaben der Kriminalitätsbekämpfung auf dem Gebiet der Informationstechnik organisatorisch stärker zusammengeführt werden. Darüber hinaus glaube ich, dass sich das BSI langfristig durch neue Erkenntnisse, Konsolidierung und Kostendruck auf eine Diskussion über originäre staatliche Aufgaben auf dem Gebiet der Sicherheit in der Informationstechnik einstellen muss.

Wie hat sich der Stellenwert der IT-Sicherheit in der Gesellschaft während Ihrer Zeit im BSI verändert?

Leiberich: Die vorherrschende Meinung vieler Unternehmer war und ist leider immer noch: „Solange die Aufwendungen für ein IT-Sicherheitssystem teurer sind als die jährlichen Schäden, tätige ich keine Investitionen.“ Vor der Gefahr eines großen Schadens werden die Augen verschlossen; Stuxnet lässt grüßen. Noch mehr Sorge bereitet mir allerdings das „Wikileaks-Phänomen“. Wenn jeder, der sich über seine Firma geärgert hat, einfach einen Datenauszug entnehmen und weitergeben kann, ohne das Risiko einzugehen, gefasst zu werden, dann laufen unsere Bemühungen ins Leere. Die sicherste Verschlüsselung ist wirkungslos, wenn der Originaltext verraten wird.

Henze: Die Zeit meiner fast zehnjährigen Tätigkeit im BSI war geprägt von einer zunehmend nicht mehr überschaubaren weltweiten Vernetzung informationstechnischer Systeme. Mit dem Beginn der breiten kostenlosen Nutzung des Internets im Jahre 1993 entstanden völlig neuartige Bedrohungen, die Staat, Gesellschaft, Unternehmen und den Einzelnen betrafen. Durch fast tägliche Pressemitteilungen über Pannen bei der Nutzung der Informationstechnik und kriminelle Handlungen insbesondere beim Online-Banking wurde einer breiten Öffentlichkeit bekannt, dass es das Thema „IT-Sicherheit“ gibt. Die Zuwächse an Personal- und Haushaltsmitteln beim BSI in dieser Zeit belegen darüber hinaus, dass das Thema auch beim Parlament angekommen war.

Helmbrecht: Das BSI hatte schon immer einen hohen Stellenwert in der IT-Branche. Mit den Bürgerservices BSI-für-Bürger und dem Bürger-CERT haben wir Angebote geschaffen, die IT-Sicherheit bis zum Privatanwender bringen. IT-Grundschutz, Common Criteria-Zertifizierung und die technischen Richtlinien haben das IT-Sicherheitsniveau auch in der Privatwirtschaft erhöht. Der Schutz vor IT-Bedrohungen hat heute einen hohen Stellenwert.

Welche Rolle spielte damals der internationale Austausch?

Leiberich: Zu meiner BSI-Zeit keine. Ich kann mich nicht an entsprechende Behörden anderer europäischer Staaten erinnern. Diese waren Anfang der 90er Jahre noch nicht so weit.

Henze: Die internationale Zusammenarbeit erstreckte sich im Wesentlichen auf den Informationsaustausch mit staatlichen Stellen, die in ein anderes Umfeld eingebunden waren als das BSI. Ich denke, die Gründung des BSI war seiner Zeit etwas voraus. Der Vorteil war, dass es dadurch im internationalen Kontext eine Vorreiterrolle spielen konnte.

Helmbrecht: IT-Bedrohungen sind global. Die Zusammenarbeit mit den Sicherheitsbehörden unserer Partnerländer ist eminent wichtig. Hier spielt gegenseitiges Vertrauen eine große Rolle. Gerade unter den CERTs hat

sich eine Partnerschaft entwickelt, die durch frühzeitigen Informationsaustausch über IT-Angriffe rechtzeitiges staatliches Handeln ermöglicht.

Wie wichtig war in Ihrer Zeit die Kommunikation mit den Privatnutzern? Was hat sich hier Ihrer Meinung nach verändert?

Henze: Erst mit dem Internet ist die Informationstechnik so richtig beim Privatnutzer angekommen. Hier ist besondere Hilfe angesagt. Hier leistet das BSI inzwischen viel.

Helmbrecht: Kommunikation mit allen Beteiligten der Gesellschaft war für mich von Anfang an wichtig. Heute wird Computer-Technologie überall eingesetzt. Verwaltungsprozesse werden modernisiert, ein Beispiel ist die elektronische Steuererklärung. Der neue Personalausweis mit dem RFID-Chip wird in privatwirtschaftlichen und behördlichen Prozessen eingesetzt. Damit übernimmt der Staat aber auch Verantwortung für die IT-Sicherheit. Kommunikation bedeutet Transparenz und bildet Vertrauen in die Nutzung neuer Technologien.

Was vermissen Sie aus Ihrer Zeit beim BSI? Woran denken Sie gern zurück?

Leiberich: Die fachliche Arbeit und die Mitarbeit in einem kompetenten und hochmotivierten Team.

Henze: Der Umgang mit Menschen verschiedenster Fachrichtungen und Mentalitäten hat mich immer gereizt. Daran denke ich gern zurück.

Helmbrecht: Ich vermisse die vielen persönlichen Gespräche, das Beisammensein nach den Veranstaltungen, die Messen mit den persönlichen Kontakten zu den Mitarbeitern. Ich denke gerne daran zurück, dass ich mich immer auf die Führungskräfte und Mitarbeiter des BSI verlassen konnte.

„Die Jahre vor der Gründung des BSI waren schwer. Das ‚Projekt BSI' hatte viele Feinde und stand oft genug vor dem Scheitern."

Dr. Otto Leiberich, BSI-Präsident von 1991 bis 1992

Woran weniger gern?

Leiberich: Ich habe mich stets mehr als Fachmann denn als Administrator gesehen. Mein Ziel war, über alle fachlichen Arbeiten genau informiert zu sein, um bei Weichenstellungen kompetent mitentscheiden zu können. Weniger hat es mir gefallen, öffentlich auftreten zu müssen, etwa vor den zuständigen Bundestagsausschüssen, dem Rechnungshof, dem Finanzministerium oder auch gegenüber Presse-Organen. Diese Auftritte haben mir zwar oft hohe Anerkennung beschert, waren aber mit schlaflosen Nächten verbunden.

Helmbrecht: Da muss ich lange nachdenken ...

Wie hat die Rolle als BSI-Präsident Ihren privaten Umgang mit Informationstechnik beeinflusst?

Leiberich: Ich verdanke der Informationstechnik viel. Nach meinem Ausscheiden aus dem Amt habe ich eine Zeit lang junge IT-Unternehmen beraten und wissenschaftlich gearbeitet. Ohne Computer und die entsprechende Software wäre das unmöglich gewesen. Aber ich gestehe, mit der Sicherheit habe ich es nicht so genau genommen. Nach kurzer Zeit habe ich alle Vorsichtsmaßnahmen, die ich vorher selbst oft gepredigte hatte, in den Wind geschlagen. Die Strafe war hart, eines Tages legte ein Schädling meinen Computer lahm. Alle Bemühungen, ihn wieder zum Laufen zu bringen, scheiterten. Meine alten Kollegen wollte ich nicht zu Hilfe rufen, den Spott wollte ich nicht ertragen. Da ich überdies nachlässig bei der Datensicherung war, habe ich wertvolle Dateien verloren.

Henze: Als Werkstudent habe ich im Jahre 1959 die Programmierung in der Maschinensprache des Rechners Z22 der Firma Zuse gelernt. Später habe ich mich über Jahrzehnte mit der Förderung innovativer IT-Anwendungen befasst, bei denen die IT- Sicherheit zeitgemäß eine eher untergeordnete Rolle spielte. Mein privater Umgang mit der IT ist heute geprägt von den genannten Erfahrungen ergänzt durch die Sensibilisierung für Fragen der IT-Sicherheit.

Helmbrecht: Ich gehe noch bewusster mit meinem Computer um, und ich rede auch im Familien- und Freundeskreis – wenn es angebracht ist – über IT-Sicherheit.

... und das passierte noch 2010

2010 im Überblick

Januar

19. – 21. Januar

Omnicard 2010

Auf der Omnicard in Berlin ist das BSI im Rahmen der eCard-Strategie der Bundesregierung, die z. B. den elektronischen Reisepass und Personalausweis sowie die elektronische Gesundheitskarte beinhaltet, der Ansprechpartner in Fragen der IT-Sicherheit.

27. – 28. Januar

LÜKEX 2010

Das BSI beteiligt sich an der LÜKEX (Länder übergreifende Krisenmanagementübung / EXercise)

Februar

4. – 5. Februar

COSADE 2010

Der „First International Workshop on Constructive Side-Channel Analysis and Secure Design“ (COSADE 2010) in Darmstadt wird von CASED und dem BSI organisiert.

9. Februar

Safer Internet Day

Anlässlich des von der EU organisierten Aktionstages Safer Internet Day hat das BSI unter einer kostenlosen Telefonhotline Fragen zum Thema Internetsicherheit beantwortet.

März

4. – 9. März

RSA Conference in San Francisco

Auf dem vom TeleTrusT im Auftrag des Bundeswirtschaftsministeriums organisierten deutschen Gemeinschaftsstand auf der RSA Conference in San Francisco präsentiert das BSI seine Dienstleistungen und Projekte.

2. – 6. März

CeBIT 2010

Auf der CeBIT 2010 beteiligt sich das BSI mit einem Messestand und einer Vortragsreihe im Convention Center. Präsentiert werden unter anderem die Themen Sicherheit im Internet, IT-Grundschutz, sichere mobile Lösungen, IT-Sicherheitszertifizierung und Sicherheit hoheitlicher Dokumente. (Foto)

16. März

1. IT-Grundschutztag

Der erste IT-Grundschutztag 2010 in Bonn behandelt schwerpunktmäßig den Themenkomplex „Virtualisierung von IT-Systemen – Risiken und Abhängigkeiten“.

April

22. April
Jahrestreffen Geheimschutz

Auf Einladung des BSI findet bei der BAköV in Brühl das erste Jahrestreffen zum Themenbereich des materiellen und IT-Geheimschutzes statt. Zielgruppe sind Mitarbeiterinnen und Mitarbeiter aus Bundes- und Landesbehörden, die Aufgaben und Tätigkeiten im Umfeld des materiellen und IT-Geheimschutzes wahrnehmen.

22. April
Girls' Day

Das BSI beteiligt sich am 10. bundesweiten Mädchen-Zukunftstag Girls' Day mit Vorträgen und Präsentationen zum Thema „Bits und Bytes für Girls".

27. – 28. April
Effizienter Staat

Das BSI beteiligt sich als Aussteller am 13. Deutschen Verwaltungskongress „Effizienter Staat" und informiert dort über das Projekt STORK (Secure idenTity acrOss boRders linKed). Das BSI vertritt in dem von der EU geförderten, groß angelegten Pilotprojekt die Bundesrepublik Deutschland.

27. – 28. April
Interdisziplinäres Symposium

Die Arbeitsgruppe Identitätsschutz im Internet (a-i3) und das BSI veranstalten in Bochum ein Symposium zum Thema „Sichere Identitäten, Daten und Dienste: eCards – De-Mail – Cloud Computing – Patientendaten".

Mai

5. Mai
SOA - Workshop

In Bonn findet der erste Workshop des BSI zum Thema „Sicherheit in Serviceorientierten Architekturen (SOA)" statt.

12. Mai
BKA/BSI-Wirtschafts-konferenz

An der vom BKA und BSI organisierten Wirtschaftskonferenz zum Thema „CyberCrime – eine globale Gefahr?" nehmen Vertreter der Sicherheitsbehörden von Bund und Ländern sowie der Wirtschaft teil.

19. Mai
RFID-Workshop

Das BSI veranstaltet den öffentlichen Workshop „Technische Richtlinien für den sicheren RFID-Einsatz". (Foto)

Juni

9. – 12. Juni
LinuxTag 2010

Auf dem LinuxTag in Berlin zeigt das BSI seine aktuellen IT-Sicherheitslösungen auf Basis von Freier, Libre und Open Source Software („FLOSS").

Juli

1. Juli

Call for Papers

Start des Call for Papers: „Sicher in die digitale Welt von morgen“ lautet das Motto des 12. Deutschen IT-Sicherheitskongresses, der im Mai 2011 in Bonn stattfindet.

August

21. – 22. August

Einladung zum Staatsbesuch in Berlin

In Berlin findet zum zwölften Mal der Tag der offenen Tür der Bundesregierung unter dem Motto „Einladung zum Staatsbesuch“ statt. Das BSI stellt sein Informationsangebot für Bürger zum Thema Internetsicherheit vor.

September

15. September

Start des Anti-Botnet-Beratungszentrum

Das Anti-Botnet-Beratungszentrum hat seine Tätigkeit aufgenommen. Unter Federführung des eco - Verbands der deutschen Internetwirtschaft bietet das Anti-Botnet-Beratungszentrum Internetnutzern eine Anlaufstelle, deren Computer mit einem Botnetz-Schadprogramm infiziert ist.

21. – 23. September

11th ICCC

Das BSI nimmt mit Zertifikatsvergaben und Vorträgen an der elften International Common Criteria Conference in Antalya/Türkei teil.

24. September

2. IT-Grundschutztag

Der zweite IT-Grundschutztag des BSI in Kooperation mit der HiSolutions AG findet in Berlin statt und steht unter dem Titel „Zertifizierung aus verschiedenen Blickwinkeln“. (Foto)

27. – 28. September

Jahrestagung für IT-SiBe

BSI und BAköV führen gemeinsam die Jahrestagung für IT-Sicherheitsbeauftragte der Bundesbehörden durch.

Oktober

5. – 7. Oktober
ISSE 2010

Das BSI fokussiert bei der Information Security Solutions Europe (ISSE) in Berlin mit seinem Ausstellungsstand und einem Workshop das Thema neuer Personalausweis (nPA).

5. – 8. Oktober
Messe Security in Essen

Auf der security 2010 in Essen präsentiert das BSI allgemeine Beratungs- und Dienstleistungen zur IT-Sicherheit und berät zu Themen wie materielle IT-Sicherheit und IT-Grundschutz für kleine und mittlere Unternehmen.

6. – 7. Oktober
PITS 2010

Unter dem Motto „Sicherheit in virtualisierten Welten“ findet die Public IT-Security (PITS) in Berlin statt. Die Kongressmesse richtet sich speziell an die öffentliche Verwaltung. BSI-Experten beteiligen sich an unterschiedlichen Foren.

19. – 21. Oktober
it-sa

Das BSI beteiligt sich an der Leitmesse für IT-Sicherheit, der it-sa in Nürnberg, mit einem Messestand, mehreren Vorträgen und einem BSI-IT-Grundschutztag.

20. Oktober
3. IT-Grundschutztag

Unter dem Motto „Effizienz und Internationale Ausrichtung im IT-Grundschutz“ findet der dritte IT-Grundschutztag in Zusammenarbeit mit der TÜV Informationstechnik GmbH auf der it-sa in Nürnberg statt.

27. – 28. Oktober
Moderner Staat 2010

Präsentationsthemen des BSI beim Modernen Staat in Berlin sind IT-Sicherheitsberatung, IT-Grundschutz und IS-Revision. Darüber hinaus bietet das BSI ein Vortragsprogramm an.

November

1. November
nPA-Einführung

Einführung des neuen Personalausweises (nPA) in der Bundesrepublik.

16. November
EICAR-Tagung

Die Tagung der Arbeitsgruppe WG2 von EICAR (European Institute of Computer Antivirus Research), die sich mit dem Informationsaustausch über Malware und Antiviren-Programme zwischen Administratoren, Verantwortlichen der IT-Sicherheit und Herstellern befasst, findet im BSI statt.

25. November
Deutscher IT-Sicherheitspreis

Verleihung des dritten Deutschen IT-Sicherheitspreises unter der Schirmherrschaft von BSI-Präsident Michael Hange.

25. November
4. IT-Grundschutztag

Der vierte IT-Grundschutztag 2010 zum Thema „Sicherheitsaspekte von Cloud Computing” findet mit dem BSI-Kooperationspartner Fraunhofer SIT in Darmstadt statt.

Dezember

6. – 7. Dezember
ZertiFA 2010

Das BSI nimmt mit Vorträgen an der ZertiFA 2010 in Berlin teil.

7. Dezember
5. Nationaler IT-Gipfel

Das BSI nimmt am fünften Nationalen IT-Gipfel in Dresden teil.

Bildnachweis
BMI, BMWI, BSI, BSI-Mitarbeiter, Deutsche Messe Hannover, eco, Eric Lichtenscheidt, Europäische Kommission, LinuxTag/Messe Berlin, Shutterstock, Susanne Stark, T-Systems/HTC, SecuMedia/Peter Hohl, secunet/Lenovo, STORK

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
53175 Bonn

Konzept und Projektleitung
Anke Gaul

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI
DauthKaun Communication Group

Layout und Gestaltung
DauthKaun Werbeagentur

Druck
Druckpartner Moser, Rheinbach

Stand
Juli 2011

Artikelnummer
BSI-JB 11602

Bezugsstelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Referat 321 – Information, Kommunikation, Öffentlichkeitsarbeit
Godesberger Allee 185 - 189
53175 Bonn
Tel.: +49 228 99 9582-0
E-Mail: oeffentlichkeitsarbeit@bsi.bund.de
Internet: www.bsi.bund.de