Bundesamt
für Sicherheit in der
Informationstechnik

Mit Sicherheit.

BSI Jahresbericht 2008/2009

Sichere Mobilkommunikation
Neue Herausforderungen durch gesteigerte Funktionalität

Immer im Einsatz
Ein Tag im nationalen IT-Lage- und Analysezentrum

Der neue Personalausweis
Sicheres Ausweisen im Internet

Mit Sicherheit.

BSI Jahresbericht 2008/2009

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

Dr. Thomas de Maizière, MdB
Bundesminister des Innern

Schnell und flexibel auf veränderte Rahmenbedingungen reagieren

Liebe Leserinnen und Leser,

die Informationstechnik eröffnet uns viele neue Chancen. Sie verändert unsere Welt so rasch wie keine der industriellen und technologischen Revolutionen zuvor. Das Internet, der „Cyber-Space", ist Ort für Innovation und Wertschöpfung. Deutschlands Wohlstand und Teilhabe an der globalen Wirtschaft hängen entscheidend von unseren Fähigkeiten ab, die Möglichkeiten der IT und des Internets zu nutzen. Ein Schlüssel dazu ist das Vertrauen in die Sicherheit der Informationstechnik.

Das Bundesamt für Sicherheit in der Informationstechnik ist bei der IT-Sicherheit ein wichtiger Partner für Wirtschaft, Verwaltung und Gesellschaft. Gegründet vor nunmehr 19 Jahren hat das BSI schon viel geleistet. Das BSI ist heute gefragter Kompetenzträger in Deutschland und Europa. Nach seinem erfolgreichen Modell werden in unseren europäischen Nachbarländern gleichartige Institution aufgebaut.

Dem BSI wird bei der Gestaltung der IT-Systeme auch in Zukunft eine wichtige Rolle zukommen. Es muss schnell und flexibel auf sich verändernde Rahmenbedingungen reagieren und innovative Lösungen für IT- Sicherheit bereitstellen. Angemessene IT-Sicherheit ist kein Zustand, sondern ein fortwährender Prozess, für den alle Beteiligten gleichermaßen verantwortlich sind – seien sie Anwender, Anbieter oder IT-Sicherheitsbehörde.

Ich wünsche Ihnen bei der Lektüre des Berichts viele Einsichten und Denkanstöße für die IT-Sicherheit.

Berlin, im Mai 2010

Ihr Dr. Thomas de Maizière

Mit Strategie und Know-how IT-Sicherheit bestärken und ausbauen

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Liebe Leserinnen und Leser,

annähernd 70 Prozent der Deutschen sind mittlerweile online, und in den meisten deutschen Haushalten befinden sich mehr als ein PC oder Notebook. Einkaufen über das Internet, Bankgeschäfte online tätigen, eGovernment, Kontakte im Internet pflegen – ein Großteil der privaten und geschäftlichen Interaktionen haben Einzug in die virtuelle Welt gehalten. Mit immer weiter steigender Popularität. In dem Maße, in dem Nutzerinnen und Nutzer Aktivitäten ins Internet verlagern, erfährt der Ansporn für Cyberkriminalität ein dynamisches Wachstum. Professionalität zeichnet Angriffe auf Systeme aus. Finanzielle Anreize – anstelle des früheren Strebens nach öffentlicher Aufmerksamkeit – sind die vorrangigen Beweggründe der Angreifer. In der Folge geben sie sich Mühe, ihre Attacken möglichst unbemerkt zu halten, was eine Bekämpfung erheblich erschwert.

Wir, das BSI mit seinen rund 500 Mitarbeitern, sehen diese Herausforderung als unsere Motivation. Lösungsmöglichkeiten für mehr IT-Sicherheit zu etablieren, auch unter dem Aspekt des Daten- und Verbraucherschutzes, erfordert Ideenreichtum, Flexibilität und nicht zuletzt auch einen mutigen Blick in die Zukunft. Erweiterter Handlungsspielraum ergibt sich für uns dabei aus dem neuen BSI-Gesetz, das seit August 2009 in Kraft ist und unser Amt mit weiteren Kompetenzen ausstattet. Das BSI sieht sich als IT-Sicherheitsgestalter und IT-Sicherheitspartner, wir kooperieren mit Institutionen in Wirtschaft und Verwaltung – für mehr IT-Sicherheit und zum Wohle aller Internetnutzerinnen und -nutzer in der Bundesrepublik. Aber auch im internationalen Umfeld treiben wir IT-Sicherheitskonzepte und -standards voran, denn in der virtuellen Welt existieren keine Grenzen.

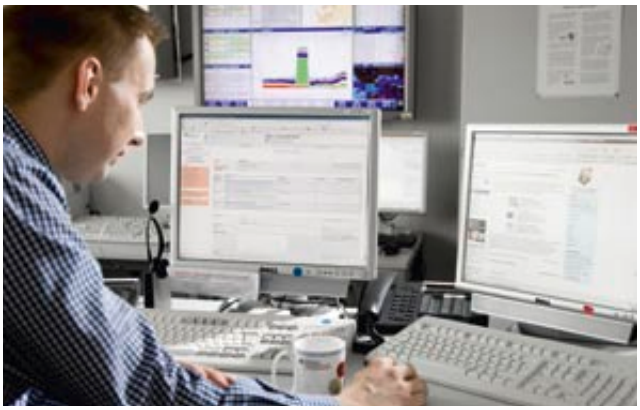
Persönlich bin ich dem BSI bereits seit vielen Jahren als Mitarbeiter verbunden und freue mich, in meiner neuen Rolle als Präsident des BSI, mit vorliegender Publikation einen Einblick in unsere Arbeit und ausgesuchte Projekte geben zu können. Berichtszeitraum sind in erster Linie die Jahre 2008 und 2009, gleichzeitig wagen wir aber einen Blick in die Zukunft. Denn eines ist sicher: Wir alle werden zukünftig noch stärker vom Funktionieren einer zuverlässigen Informationstechnik abhängig sein. Meine Mitarbeiter und ich werden uns weiterhin dafür einsetzen, dass Prozesse und Anwendungen sicher und vertrauenswürdig gestaltet werden und Nutzerinnen und Nutzer uneingeschränkt von den Möglichkeiten der Informationstechnik profitieren können.

Bonn, im Mai 2010

Ihr Michael Hange

Seite 8
Wendepunkte für die Informationssicherheit

Seite 18
Ganzheitliche Informationssicherheit als Erfolgsmodell – Maßstäbe für Informationssicherheitsmanagement



Seite 24
Immer im Einsatz: Ein Tag im nationalen IT-Lage- und Analysezentrum

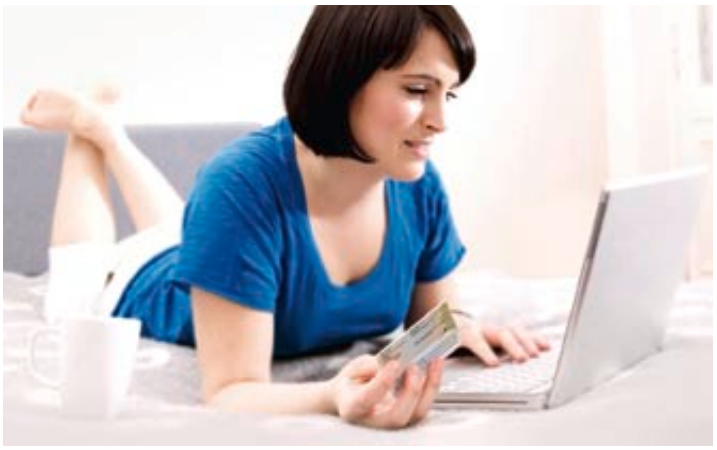
Weichen stellen – Zukunft planen

IT-Sicherheit gestalten

Sicherheit für die Cyberwelt

Seite 37

Garantiert abhörsicher! Lauschabwehr beim NATO-Gipfel in Baden-Baden und beim Besuch des US-Präsidenten Obama in Dresden



Seite 44

Sicheres Ausweisen im Internet mit dem neuen Personalausweis – ein weltweit einmaliges Projekt des BSI

Seite 54

Herz und Hirn des BSI: Unsere Mitarbeiter

Kommunizieren – mobil und geschützt

Sichere elektronische Identitäten

Herausforderungen gemeinsam angehen

Weichen stellen – Zukunft planen

Wendepunkte für die Informationssicherheit

Horst Samsel, Abteilungsleiter Zentrale Aufgaben

Zahlreiche Prozesse und Aufgaben in Verwaltung und Unternehmen sind heute IT-gestützt. Wirtschaft, Verwaltung sowie Bürgerinnen und Bürger sind damit in hohem Maße von einer funktionierenden Informationstechnik und sicheren Informationsinfrastrukturen abhängig. Den Chancen, die sich aus der Nutzung der Informations- und Kommunikationstechnologie ergeben, stehen aufgrund der wachsenden Abhängigkeit von der Technologie jedoch auch eine Vielzahl von Risiken gegenüber. Diese ergeben sich aus der immer stärkeren Bedrohung durch Cyberkriminelle. Nachrichtendienste und organisierte Kriminalität führen heute hoch professionelle IT-Angriffe durch, bei denen Informationen und IT-Strukturen der Bundesverwaltung, von Unternehmen und auch der Privatnutzer im Mittelpunkt des Interesses stehen. So verwundert es nicht, dass der IT-Sicherheit eine immer größere Bedeutung auf wirtschaftlicher, gesellschaftlicher, politischer und rechtlicher Ebene zukommt.

GEWÄHRLEISTUNG DER DATENSICHERHEIT ALS BESTANDTEIL DES GRUNDGESETZES

Mit dem so genannten Volkszählungsurteil vom 15. Dezember 1983 hat das Bundesverfassungsgericht erstmals anerkannt, dass es ein Grundrecht auf informationelle Selbstbestimmung gibt. Abgeleitet wird dies aus dem allgemeinen Persönlichkeitsrecht und der Menschenwürde-Garantie des Grundgesetzes. Mit seinem Urteil vom 27. Februar 2008 zum „Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme“ hat das Bundesverfassungsgericht nunmehr einen weiteren Meilenstein zur Etablierung des Schutzes von Daten gesetzt. Das Grundrecht dient dem Schutz von persönlichen Daten, die in informationstechnischen Systemen gespeichert oder verarbeitet werden; ein Eingriff in dieses Grundrecht ist nur in engen Grenzen möglich.

Daneben ist die IT-Sicherheit auch durch Neufassung des Art. 91c indirekt in das Grundgesetz gelangt. Dieser Artikel normiert die Zusammenarbeit von Bund und Ländern in der Informationstechnik der öffentlichen Verwaltungen. Danach können Bund und Länder bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammenwirken und auf Grund von Vereinbarungen, die für die Kommunikation zwischen ihren informationstechnischen Systemen notwendigen Standards und Sicherheitsanforderungen festlegen.

In einer Stellungnahme vom 27. März 2008 erklärte der damalige Bundesinnenminister Dr. Wolfgang Schäuble:

„In der Kommission besteht Einvernehmen, dass wir eine neue verfassungsrechtliche Grundlage für die zentrale Infrastruktur des 21. Jahrhunderts brauchen. Was die Eisenbahn für das 19. und die Luftfahrt für das 20. Jahrhundert waren, ist die IT für unser Jahrhundert: Sie revolutioniert unsere Art zu arbeiten, zu leben und zu kommunizieren. Eisenbahn und Luftverkehr stehen schon im Grundgesetz, es ist höchste Zeit, dass sich auch die IT dort wiederfindet und klare Verantwortlichkeiten für die Nutzung der Informationstechnik in der öffentlichen Verwaltung geschaffen werden.“ (http://www.cio.bund.de)

„Das BSI-Gesetz stellt unsere Behörde für heutige und künftige Herausforderungen in der IT-Sicherheit besser auf.“

Horst Samsel

DIE NOVELLIERUNG DES BSI-GESETZES (BSIG)

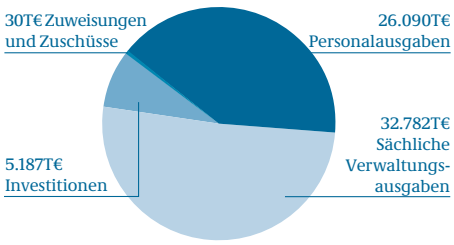
Mit dem am 19. Juni 2009 vom Bundestag verabschiedeten „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes“ wurde die Rolle des BSI als IT-Sicherheitsbehörde des Bundes gestärkt – und gleichzeitig ist damit auch die für das BSI weitreichendste Veränderung bei der gesetzlichen Verankerung der IT-Sicherheit erfolgt. Denn mit dem Gesetz wurde das Spektrum der Aufgaben und Befugnisse des BSI deutlich erweitert und die Behörde für heutige und künftige Herausforderungen in der IT-Sicherheit besser aufgestellt.

INFORMATIONSSTELLE FÜR SICHERHEITSLÜCKEN UND SCHADPROGRAMME

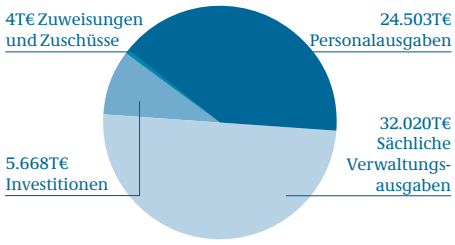
Um den aktuellen Bedrohungen adäquat begegnen zu können und der zunehmenden Bedeutung der Informations- und Kommunikationstechnologie in der heutigen Gesellschaft Rechnung zu tragen, wurden dem BSI mit der Novellierung des BSI-Gesetzes (BSIG) weitergehende Aufgaben und Befugnisse eingeräumt. Gemäß § 4 des BSIG sammelt und analysiert das BSI künftig als zentrale Meldestelle für die Zusammenarbeit der Bundesbehörden in Angelegenheiten der IT-Sicherheit Informationen über Sicherheitslücken und neue Angriffsmuster.

Das BSI in Zahlen

Haushaltsvolumen 2009: 64.089T€



Haushaltsvolumen 2008: 60.195T€



Hierdurch kann ein verlässliches Lagebild erstellt, können Angriffe frühzeitig erkannt und Gegenmaßnahmen ergriffen werden. Datenschutzrechtliche Belange sind dabei selbstverständlich zu berücksichtigen. Die Bestimmung meldepflichtiger Informationen sowie das Meldeverfahren wurden in Form einer Verwaltungsvorschrift durch das Bundesministerium des Innern unter Einbindung des Rates der IT-Beauftragten der Bundesregierung Ende 2009 erlassen.

Richtet sich § 4 BSIG primär an die Verwaltung, so ist das BSI nach § 7 BSIG jedoch auch für die Warnung der Wirtschaft und der Bürgerinnen und Bürger vor Sicherheitsrisiken zuständig. Danach darf das BSI künftig Informationen und Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten sowie vor Schadprogrammen an die betroffenen Stellen oder die Öffentlichkeit weitergeben. Zunächst besteht dabei grundsätzlich die Pflicht, den Hersteller vorab zu informieren. Er soll die Gelegenheit haben, Sicherheits-Updates zu entwickeln und seinen Kunden zur Verfügung zu stellen. Erst im Anschluss daran – oder wenn der Zweck der Maßnahme bei einer Vorabinformation nicht erreicht werden

kann – wendet sich das BSI an die Öffentlichkeit. **Über www.buerger-cert.de stehen die Informationen allen Interessierten zur Verfügung und können per Newsletter abonniert werden.**

ABSICHERUNG DER INFORMATIONSTECHNIK DES BUNDES

Neben den Aufgaben der Informationssammlung und Warnung kommt dem BSI darüber hinaus eine aktive Rolle beim Schutz der Kommunikationstechnik des Bundes zu. Das BSI hat gemäß § 5 BSIG die Befugnis erhalten, Protokolldaten sowie Daten, die beim Betrieb der Kommunikationstechnik des Bundes anfallen, zu erheben, auszuwerten, zu speichern, zu verwenden und zu verarbeiten. Hierdurch können Anzeichen für IT-Angriffe erkannt und gezielt bekämpft werden.

Um der besonderen Sensibilität der Daten gerecht zu werden, bestimmt § 5 BSIG detaillierte Anforderungen an die Datenerhebung und -auswertung. Diese Vorschrift gibt dem BSI ausschließlich die Befugnis, die beim Betrieb der Kommunikationstechnik des Bundes anfallenden Daten zu erheben und automatisiert auszuwerten. Sofern eine Weiterverarbeitung nicht ausnahmsweise zulässig ist, sind die Daten nach der Auswertung unverzüglich und spurenlos zu löschen. Insbesondere ist die personenbezogene Verwendung der Daten zu sachfremden Zwecken, beispielsweise zur Erstellung von Kommunikationsprofilen oder zur Verhaltens- und Leistungskontrolle der Mitarbeiter, unzulässig. Nur wenn konkrete Verdachtsmomente vorliegen, dass die Daten zur Abwehr von Gefahren durch Schadprogramme erforderlich sein können, dürfen sie individuell ausgewertet werden. Erfasst werden lediglich diejenigen Daten, die beim Betrieb der Kommunikationstechnik des Bundes anfallen – und nicht von unbeteiligten Dritten stammen, die sich im Internet bewegen. Auch die Verwendung von Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, ist untersagt.

SICHERHEITSZERTIFIKATE ALS QUALITÄTSNACHWEIS

Das BSI ist weiterhin befugt, einheitliche und strenge Sicherheitsstandards für die Bundesverwaltung zu definieren und bei Bedarf geeignete Produkte entwickeln zu lassen beziehungsweise auszuschreiben und bereitzustellen (§ 8 BSIG). So kann verhindert werden, dass ungeeignete Produkte mit Schwachstellen oder manipulierte IT-Komponenten in der Bundesverwaltung und in den Regierungsnetzen zum Einsatz kommen.

Mit § 9 BSIG wird das BSI als nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit in die Lage versetzt, durch die Aufstellung von Zertifizierungskriterien und die Ausstellung von Zertifikaten für geeignete Qualitätsnachweise sicherheitsrelevanter Angebote zu sorgen (vgl. S. 14ff).

Der Koalitionsvertrag: Handlungsfelder für das BSI

Auf dem Fundament der erweiterten gesetzlichen Vorgaben kann das BSI den gestiegenen Herausforderungen der IT-Sicherheit wirkungsvoll begegnen. Doch schon heute ist klar, dass aufgrund der schnellen technischen Entwicklungen und sich immer wieder neu ergebender Rahmenbedingungen weiterhin neue Handlungsfelder auf das BSI zukommen. So heißt es in dem von CDU/CSU und FDP im Oktober 2009 nach der Bundestagswahl 2009 geschlossenen Koalitionsvertrag:

„Wir (der Verfasser: die Koalitionsparteien) werden uns für die Stärkung der IT-Sicherheit im öffentlichen und nichtöffentlichen Bereich einsetzen, um vor allem kritische IT-Systeme vor Angriffen zu schützen. Hierzu wollen wir insbesondere durch Aufklärung und Sensibilisierung der Öffentlichkeit die Menschen zu mehr Selbstschutz und zur Nutzung sicherer IT-Produkte anregen. Das Bundesamt für Sicherheit in der Informationstechnik werden wir mit dieser Zielrichtung stärken.“

„Eine vertrauenswürdige, leistungsfähige und sichere Informations- und Kommunikationstechnik ist für unser Hochtechnologieland und den Wirtschaftsstandort Deutschland unverzichtbar. Wir werden die IT gegen innere und äußere Gefahren schützen, um die wirtschaftliche Leistungsfähigkeit und administrative Handlungsfähigkeit zu erhalten. Daher werden wir ein besonderes Augenmerk auf die Abwehr von IT-Angriffen richten und hierfür Kompetenzen in der Bundesverwaltung beim Beauftragten der Bundesregierung für Informationstechnik bündeln. Zu seiner Unterstützung werden wir das Bundesamt für Sicherheit in der Informationstechnik als zentrale Cyber-Sicherheitsbehörde weiter ausbauen, um insbesondere auch die Abwehr von IT-Angriffen koordinieren zu können.“

Investition in IT-Sicherheit

Frank Koob, Forschungskoordinator im BSI

IT-Sicherheitsforschung: Investition in die Zukunft

Eine vorausschauende nationale IT-Sicherheitspolitik muss Schritt halten mit der Technologieentwicklung, denn das Innovationspotenzial im Umfeld der Informations- und Kommunikationstechnik vergrößert sich zunehmend. Damit geht eine ansteigende Gefährdung durch IT-Sicherheitsrisiken einher, was deutlich macht, dass neben der eigentlichen Technologieforschung die IT-Sicherheitsforschung immer mehr an Bedeutung gewinnen muss, wenn der wachsenden Bedrohungslage zukünftig präventiv und nachhaltig begegnet werden soll. Sowohl der querschnittliche Charakter als auch die besondere Bedeutung der IT-Sicherheit begründen dabei zunehmend die Notwendigkeit einer eigenständigen IT-Sicherheitsforschung, im Gegensatz zur bisherigen begleitenden Betrachtung und Behandlung innerhalb der allgemeinen Technologieforschung. Über diese Eigenständigkeit wurde und wird es zunehmend möglich, eine nachhaltige IT-Sicherheitsforschung mit Partnern in Deutschland zu fördern und frühzeitig die IT-Sicherheit als integralen Bestandteil in Technologieentwicklungen einzubinden und – basierend auf neuen Entwicklungen – auch innovative IT-Sicherheitsverfahren auszuarbeiten und in marktfähige Produkte zu überführen. Hierdurch kann ein massiver Sicherheitsgewinn realisiert werden.

Innovative Forschungsprogramme

Anwendungsbezogene Neuerungen in den Technologiefeldern Internet-Frühwarnsysteme, Trusted-Computing sowie Biometrie- und Ausweissysteme werden im BSI-eigenen IT-Sicherheitsforschungsprogramm (Zukunftsfonds) erarbeitet. Hierfür wurden von 2006 bis 2009 Mittel in Höhe von 36,5 Millionen Euro aus dem sechs Milliarden-Euro-Innovationsprogramm der Bundesregierung bereitgestellt. Die Projekte sollen im Jahr 2010 abgeschlossen werden.

Im Oktober 2008 verständigten sich das Bundesministerium des Innern (BMI) und das Bundesministerium für Bildung und Forschung (BMBF) zudem in einer gemeinsamen Erklärung darauf, IT-Sicherheit als einen neuen Schwerpunkt der Forschungsförderung im IKT-Bereich zu etablieren. Hierzu präsentierten der damalige Bundesinnenminister Dr. Wolfgang Schäuble und Bundesforschungsministerin Prof. Dr. Annette Schavan im September 2009 ein umfangreiches gemeinsames Arbeitsprogramm zur IT-Sicherheitsforschung. Für eine Laufzeit von fünf Jahren werden hierfür Fördermittel in Höhe von 30 Millionen Euro bereit gestellt. Die Förderung zielt auf die Schaffung der Grundlagen für die Entwicklung überprüfbarer und durchgehend sicherer IT-Systeme sowie auf die Erforschung neuer Ansätze bei der Analyse und Absicherung von IKT-Systemen ab. Auf die Festlegung der Themen des Arbeitsprogramms hatte das BSI einen maßgeblichen Einfluss. Darüber hinaus ist die Behörde bei der Bewertung der Anträge und an der Auswahl der zu fördernden Projekte beteiligt. An dem Programm können Hochschulen, Forschungseinrichtungen und andere FuE-Institute, Behörden und Unternehmen teilnehmen, die ihren Sitz und die überwiegende Ergebnisverwertung in der Bundesrepublik haben.

Forschungskooperationen für IT-Sicherheit

Die zunehmend komplexeren Anforderungen an die IT-Sicherheitsforschung erfordern aber auch eine ebenso langfristige wie kontinuierliche interdisziplinäre Zusammenarbeit von Forschungseinrichtungen, Industrie und dem BSI. Ein Instrument, um diese Zusammenarbeit zu organisieren, ist die Bildung von Forschungsclustern und Kooperationen. Ziel der BSI-Beteiligung an diesen Clustern ist, eine strategische Einflussnahme auf die inhaltliche Ausrichtung und damit insbesondere eine Berücksichtigung von BSI-spezifischen IT-Sicherheitsaspekten als Teil der IT-Forschung und -Entwicklung zu erreichen. Außerdem wird über die Förderung von Innovationen und die Verbesserung der Ausbildung indirekt auch die deutsche IT-Sicherheitsindustrie gestärkt. Aktuell besteht eine Kooperation mit dem Center for Advanced Security Research Darmstadt (CASED) und eine Zusammenarbeit auf Basis eines Memorandum of Understanding zwischen dem BMI/BSI und der Fraunhofer-Gesellschaft auf dem Gebiet der IT-Sicherheit.

220 Millionen Euro für mehr IT-Sicherheit – Das IT-Investitionsprogramm des Bundes

Neben der Novellierung des BSI-Gesetzes steht die IT-Sicherheit in einem weiteren Bereich im Fokus der politischen Öffentlichkeit: Mit dem Gesetz zur Sicherung von Beschäftigung und Stabilität hat der Bundestag im Jahr 2009 auch Investitionen von rund 500 Millionen Euro in der Informations- und Kommunikationstechnik beschlossen. Mit rund 220 Millionen Euro soll fast die Hälfte des Budgets in Maßnahmen zur IT-Sicherheit investiert werden. Zu diesen zählen unter anderem Krypto-Handys, Verschlüsselungstechnologien, Maßnahmen zur Erhöhung der Netzsicherheit, Grundschutz-Zertifizierungen, Sicherheitsschulungen sowie Maßnahmen im Umfeld des neuen Personalausweises (nPA).

Das BSI schafft Lösungen

Konkret führt das BSI Projekte zur Bereitstellung sicherer mobiler Sprach- und SMS-Kommunikation – bis VS-NfD – für die Bundesverwaltung durch. Ziel der Maßnahme ist, die vorhandenen Lösungen interoperabel zu gestalten und entsprechende Geräte, die sogenannten Krypto-Handys, zu beschaffen (vgl. S. 34ff). Ein weiteres Projekt ist die gemeinsame Beschaffung von Geräten für die sichere, mobile E-Mail-Kommunikation mit PDAs, die den IT-Sicherheitsanforderungen des Bundes gemäß den BSI-Vorgaben entsprechen. Auch die initiale Einführung einer sicheren, zugelassenen Lösung für mobile Arbeitsplätze (Laptops) zur Verarbeitung lokaler Daten sowie der sicheren Netzanbindung über öffentliche Netze an die Intranets von Behörden mit erhöhtem Schutzbedarf werden vom BSI verantwortet.

Aber nicht nur die sichere mobile Kommunikation wird durch Maßnahmen des BSI vorangetrieben. Weitere Projekte im Rahmen des Investitionsprogramms befassen sich mit der flächendeckenden Abwehr von Schadprogrammen (Malware) in den Regierungsnetzen. Insbesondere die Verbesserung der Internetsicherheit und die Sicherheit der Webangebote der Verwaltung sind hier zu nennen, aber auch die Beschaffung spezialisierter IT-Sicherheitsprodukte zur Abwehr von Schadprogrammen in Netzen für den lokalen Einsatz in Behörden.

Schwerpunkte der Forschungsförderung

- Sicherheit in unsicheren Umgebungen: Eine Absicherung großer IKT-Umgebungen (beispielsweise im Internet) ist aufgrund der Komplexität de facto nicht mehr möglich. Die Sicherheit von IKT-Systemen, insbesondere von mobilen Systemen, soll deshalb auch in unsicheren Umgebungen gewährleistet werden.
- Schutz von Internet-Infrastrukturen: Eine vollständige Absicherung von IKT-Systemen gegen Angriffe ist nicht möglich, aber die Systeme können gegen „Epidemien“ geschützt werden. Dazu müssen Angriffe erkannt, Schadsoftware isoliert, eine Weiterverbreitung verhindert und Dritte rechtzeitig informiert werden.
- Eingebaute Sicherheit: Die nachträgliche Absicherung von IKT-Systemen ist extrem aufwendig und vielfach gar nicht möglich. IKT-Systeme sollen deshalb bereits vorab so konzipiert und entwickelt werden, dass sie (beweisbar) über ein definiertes IT-Sicherheitsniveau verfügen.
- Neue Herausforderungen zum Schutz von IT-Systemen und zur Identifikation von Schwachstellen: Um speziellen – und zukünftig eventuell möglichen – Angriffen entgegenwirken zu können, müssen zur Absicherung von IKT-Systemen auch neuartige Techniken, Methodiken und Ansätze entwickelt werden.

Quelle: BMBF/BMI „Arbeitsprogramm IT-Sicherheitsforschung“

IT-Sicherheit gestalten

Maßstäbe für die Produktsicherheit

Gereon Killian, Referatsleiter Zertifizierung im BSI

„Die Nachfrage nach vertrauenswürdigen IT-Produkten steigt.“

Gereon Killian

Um IT-Sicherheit in Produkte zu integrieren stellt das BSI angemessene IT-Sicherheitsstandards und Prüfvorschriften bereit. Sie werden gemäß den ständig steigenden Erfordernissen entwickelt, angepasst und für die Wirtschaft bereitgehalten.

Die IT-Sicherheitsstandards – insbesondere die Schutzprofile (Protection Profiles, PP) nach den weltweit anerkannten Common Criteria (CC) und die Technischen Richtlinien (TR) – dienen als Grundlage für die Entwicklung von IT-Sicherheitsprodukten und legen auch systematisch aufgebaute Prüfvorschriften für die IT-Sicherheitsevaluierung fest. Darüber hinaus liefern die Technischen Richtlinien Kriterien und Methoden für Konformitätsprüfungen – sowohl bei der Interoperabilität von IT-Sicherheitskomponenten als auch bei umgesetzten funktionalen IT-Sicherheitsanforderungen. Neben der Zertifizierung von Schutzprofilen und IT-Sicherheitsprodukten nach den Common Criteria werden auch Bestätigungen nach dem deutschen Signaturgesetz ausgestellt.

In den Jahren 2008 und 2009 wurden – wie bereits in den Jahren zuvor – Steigerungen an Zertifizierungsverfahren verzeichnet. Die Nachfrage nach vertrauenswürdigen IT-Produkten ist ungeachtet der Wirtschaftskrise weiter gestiegen. Das BSI setzt deshalb neue Maßstäbe für die Sicherheit von IT-Produkten.

Ein Beispiel aus der Praxis: Die Technische Richtlinie zur vertrauenswürdigen elektronischen Langzeitspeicherung

Wachsende Berge von Akten und Dokumenten machen für Behörden den Einsatz effizienterer Prozesse zur Interaktion mit Bürgern, Unternehmen und anderen Institutionen unumgänglich. Der hierfür erforderliche Einsatz entsprechender elektronischer Kommunikations- und Informationstechniken ermöglicht neben der Vereinfachung und Beschleunigung des Datenaustausches in vielen Fällen auch Einsparungen.

Durch die immer schneller fortschreitende Digitalisierung ergeben sich neue Herausforderungen:

- Elektronische Dokumente liefern zunächst keine Anhaltspunkte für ihre Integrität und Authentizität. Der Schutz der Wahrung von Rechtsansprüchen des Ausstellers oder Dritter und der Nachweis der Ordnungsmäßigkeit im elektronischen Rechts- und Geschäftsverkehr ist nicht gewährleistet und muss durch zusätzliche technische und organisatorische Maßnahmen erreicht und dauerhaft erhalten werden.
- Über die geforderten langen Aufbewahrungszeiträume und damit über immer kürzer werdende informationstechnische Innovationszyklen hinweg müssen Lesbarkeit und Verfügbarkeit von Speichermedien und Datenformaten gewährleistet sein – unabhängig von einzelnen Produkten und Herstellern.
- Der Zugriff auf elektronische Daten und Dokumente muss den Anforderungen des Datenschutzes und der Datensicherheit genügen, auch über lange Zeiträume und den Wechsel von Systemen hinweg.

Gegenstand der vom BSI entwickelten Technischen Richtlinie 03125 ist es, auf der Grundlage bestehender rechtlicher Normen und bereits bestehender technischer Standards sowie nationaler und internationaler Erfahrungen, Anforderungen zum Beweiswerterhalt kryptografisch signierte Dokumente zu definieren, die bei der elektronischen Aufbewahrung bis zum Ende der jeweiligen Fristen zu beachten sind.

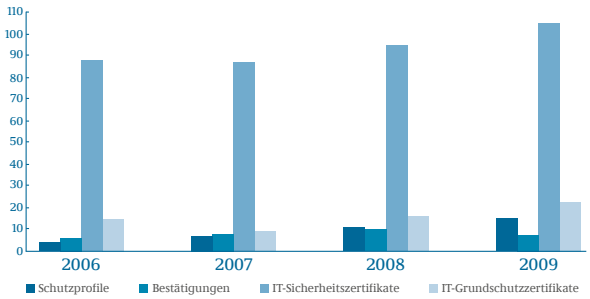
Da die bei elektronischen Signaturen zum Einsatz kommenden kryptografischen Verfahren im Laufe der Zeit einem „technischen Verfall“ unterliegen können, existiert ein gesetzlich vorgegebenes Verfahren, wie dem drohenden Verlust der Sicherheitseignung der eingesetzten Schlüssel- und Hashverfahren bei elektronischen Signaturen entgegengewirkt werden kann, ohne dass es dabei zu einem Beweisverlust kommt. Mit der BSI-TR 03125 stellt das BSI einen Leitfaden zur Verfügung, der beschreibt, wie elektronisch signierte Daten und Dokumente über lange Zeiträume vertrauenswürdig gespeichert werden können und der Beweiswert aufrecht erhalten werden kann, ohne dass jedes einzelne archivierte Dokument nach einigen Jahren vollständig neu signiert werden muss. Dabei zielt die TR 03125 nicht darauf ab, bekannte und etablierte Anforderungen und Begriffsdefinitionen zu ersetzen. Vielmehr sind die Anforderungen an die ordnungsgemäße Aufbewahrung ebenfalls für elektronisch signierte Dokumente einzuhalten. Sie werden von der TR 03125 vorausgesetzt. Die Referenz-Architektur der TR 03125 versteht sich daher nicht als Ersatz für ein Archiv-System, sondern als Konzept einer Middleware, das die Umsetzung der Anforderungen zum rechtswirksamen Beweiswerterhalt während des Aufbewahrungszeitraums beschreibt.

Die TR richtet sich vornehmlich an Bundesbehörden, die ihren gesetzlichen Aufbewahrungspflichten nachkommen müssen. Darüber hinaus besitzt die Technische Richtlinie empfehlenden Charakter, denn in nahezu allen geschäftlichen Bereichen gewinnt der Bedarf an rechtswirksamer Beweiswerterhaltung kryptografisch signierter Dokumente an Bedeutung: Elektronische Unterlagen im Gesundheitswesen, Personenstandsregister und viele Dokumente mehr verlangen nach adäquaten Lösungen im Rahmen fortschreitender Digitalisierung der Geschäftstätigkeiten. Diese Beispiele zeigen die hohe Relevanz der beweiswerterhaltenden Aufbewahrung kryptografisch signierter Dokumente im Rahmen einer vertrauenswürdigen elektronischen Langzeitspeicherung.

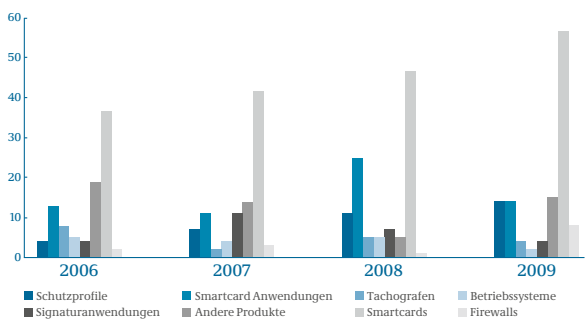
Eine BSI-Zertifizierung nach der TR 03125 dient den Herstellern entsprechender Lösungen als Nachweis einer unabhängigen neutralen Stelle, dass ihre Produkte den Anforderungen gerecht werden.

Zertifikatsübersicht

Erstellte Zertifikate



Erstellte Zertifikate nach Produktgruppen



Die Bedeutung der Zertifizierung für die Industrie

Gastbeitrag von Dr. Peter Laackmann und Marcus Janke, Infineon Technologies AG

Die heutige Gesellschaft benötigt in vielen Bereichen eine hohe, auf die Erfordernisse der Anwendung hin optimierte Sicherheit. Dies wird beispielsweise deutlich, wenn es um die Speicherung oder Verarbeitung von vertrauenswürdigen Daten geht. Das Feld erstreckt sich von personenbezogenen Daten über Vertragsdaten bis hin zu Zahlungsdaten. Solche Daten müssen unter anderem gegen unbefugten Zugriff und gegen Veränderungen geschützt werden.

Moderne Sicherheitslösungen, insbesondere Chipkarten, werden vom Hersteller zur Abwehr der vielfältigen Angriffe mit entsprechenden Gegenmaßnahmen ausgestattet. Angesichts umfangreicher Variationsmöglichkeiten der Angriffe ist es jedoch für Kunden sehr schwer ein möglichst objektives Bild der Produkte zu erhalten und damit zu einer vergleichenden Bewertung der Produktsicherheit zu kommen. Das Vertrauen in die Herstellerangaben kann jedoch durch eine unabhängige Prüfung gestärkt werden. Im Bereich der Sicherheit ist die international akzeptierte und angewandte Common Criteria-Zertifizierung das bevorzugte Mittel der Wahl.

Die Schwachstellenanalyse im Rahmen einer Common Criteria-Zertifizierung umfasst umfangreiche Untersuchungen, bei denen praktische Angriffe durchgeführt werden und der notwendige Aufwand mit Hilfe eines Punktesystems bewertet wird. Für jeden durchgeführten Angriff werden die benötigte Expertise, der Geräteaufwand, die Zeitdauer und die Anzahl der benötigten Chips berücksichtigt.

Nur wenn alle Angriffe einem hohen Angriffspotenzial widerstehen, wird für das Produkt die Sicherheitsstufe HIGH[1] vergeben.

Bereits in der Vergangenheit hat das BSI viele bedeutende Meilensteine in der Common Criteria-Zertifizierung gesetzt: Auf Betreiben des BSI wurden weltweit erstmals im Rahmen einer Produktzertifizierung Alpha-Strahlung für Fehler-Induktions-Angriffe eingesetzt. Hiermit wurde die kontinuierliche Weiterentwicklung von Angriffen in der Sicherheitszertifizierung berücksichtigt. Ein weiteres international adaptiertes Beispiel ist die Definition von Qualitätskriterien für Generatoren von echten, physikalischen Zufallszahlen, welche in der Richtlinie AIS-31 festgelegt wurden. Diese Richtlinie entwickelte sich zu einem De-facto-Standard im Bereich der Sicherheitsprodukte.

Die unabhängige Prüfung und Zertifizierung von Produkten für den Sicherheitsmarkt jeweils unter Berücksichtigung der neusten Entwicklungen ist in der heutigen Industrie unverzichtbar. Hersteller können die Common Criteria-Zertifizierung einerseits als vertrauensbildendes Instrument verwenden und andererseits die erreichte Sicherheitsstufe als werbewirksamen Nachweis einsetzen. Für Industriekunden entsteht durch die Zertifizierung ein objektiveres und vergleichbareres Bild der Marktanbieter, und durch die Forderung im Rahmen von Lastenheften oder Lieferantenbedingungen kann ein geeigneter Sicherheitslevel für Systeme erreicht werden. Endkunden und Nutzer profitieren letztlich von dem Qualitätsmerkmal der zertifizierten Sicherheit, da sie in puncto Sicherheit Vertrauen in das resultierende komplexe System erhalten. **Durch die Veröffentlichung der Zertifizierungen und deren Details auf der Internet-Seite des BSI entsteht für alle Partner eine transparente Sicherheit. Den hohen Sicherheitsanforderungen der heutigen Gesellschaft kann damit entsprochen werden.**

[1] Höchstmögliche Sicherheitsstufe bei der CC-Zertifizierung

Erhöhte Akzeptanz der Produkte

Gastbeitrag von Armin Lunkeit, Chief Development Officer und Mitglied der Geschäftsleitung, OpenLimit Group

Unser Unternehmen hat bereits zu einem frühen Zeitpunkt die Entscheidung getroffen, zertifizierte Komponenten anzubieten, wobei die Ausrichtung unseres Unternehmens an den Erfordernissen des Signaturgesetzes und der Signaturverordnung dabei im Vordergrund stehen.

Die Common Criteria-Evaluierung und -Zertifizierung hat die Entwicklungs- und QS-Prozesse des Unternehmens stark positiv beeinflusst. So konnte unter Einbeziehung der Vorgaben der Common Criteria ein Entwicklungs- und Qualitätsmodell aufgebaut werden, das die Robustheit und Sicherheit der OpenLimit Software aktiv unterstützt und Risiken in Form von Schäden bei z. B. fehlerhafter Software minimiert.

Seitdem kann OpenLimit ein beständig wachsendes Interesse an seinen Produkten verzeichnen. **Die Zertifizierung gemäß Common Criteria führt zu einer erhöhten Akzeptanz und Nachfrage der Produkte bei den Kunden, da die Common Criteria als internationale Prüfnorm in vielen Ländern anerkannt wird.** Ein immer wieder angeführtes Kriterium ist dabei, dass das angewandte Prüfschema die Unabhängigkeit der Prüf- und Zertifizierungsstelle garantiert und somit maximale Transparenz bei der Erfüllung der zugesicherten funktionalen und sicherheitstechnischen Leistungen absichert.

Ganzheitliche Informationssicherheit als Erfolgsmodell – Maßstäbe für Informationssicherheitsmanagement

Isabel Münch, Referatsleiterin IT-Grundschutz, BSI

2009 feierte der IT-Grundschutz sein 15-jähriges Bestehen. Die IT-Grundschutz-Methodik wurde 1994 vom BSI mit dem Ziel eingeführt, Behörden und Unternehmen den Aufbau und Betrieb einer sicheren IT-Landschaft zu erleichtern. Seitdem haben sich die Geschäftsprozesse, die Informationstechnik sowie viele andere Rahmenbedingungen immer wieder massiv verändert. Wie der aktuelle Lagebericht des BSI zur IT-Sicherheit 2009 belegt, ist das Bedrohungsniveau unverändert hoch. Gleichzeitig werden IT-Anwender jedoch mit immer neuen Formen von Schadsoftware konfrontiert. Bedrohungen aus der realen Welt finden sich heute auch im Internet wieder. Ein DDoS-Angriff, der die Verfügbarkeit eines ganzen IT-Systems lahmlegt, ist nichts anderes als Vandalismus mit den Mitteln der Informationstechnologie. Trotzdem sind sich die Nutzer der Gefahren oft nicht bewusst, denn die Bedrohungen sind meist schwer greifbar, und Angriffe verlaufen nahezu unsichtbar. Verwaltungen und Unternehmen müssen daher weiter dafür sensibilisiert werden, wie sie sich richtig schützen können.

Mit IT-Grundschutz die zunehmende Komplexität der IT beherrschbar machen

Die immer größer werdende Komplexität der IT-Systeme erschwert es Unternehmen und Verwaltungen, geeignete Maßnahmen zur Erhöhung der Informationssicherheit zu ergreifen. Der IT-Grundschutz hilft, diese Komplexität der Thematik durch systematisches und nachhaltiges Vorgehen beherrschbar zu machen. Dieser Ansatz hat sich in den vergangenen 15 Jahren bewährt und die IT-Grundschutz-Methodik zu einem anerkannten Standard für Informationssicherheit gemacht. IT-Grundschutz strukturiert das komplexe Thema IT-Sicherheit und macht es handhabbar. 1994 erschien die erste Ausgabe des IT-Grundschutzhandbuchs mit einem Umfang von knapp 150 Seiten im Eigendruck. Heute gibt es auf der IT-Grundschutz-Webseite Informationen und Hilfsmittel für die verschiedenen Zielgruppen. Das Angebot umfasst mittlerweile vier BSI-Standards, die IT-Grundschutz-Kataloge sowie zahlreiche Instrumente zur Umsetzung. Damit bietet das BSI eine fundierte Methodik inklusive unterstützendem Material, um die Informationssicherheit einer Institution einzuschätzen und zu erkennen, welche Maßnahmen erforderlich sind und wie sie umgesetzt werden können. Zahlreiche Behörden und Unternehmen nutzen IT-Grundschutz zur effizienten Umsetzung ihrer Sicherheitskonzepte und auch viel gefragte Management-Ansätze wie GRC (Governance, Risk and Compliance) können abgedeckt werden.

Rund um den IT-Grundschutz sind inzwischen sogar neue Tätigkeitsfelder entstanden: Auditoren für die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, IT-Grundschutz-Berater, IT-Grundschutz-Revisoren oder die IT-Sicherheitsbeauftragten des Bundes, bei denen IT-Grundschutz zur Basisausbildung gehört. Als Best-Practice-Modell wird IT-Grundschutz auch in zahlreichen anderen europäischen Ländern wie z. B. Estland und Schweden genutzt. Dafür stehen mittlerweile viele Materialien auf Englisch und in weiteren Sprachen zur Verfügung.

Die IT-Welt hat sich in den vergangenen 15 Jahren radikal gewandelt, die IT-Grundschutz-Idee funktioniert noch immer. Grundlage für das Erfolgsmodell ist eine ganzheitliche Betrachtung der Informationssicherheit, aber auch die kontinuierliche Anpassung an neue Herausforderungen und Änderungen in Geschäftsmodellen und IT-Umgebungen. Daher wurden und werden immer wieder neue Themengebiete aufgegriffen und in die vorhandenen Werke integriert. So ist Anfang 2009 der BSI-Standard 100-4 zum Thema Notfallmanagement veröffentlicht worden. Im Dezember 2009 ist die elfte Ergänzungslieferung der IT-Grundschutz-Kataloge erschienen. Sie umfasst eine Reihe von neuen Texten und Überarbeitungen, um der sich stetig ändernden Bedrohungslage gerecht zu werden. Die elfte Ergänzungslieferung enthält neue Bausteine zum Löschen und Vernichten von Daten, zu Microsoft Vista und zur freien Software Samba sowie Überarbeitungen vorhandener Bausteine wie dem Baustein B 1.3 zum Notfallmanagement und dem Baustein B 1.6 zum Schutz vor Schadprogrammen.

Unterstützung durch das IT-Grundschutz-Tool

Mit dem Grundschutz-Tool (GSTOOL) stellt das BSI seit 1998 eine regelmäßig aktualisierte und ergonomisch handhabbare Software bereit, die den Anwender bei Erstellung, Verwaltung und Fortschreibung von Sicherheitskonzepten entsprechend dem IT-Grundschutz effizient unterstützt. Der Entwicklung des IT-Grundschutzes und den Wünschen der Anwender folgend steht inzwischen das GSTOOL in der Version 4.7 zur Verfügung.

Roland Schubert, Mitarbeiter des IT-Sicherheitsteams, SIGNAL IDUNA Gruppe

„Wir haben in unserem Konzern jetzt die ersten praktischen Erfahrungen dieses Tools im Zuge des BSI-Grundschutzes machen können, und ich muss sagen: Hochachtung. Alle Aspekte der Benutzerführung wurden sinnvoll abgedeckt, die Verständlichkeit ist gegeben, den Anforderungen der Modellierung und der Reporterzeugung wurde Rechnung getragen. Der Grundgedanke der Objektorientierung mit seinen Vererbungsmechanismen findet hier einen sinnvollen Niederschlag. Wenn man das System einmal verstanden hat, ist es einfach und effizient einzusetzen. Hier spürt man, dass nicht nur ein ‚schönes optisches Tool' entwickelt wurde, sondern, dass sich die Entwickler auch mit der Zielfunktionalität aus Sicht der Endanwender auseinander gesetzt haben."

Um die Benutzerfreundlichkeit des GSTOOLs zu verbessern und den Nutzen für die Anwender zu optimieren, wird es fortlaufend überarbeitet und an den aktuellen technischen Stand angepasst. In Kürze wird das BSI eine moderne und über ein Web-Frontend bedienbare Anwendung mit verbesserter Benutzeroberfläche zur Verfügung stellen. Zudem wird das GSTOOL komplett betriebssystemunabhängig einsetzbar sein. Neben diversen funktionalen Erweiterungen werden – insbesondere zur Unterstützung größerer Institutionen – ein Gruppierungsmanager, eine Schnittstelle zu Verzeichnisdiensten und eine offene Schnittstelle für den Zugriff aus externen Anwendungen heraus geschaffen.

ISO 27001-Zertifizierung auf Basis von IT-Grundschutz

IT-Grundschutz hat sich die ISO-Reihe 2700x zum Vorbild genommen und dafür eine handhabbare und technisch fundierte Darstellung und Handlungsanleitung bereit gestellt. Damit entspricht IT-Grundschutz internationalen Anforderungen und ist international verwendbar.

Eine BSI-Zertifizierung umfasst sowohl eine Prüfung des Managementsystems zur Informationssicherheit (ISMS) als auch der konkreten Sicherheitsmaßnahmen auf Basis von IT-Grundschutz. Hervorzuheben ist, dass das Zertifikat immer eine offizielle ISO-Zertifizierung nach ISO 27001 beinhaltet, aber aufgrund der zusätzlich geprüften technischen Aspekte wesentlich aussagekräftiger als eine reine ISO-Zertifizierung ist. Vom BSI lizenzierte Auditoren erfüllen alle Anforderungen, die die ISO an Auditoren für ein ISMS stellt.

Weitere Hilfsmittel zum IT-Grundschutz

Regelmäßig veröffentlicht das BSI weitere Hilfsmittel wie die IT-Grundschutz-Profile. In den IT-Grundschutz-Profilen wird anhand von Beispiel-Institutionen der Prozess erläutert, wie ein Sicherheitskonzept zu planen, umzusetzen und zu pflegen ist. Anfang 2009 ist das IT-Grundschutz-Profil für das produzierende Gewerbe erschienen, in dem für ein kleines produzierendes Unternehmen gezeigt wird, wie sich IT-Grundschutz auch für diesen Bereich anwenden lässt. Hilfsmittel entstehen durch Fragen und Anregungen der IT-Grundschutz-Anwender. Zu den Aufgaben und zur Rolle des IT-Sicherheitsbeauftragten gibt es immer wieder Fragen. Jede Behörde und jedes Unternehmen sollte einen IT-Sicherheitsbeauftragten ernannt haben. Für deutsche Bundesbehörden ist dies verbindlich vorgeschrieben. Daher konkretisiert das „Muster für die Bestellung eines IT-Sicherheitsbeauftragten“ die im BSI Standard 100-2 definierte Rolle.

Auch Spezialthemen wie die Sicherheit von Vermittlungsverfahren – etwa Datenübertragungsmöglichkeiten über DWDM (Dense Wavelength Division Multiplexing) und bei MPLS (Multiprotocol Label Switching) – finden sich unter den Hilfsmitteln zum IT-Grundschutz. Mitte 2009 wurde jeweils eine Kurzstudie zu den Themen DWDM und MPLS erstellt. Die Studien bieten einen Überblick über die spezifischen Gefährdungen und Sicherheitsmaßnahmen beim Einsatz dieser Technologien.

Dr. Günter Steinau,
Geschäftsführer, BEIT Systemhaus GmbH

„Die Anforderungen der internationalen Norm ISO 27001 sind überwiegend allgemein gehalten. Sie beschreibt zwar, was getan werden soll, sagt aber vergleichsweise wenig darüber, wie die Anforderungen erfüllt werden können. Wir erkannten daher sehr früh den Wert des BSI-Grundschutz-Modells, um unseren kontinuierlichen ISMS-Prozess mit Leben zu füllen. Wir nutzen dessen reichhaltigen Fundus an Werkzeugen, Konzepten, Richtlinien und Musterlösungen, um unseren ISMS-Prozess zu strukturieren und uns bei der kontinuierlichen Aufrechterhaltung und Verbesserung unserer Informationssicherheit daran zu orientieren.“

Dr. Johann Bizer, Vorstand Lösungen, Dataport

„Datensicherheit setzt einen strukturierten IT-Betrieb voraus. Strukturieren kann man aber nur, wenn man seinen IT-Betrieb auch konzeptioniert und die erforderlichen Prozesse aufgesetzt hat. Wir haben in den letzten fünf Jahren vier unterschiedliche Standortkulturen mit ihren jeweiligen Vorverständnissen in eine Sicherheitskultur integriert. Das ist eine beachtliche Leistung. Gelungen ist dies, weil wir uns mit IT-Grundschutz an einem anerkannten Sicherheitsstandard orientieren und die Sicherheitsprozesse in unsere ITIL-Prozesskultur integrieren. Das ist eine permanente Anforderung und Leistung, die ohne die in hohem Maße engagierten Mitarbeiterinnen und Mitarbeiter von Dataport nicht zu bewältigen wäre.“

Standard zur Hochverfügbarkeit kritischer Geschäftsprozesse

Mit dem Hochverfügbarkeitskompendium „HV-Kompendium“, welches das BSI auf der CeBIT 2009 erstmals präsentierte, sellt das BSI einen neuen Standard zur Beschreibung und Gewährleistung der Hochverfügbarkeit für kritische Geschäftsprozesse vor. Für die Konzeption hoch verfügbarer Architekturen wurden überarbeitete Maßnahmenkataloge online zur Verfügung gestellt, bei denen der Aspekt der Verfügbarkeit durch Aspekte des IT-Betriebs und der IT-Organisation erweitert wurde. Das BSI wendet sich damit an die Betreiber von IT-Systemen, die IT-Dienste für kritische Geschäftsprozesse anbieten. Das HV-Kompendium liefert umfassende Empfehlungen zur Absicherung der Verfügbarkeit in System- und Netzarchitekturen. Über eine rein technische Sichtweise hinaus werden in einer ganzheitlichen Betrachtung Empfehlungen zur Verfügbarkeitssicherung von Anwendungen und Diensten getroffen. Diese Maßnahmenbeschreibungen werden in den Maßnahmenkatalogen des HV-Kompendiums zusammenfassend und kompakt dargestellt. Mit der geplanten Fortschreibung des HV-Kompendiums sollen Bewertungs- und Steuerungsinstrumente aufgenommen werden. Dabei bilden die Prozessorientierung der IT-Organisation sowie Instrumente für die Bewertung des Architekturpotenzials und Steuerung der IT-Prozesse die zentralen Inhalte. Das Kompendium umfasst bislang drei Bände und steht in der neuesten Version auf der Internetseite des BSI als Download zur Verfügung.

De-Mail – So einfach wie E-Mail und so sicher wie die Papierpost

Dr. Astrid Schumacher,
Projektleiterin De-Mail im BSI

De-Mail – eine Infrastruktur für sichere Kommunikation

Das Projekt „De-Mail" – entstanden aus dem Projekt „Bürgerportal" – zielt auf die Einrichtung einer sicheren Kommunikationsinfrastruktur für Bürger, Unternehmen und Verwaltung und soll ohne viel Aufwand von allen genutzt werden können. Es ist ein wesentlicher Bestandteil des Programms E-Government 2.0 des Bundes und gehört zu den vier Handlungsfeldern, auf denen der Bund das E-Government vorantreibt, um die Verwaltung und den Standort Deutschland zu modernisieren. Das BSI ist maßgeblich an der konzeptionellen Gestaltung beteiligt.

Vertrauen durch Sicherheit und Zertifizierung

Entscheidend für den Erfolg von De-Mail ist, dass die Anbieter der Dienste die Sicherheit, die sie versprechen, auch tatsächlich gewährleisten. Grundlage dafür ist insbesondere ein geeignetes IT-Rahmen-Sicherheitskonzept, das alles, was für die Infrastruktur relevant ist, mit einbezieht. Für die Akkreditierung als De-Mail-Diensteanbieter sind auf dieser Grundlage Sicherheitszertifikate für die Bereiche Sicherheit, Interoperabilität und Funktionalität zu erbringen, die nach den bewährten Zertifizierungsverfahren beim BSI erlangt werden können. Ziel ist es, potentiellen Anbietern das Erreichen eines angemessenen Sicherheitsniveaus zu ermöglichen, gleichzeitig aber genügend Spielraum für eine individuelle Gestaltung der Einsatzumgebung zu lassen. Das BSI ist für das Sicherheits- sowie Zertifizierungskonzept verantwortlich und bringt so seine Kernkompetenzen in das Projekt ein. Damit leistet es einen wesentlichen Beitrag zur Umsetzung der Vision einer sicheren und verlässlichen Infrastruktur für eine vertrauliche und verbindliche elektronische Kommunikation.

Staat und Wirtschaft definieren gemeinsam den Rahmen – die Wirtschaft setzt De-Mail um

Die grundlegenden Anforderungen an Sicherheit, Funktionalität und Interoperabilität wurden vom Bund gemeinsam mit den künftigen De-Mail-Providern erarbeitet und in Form von Technischen Richtlinien beim BSI festgeschrieben. Die Einhaltung dieser Richtlinien durch die De-Mail-Provider wird in einem gesetzlich geregelten Akkreditierungs- und Zertifizierungsverfahren geprüft.

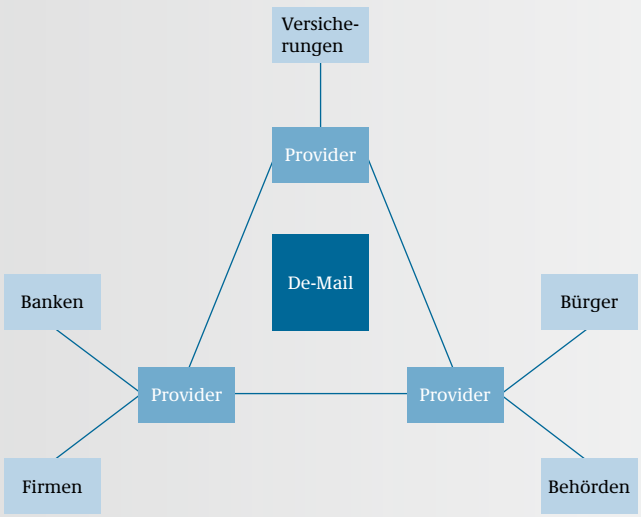
Das Angebot von De-Mail-Diensten erfolgt so durch miteinander im Wettbewerb stehende Unternehmen, die sich auf Grundlage des einheitlichen Rahmens durch Zusatzangebote voneinander abgrenzen können. De-Mail ist damit die Basis für eine flächendeckende und gleichzeitig wettbewerbsfreundliche Infrastruktur – zugunsten einer sicheren elektronischen Kommunikation.

Startschuss in Friedrichshafen

Mit den ersten De-Mail-Pilot-Providern GMX, T-Home, T-Systems und WEB.DE wurde De-Mail inzwischen so weit fertiggestellt, dass die Pilotierung am 9. Oktober 2009 in Friedrichshafen am Bodensee beginnen konnte (www.fn.de-mail.de). An den Tests beteiligen sich u.a. die Firmen AWD, Citibank, CosmosDirekt, EADS, Gothaer, HUK24, LVM, Sparkasse Bodensee, Volksbank Friedrichshafen, ZF sowie die Stadt Friedrichshafen, die Handwerkskammer Ulm und die IHK Bodensee/ Oberschwaben sowie viele Bürgerinnen und Bürger, die De-Mail während der Pilotierung kostenlos nutzen können. Als Startschuss der Pilotierung wurde die erste De-Mail durch den BITKOM an Herrn Prof. Werner Zorn verschickt, der als einer der Gründungsväter des deutschen Internets vor 25 Jahren auch die erste E-Mail in Deutschland erhalten hatte.

Ziel der Pilotierung, die auf sechs Monate festgelegt ist, ist insbesondere die Erhebung der Nutzerakzeptanz von De-Mail in unterschiedlichen Anwendungsfeldern zwischen Unternehmen und Bürgern sowie mit und innerhalb der Verwaltung. Auftretende Akzeptanzprobleme und Schwierigkeiten in der Bedienerführung sollen früh erkannt und behoben werden, so dass mit Beginn des Wirkbetriebes allen Bürgerinnen und Bürgern, Unternehmen und Behörden eine ausgereifte und anerkannte Plattform zur Verfügung gestellt werden kann.

De-Mail-Struktur



Das sagen Anbieter und Nutzer:

„Es besteht großer Bedarf an einer sicheren und vertraulichen elektronischen Kommunikation zwischen Unternehmen, Verwaltungen und auch Privatpersonen im Internet. Durch De-Mail sehen wir die Chance, nun endlich in Deutschland einen weit verbreiteten Standard zu schaffen, der diesen Ansprüchen gerecht wird. Deshalb unterstützen die Deutsche Telekom und T-Systems das Bundesinnenministerium und das BSI mit großem Engagement dabei, die Funktionen und Architektur der De-Mail zu konzipieren und die Lösung benutzerfreundlich zu gestalten. Hierbei war und ist das BSI ein strenger, aber gleichzeitig kooperativer und deshalb idealer Sparringpartner. Unser Ziel ist es darüber hinaus, einer der ersten Provider für De-Mail zu werden."

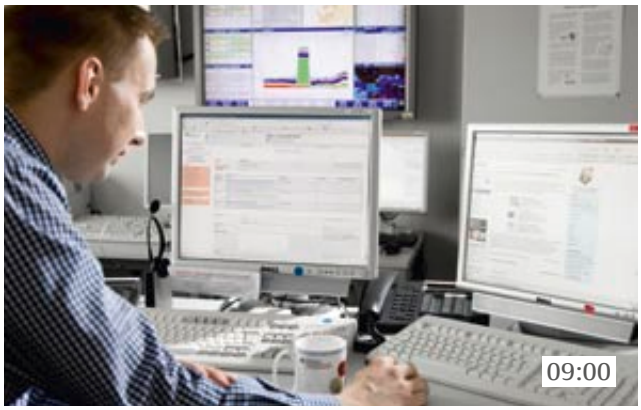
Gert Metternich, T-Systems International

„Als größte E-Mail-Provider in Deutschland begrüßen GMX, WEB.DE und 1&1 das Projekt De-Mail. Kommunikation, die eine hohe, standardisierte Rechtssicherheit und Rechtsverbindlichkeit erfordert und daher aktuell in papierbasierter Form erfolgt, benötigt ein entsprechendes digitales Zusatzangebot. GMX, WEB.DE und 1&1 begleiten das Projekt seit Beginn, nehmen an der Pilotierung der De-Mail in Friedrichshafen teil, und planen – bei entsprechendem Erfolg des Piloten – De-Mail-Anbieter für Bürgerinnen und Bürger, Wirtschaft sowie die öffentliche Verwaltung zu werden. Um als De-Mail-Provider tätig werden zu dürfen, müssen künftig die Umsetzung technischer und organisatorischer Maßnahmen sowie der Interoperabilität der De-Mail Dienste im Rahmen einer Akkreditierung durch das Bundesamt für Sicherheit in der Informationstechnik nachgewiesen werden. Wir freuen uns, dass die zu implementierenden Prozesse eng mit der Wirtschaft abgestimmt wurden, um ein hochsicheres, schnelles und kosteneffizientes Akkreditierungsverfahren zu gewährleisten."

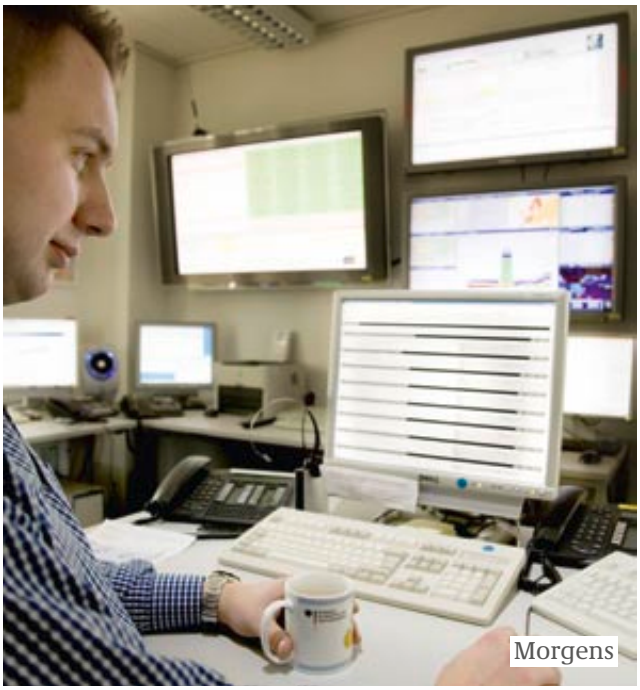
Michael d'Aguiar, 1&1 Internet Portale (GMX und WEB.DE)

„Die Versicherungswirtschaft bietet ihren Kunden und Geschäftspartnern umfassende Informationsangebote und Möglichkeiten zum Datenaustausch in elektronischer Form. Soll jedoch heute ein Geschäftsprozess als rechtlich verbindlich Bestand haben, müssen die elektronischen Unterlagen ausgedruckt, versandt und im nächsten Schritt z. B. vom Kunden oder Partner ausgefüllt, unterschrieben und zurückgeschickt werden. Mit der geplanten De-Mail werden die – aus Sicht der Versicherungswirtschaft dringend erforderlichen – standardisierten Rahmenbedingungen und IT-Infrastrukturen definiert, auf deren Basis dann IT-Dienstleister und Provider sichere und verbindliche E-Mail-Services anbieten können. Diese sichere und rechtsverbindliche E-Mail-Kommunikation mit Kunden und Geschäftspartnern sowie der Verwaltung ist für die Versicherungsunternehmen von zentraler Bedeutung. Informationen der Versicherungswirtschaft an ihre Kommunikationspartner können dann schnell und medienbruchfrei übermittelt sowie elektronisch weiterverarbeitet werden. Entscheidend ist dabei, dass diese Infrastrukturen auf überprüfbaren Standards aufbauen und vom BSI als zuständiger Institution begleitet werden."

Gesamtverband der deutschen Versicherungswirtschaft e.V.


09:00


10:00


Morgens

„Die Kommerzialisierung der kriminellen, existenzbedrohenden Angriffe schreitet immer stärker voran.“

Stefan Ritter, Leiter des IT-Lagezentrums im BSI


11:00


Mittags

Sicherheit für die Cyberwelt

Immer im Einsatz: Ein Tag im nationalen IT-Lage- und Analysezentrum

365 Tage im Jahr ist das nationale IT-Lage- und Analysezentrum im BSI besetzt und erreichbar: Es hat den Auftrag, jederzeit ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland zur Verfügung stellen zu können. Dadurch lassen sich Handlungsbedarf und -optionen bei IT-Sicherheitsvorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft schnell und kompetent einschätzen.

Morgens: Übernahme des Dienstes im Lagezentrum
Der Lagebeobachter prüft die Rechner und verschiedenen Beobachtungssysteme im Lagezentrum und hält Rücksprache mit dem Kollegen, der während der Nacht in Bereitschaft war. Anschließend wertet er die unkritischen Alarmierungen der Nacht aus. Konzentriert sichtet er die Medienlage.

09:00 Uhr: Lagebeobachtung
Punkt für Punkt sichtet der Lagebeobachter während seines Dienstes anhand einer umfangreichen webbasierten Checkliste mit Arbeitsanweisungen mehr als 60 nationale und internationale Informationsquellen. Dabei geht er verschiedenste Fachquellen und -portale durch und filtert alle relevanten Meldungen. Besonders interessante Sachverhalte werden nachrecherchiert, dokumentiert und sofort an die zuständigen Kollegen weitergeleitet.

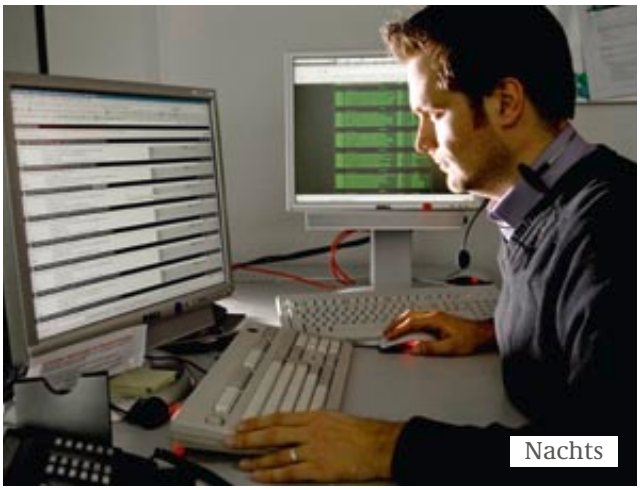
10:00 Beobachtung der technischen Sensoren
Parallel zur Quellensichtung hat der Lagebeobachter immer einen Blick auf die Anzeigen der verschiedenen technischen Sensoren in und außerhalb der Regierungsnetze. Hierzu zählen E-Mail- und Virenaufkommen, Flowdaten und verschiedenste Messdaten. Bei Abweichungen vom Regelverhalten, insbesondere beim Überschreiten von Schwellwerten, alarmiert er die jeweiligen Experten, die dann umgehend den Sachverhalt prüfen und geeignete Maßnahmen ergreifen.

11:00 Redaktionssitzung zum IT-Sicherheitslagebericht
Quartalsweise gibt das Lagezentrum eine Zusammenfassung der IT-Sicherheitslage heraus. Dabei werden für die interessierte Öffentlichkeit Angriffe und Sicherheitsereignisse, Bedrohungen und Gefahren sowie Trends und Statistiken dargestellt, erklärt und kommentiert. Die täglichen Lagebeobachtungen bilden dafür die zentrale Grundlage. Hinzu kommen Erkenntnisse aus weiteren nicht öffentlich zugänglichen Quellen des BSI.

Mittags: Mittagslage
Der Lagebeobachter stellt den Vertretern der Fachreferate bei der mittäglichen Zusammenkunft die Ergebnisse seiner Lagefeststellung vor. Dabei werden die Sachverhalte von den Spezialisten ergänzt, hinterfragt und analysiert. Darüber hinaus sind aktuelle Beiträge aus den Fachreferaten und Neuigkeiten aus Besprechungen, von Veranstaltungen und Kongressen Thema dieser Runde.

„Unser Lagezentrum beobachtet und analysiert die tägliche Sicherheitslage und warnt bei kritischen Vorkommnissen.“

Stefan Ritter, Leiter des IT-Lagezentrums im BSI



13:30 Sondersitzung aufgrund eines IT-Sicherheitsvorfalls
Eine Behörde hat einen schweren IT-Sicherheitsvorfall gemeldet. Der Vorfall wird zielgerichtet erfasst und weitere Fakten beim betroffenen Amt erfragt. Da das Geschehen dem Lagebeobachter kritisch erscheint, wird ad hoc eine Besprechung zur Beurteilung des Sachverhalts einberufen. Der Lagebeobachter stellt sämtliche bekannten Fakten vor – die verschiedenen hinzugezogenen Experten aus den Fachreferaten diskutieren und bewerten die Situation. Im nächsten Schritt werden Lösungsmöglichkeiten und Maßnahmen erarbeitet und der Behörde vorgeschlagen.

14:30 Warnmeldung
Der IT-Sicherheitsvorfall wurde weiter untersucht – und offenbart eine systematische Schwachstelle in einem in der Bundesverwaltung eingesetzten Produkt. Jetzt heißt es schnell informieren und vorbeugen: Das Lagezentrum verfasst zusammen mit dem Computer-Notfallteam der Bundesverwaltung CERT-Bund eine technische Warnmeldung, die sofort über den Warn- und Informationsdienst (https://www.cert-bund.de) und über BürgerCERT (www.buerger-cert.de) als Extraausgabe des Newsletters verteilt wird.

15:00 Warnung der Betreiber Kritischer Infrastrukturen
Der Sicherheitsvorfall beschäftigt das Lagezentrum weiter: Die entdeckte Schwachstelle betrifft offenbar auch Systeme, die bei den Betreibern Kritischer Infrastrukturen (KRITIS) eingesetzt werden. Das Lagezentrum beschließt daher nach kurzer Rücksprache mit den für Kritische Infrastrukturen zuständigen BSI-Kollegen, auch eine Schwachstellenwarnung an die Partner zu senden. Gemeinsam mit den öffentlichen und privatwirtschaftlichen Betreibern der Kritischen Infrastrukturen in Deutschland wurde in den vergangenen Jahren ein entsprechendes Alarmierungsverfahren etabliert. Mittels bei den Betreibern eigens eingerichteter Notfallkontakte werden die entsprechenden Stellen in den Unternehmen zeitnah über die Schwachstelle informiert.

KRITIS

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit hoher Bedeutung für das staatliche Gemeinwesen. Bei Ausfall oder Beeinträchtigung würden erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten.

16:00 Übungsvorbereitung
Die heute notwendigen Warnungen haben gezeigt, wie wichtig etablierte Kontakte und eingespielte Mechanismen im Krisenfall sind. Daher übt das BSI Lagezentrum mit dem Nationalen IT-Krisenreaktionszentrum die Reaktion auf kleinere und größere Krisen in der Bundesverwaltung und mit Kritischen Infrastrukturen. Die Stabsarbeit und Lagebearbeitung wird durchgespielt, Schwachstellen werden identifiziert und fürs nächste Mal abgestellt. So weiß jeder, was er im Krisenfall zu tun hat. Diese Übungen sind aufwändig und bedürfen guter Vorbereitung, um die Übungsziele zu erreichen.

Nachts: Allzeit bereit
Die Lage wird konstant beobachtet. Auch außerhalb der regulären Dienstzeiten ist das Lagezentrum jederzeit ansprechbar und reaktionsfähig. Eine Fachkraft in Bereitschaft sowie ein Leiter des Einsatzstabes stehen der Bundesverwaltung und den Partnern des BSI rund um die Uhr als Ansprechpartner zur Verfügung. Über unterschiedliche Alarmierungsketten können sie in Notfällen lageabhängig eskalieren – und damit in kurzer Zeit die Reaktionsfähigkeit auf besondere IT-Sicherheitsvorfälle im In- und Ausland sicherstellen.

Sicherheit in der virtuellen Welt:
Analyse und Maßnahmen

Maßnahmen für mehr Sicherheit im Internet

Dr. Lothar Eßer, Referatsleiter Internetsicherheit

Botnetze – Nein, danke!

Das Problem der Botnetze hat in den letzten Jahren massiv zugenommen. Immer mehr Nutzer verfügen über einen Breitband-Internetanschluss. Viele Computer sind rund um die Uhr ans Internet angeschlossen. Die Infektion eines PCs mit Bots erfolgt zum Beispiel unter Ausnutzung bekannter Sicherheitslücken in Diensten und Applikationen. Eine weitere effektive Infektionsmethode ist der Einsatz von Social Engineering, um den Anwender zu einer unbedachten Handlung wie dem Klicken auf bösartige E-Mail-Links bzw. Instant- Messaging-Nachrichten oder die Ausführung von E-Mail-Anhängen zu verleiten. Zudem ist in jüngster Zeit zu beobachten, dass legitime und stark frequentierte Webseiten manipuliert werden, um sie für die Verbreitung von Schadcode zu missbrauchen.

Botnetze sind die größte Gefahr des Internets und bedrohen unter anderem durch Spam, Phishing, Identitäts- oder Datendiebstahl (z. B. von Kennwörtern, PIN oder TAN), Erpressung, Spionage und Distributed Denial of Service-Angriffe (DDoS). Ein Ländervergleich zeigt Deutschland in den Top 5 der mit Botsoftware infizierten Rechner. Benutzer sind mit dem Schutz ihres Rechners zumeist überfordert und merken oftmals nicht einmal, dass er Teil eines Botnetzes ist.

Das BSI unterstützt deshalb mit fachlichem Know-how die Anti-Botnetz-Initiative des eco -Verbands der deutschen Internetwirtschaft e.V. zur Reduzierung

infizierter Rechner. Diese Initiative, die auf dem vierten Nationalen IT-Gipfel der Bundesregierung Ende 2009 in Stuttgart vorgestellt wurde, schafft mehr Sicherheit für den Endnutzer und soll Botnetzen, die in bzw. aus Deutschland agieren, in weiten Teilen nachhaltig den Boden entziehen. Das BSI ist an der Entwicklung und Abstimmung der technischen Konzepte zur Realisierung der Initiative beteiligt.

Als erste Stufe beinhaltet die Initiative die Identifizierung infizierter Rechner in datenschutzkonformer Weise mittels Honeypots und Spamtraps. Die Honeypot-Systeme stehen im Netzbereich des Providers und werden vom infizierten Rechner angegriffen. Die Spamtraps der Provider empfangen die von dort versendeten Spam-E-Mails. In der zweiten Stufe sollen infizierte Nutzer über die Infektion ihres Rechners informiert werden und zugleich bei der Beseitigung der Infektion unterstützt werden. Zusätzliche Hilfestellungen sind in Form von Informationen auf einer zentralen Webseite und einer telefonischen Beratung verfügbar.

„Mit der Botnetz-Initiative möchten wir Deutschland mittelfristig aus den Top 10 der Länder, von denen schädliche Online-Aktivitäten ausgehen, herausbringen."

Sven Karge, Fachbereichsleiter Content, eco

Verbesserung der Sicherheit des Domain Name Systems (DNS)

Im Jahr 2008 wurde in einem für das Internet wichtigen Dienst, dem DNS (Domain Name System), eine Schwachstelle entdeckt, die es Angreifern potenziell ermöglichte, den Internetverkehr von Anwendern umzulenken, Daten mitzulesen und Inhalte zu manipulieren. Um die Schwachstelle zu schließen, mussten Internetanbieter Softwareupdates einspielen. Da aber zwischenzeitlich Hacker die Schwachstelle ausnutzten, warnte das BSI alle Internetnutzerinnen und -nutzer und empfahl, die eigene Internetverbindung mittels eines bereitgestellten Tools auf Anfälligkeit für die DNS-Schwachstelle zu überprüfen. Anwender konnten auf diese Weise herausfinden, ob ihre bestehende Internetverbindung angemessen geschützt ist oder weiterer Handlungsbedarf auf Seiten des Providers besteht. Seitdem hat das BSI noch öfter vor Schwachstellen im DNS gewarnt. Sicherheitslücken konnten bislang nur temporär geschlossen werden.

Um das Domain Name System nachhaltig zu verbessern, empfiehlt das BSI die Einführung der DNS-Erweiterung Domain Name Security Extensions (DNSSEC), bei der die DNS-Einträge mittels kryptografischer Verfahren auf ihre Gültigkeit geprüft werden. Mit DNSSEC können die bekannten Sicherheitslücken geschlossen und Manipulationen erschwert werden.

Initiative für mehr Sicherheit

Zusammen mit eco und DENIC (Deutsches Network Information Center) hat das BSI daher eine Initiative gestartet, deren Ziel die Einführung von DNSSEC für Deutschland ist. Innerhalb einer von DENIC bereitgestellten Testumgebung sollen operative und technische Erfahrungen gesammelt und geprüft werden. Potentielle Auswirkungen auf die Sicherheit und Zuverlässigkeit sollen so vor einer möglichen Einführung evaluiert werden. So hat das BSI etwa Heimrouter auf DNSSEC-Tauglichkeit getestet. Das Ergebnis zeigt, dass viele Hersteller noch nacharbeiten müssen: Von 36 getesteten Geräten ermöglichen nur neun der in den Geräten eingebauten DNS-Proxies die Nutzung der durch DNSSEC eingeführten Sicherheitserweiterungen. Bei den anderen kann DNSSEC nur bei Umgehung der eingebauten DNS-Proxies verwendet werden. Ziel der Initiative ist es folglich, die Produkte und Produkteigenschaften im Hinblick auf die zu implementierenden Sicherheitsfeatures von Anfang an sicherer zu gestalten.

Die BSI-Studie zur „DNSSEC-Tauglichkeit von Internetzugangsroutern" steht auf www.bsi.bund.de zum Download bereit.

Das DNS (Domain Name System)-Protokoll ist für die Umsetzung von Domainnamen wie z. B. „www.buerger-cert.de" in die entsprechende Internetadresse (IP-Adresse) 62.50.36.75 zuständig. Das DNS ist ein hierarchisch organisiertes Verzeichnis. Kann ein Nameserver eine Anfrage nicht selbst beantworten, bezieht er die Antwort vom zuständigen System und hält diese dann in der Regel für die schnelle Bearbeitung zukünftiger Anfragen im Cache vor.

Sichere Internetzugänge bei Bundesbehörden

„Angreifer zeichnen sich durch ein hohes Maß an Professionalität aus“

Die Internetzugänge der Bundesverwaltung sind besonders sensibel und unterliegen höchsten Sicherheitsanforderungen. Schließlich ist einerseits die Verfügbarkeit des Internets und die Online-Erreichbarkeit für eine moderne Verwaltung sehr wichtig, andererseits stellt sie aber auch für Angreifer ein ausgesprochen interessantes Ziel dar. Ihr Schutz muss daher hohe Ansprüche im Hinblick auf die einzusetzende Technik und ihre Verantwortlichen erfüllen.

Ein Gespräch dazu mit Dr. Dirk Häger – Referatsleiter IT-Penetrationszentrum, Abwehr von Internetangriffen im BSI

Welche Bedeutung haben Netze für die Arbeitsfähigkeit der deutschen Verwaltung?

Ob Stromausfälle, Oderhochwasser oder gar terroristische Angriffe – die Kommunikationsfähigkeit der Bundesbehörden untereinander muss in jeder Situation gegeben sein. Nur so lassen sich Hilfsmaßnahmen effektiv koordinieren. Aber auch normales Verwaltungshandeln kann durch Störungen der eingesetzten Informationstechnik bedroht werden, so z. B. wenn Verfahren zur Steuerung des Bundeshaushalts nicht richtig arbeiten oder vertrauliche Informationen aus Beschaffungsvorgängen bekannt werden.

Welche besonderen Herausforderungen stellen sich beim Schutz dieser Netze?

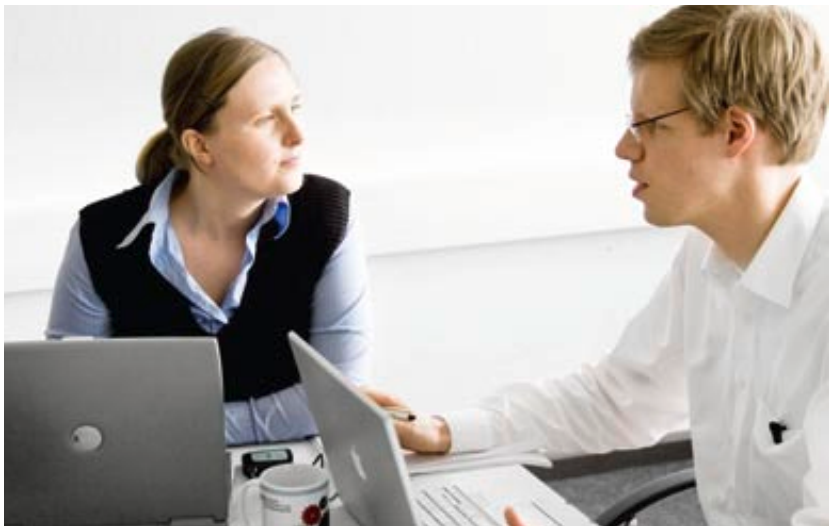
Nicht nur einfache PCs oder Server, wie sie aus dem heimischen Umfeld bekannt sind, werden von Angreifern als Ziele genutzt. Auch die speziellen, teilweise nur im Bereich der öffentlichen Verwaltung eingesetzten IT-Systeme werden durch professionelle Täter analysiert und die schwächsten Punkte ausspioniert. Lücken in Betriebssystemen und Anwendungsprogrammen werden ausgenutzt, Spam-E-Mails versendet, und es wird versucht, die Verfügbarkeit der Dienste durch Botnetze zu behindern. Auch der großflächige Versand von E-Mails mit Hintertüren und die Manipulation von mobilen Endsystemen sind Szenarien, die leider täglich beobachtet werden. Die eingesetzte Informationstechnik im Bereich der öffentlichen Verwaltung ist so vielfältig und komplex, dass ein Schutz der Technik und der Daten mit einfachen Maßnahmen, wie sie beispielsweise für einen privaten PC ausreichen würden, nicht möglich ist. Der Schutz der Kommunikationsinfrastrukturen und insbesondere der übergreifenden Verwaltungsnetze IVBB und IVBV ist daher eine der Hauptaufgaben des BSI. Im Projekt „Netze des Bundes“, das das BSI verantwortet, wird seit 2008 der Übergang dieser beiden zentralen ressortübergreifenden Regierungsnetze in eine leistungsfähige und sichere gemeinsame Netzinfrastruktur geplant und realisiert. Dies geschieht auch im Hinblick auf die zuletzt gestiegene Bedrohung für ganze Staaten – was beispielsweise die Cyber-Attacken auf Estland belegen.

Warum sind die E-Mailzugänge einer Bundesbehörde so sensibel? Und was heißt das in der Praxis?

Wer Offenheit will, muss auch mit den damit einhergehenden Problemen umgehen. Unsere Situation: Auf vielen Webseiten der Bundesverwaltung sind E-Mailadressen angegeben, damit sich Bürger möglichst unkompliziert und direkt an die zuständigen Stellen wenden können. Die Kehrseite der Medaille: Leider werden diese Adressen auch von Spamversendern gesammelt und ausgenutzt. Dies hat zur Folge, dass das Spam-Aufkommen in der Bundesverwaltung enorm hoch ist, nämlich bis zu 99 Prozent aller eingehenden E-Mails ausmacht. Seit 2006 hat sich das Volumen um das 20-fache erhöht. Mit besonderen Techniken ist es dem BSI – bis auf wenige Ausnahmen – aber möglich, diese E-Mails abzuwehren. Die individuelle Belastung der Mitarbeiter durch Spam kann so auf ein Minimum gesenkt werden. Das ist ein echter Erfolg. Ohne diese Schutzmaßnahmen hätte jeder Bundesbedienstete im Schnitt 20.000 E-Mails pro Monat zu bearbeiten. Auch das Schadpotenzial von Spammails in Form von schadhaften Anhängen und Verlinkungen kann so wirkungsvoll eingedämmt werden.

Wodurch zeichnen sich die Angriffe aus?

Durch ein hohes Maß an Professionalität der Angreifer und die Tatsache, dass die Angriffe zunehmend auf ganz spezielle Personenkreise ausgerichtet sind. Schadprogramme werden häufig in ein auf den Empfänger abgestimmtes, unverdächtiges Dokument eingebettet und nur an einen oder einige wenige Empfänger adressiert. Hierbei handelt es sich in der Regel um offiziell aussehende Doku-



mente, deren Schädlichkeit selbst von aufmerksamen Mitarbeitern nicht zu erkennen ist. Aufgrund des individuell programmierten Schadcodes werden solche zielgerichteten Angriffe auch häufig von Virenscannern nicht erkannt.

Welche weiteren Ziele wurden beim Schutz der deutschen Verwaltungsnetze verfolgt?

Wesentliches Designziel beim Aufbau des IVBB/IVBV wie auch bei der Planung des Projekts „Netz des Bundes“ ist die Gewährleistung eines hohen Schutzes auch in besonderen Lagen. Hierzu wurden folgende wesentliche Maßnahmen vom BSI geplant bzw. umgesetzt:

- Redundanz: Alle wesentlichen Komponenten der Netze sind redundant ausgelegt, und zwar nicht nur an einem Ort, sondern bei allen wesentlichen Knotenstandorten in verschiedenen Orten Deutschlands.
- Verschlüsselung: Die Informationen werden verschlüsselt übertragen. Ein Mitlesen oder Verändern ist somit ausgeschlossen.
- Zentrale Übergänge: Obgleich die verschiedenen Behörden an vielen Standorten Deutschlands vertreten sind, wird durch das gemeinsame Netz erreicht, dass nur wenige, zentrale Übergangspunkte genutzt werden. Dadurch können die notwendigen Sicherheitsmaßnahmen professionell, zentral und wirtschaftlich angeboten werden.

Wesentlich ist auch ein einheitliches Sicherheitsmanagement: Das BSI hat als zentraler IT-Sicherheitsdienstleister des Bundes Eckpunkte für die Sicherheit der Netze erarbeitet und bei deren Realisierung mitgewirkt. Das BSI-Gesetz bietet hierzu eine verbesserte Grundlage. Nicht zuletzt bieten wir allen Einrichtungen der Bundesverwaltung Sicherheitssoftware und Dienstleistungen für verschiedene Einsatzzwecke an. Dazu gehören u. a. Viren-Schutzprogramme für Arbeitsplatzrechner, für mobile Geräte wie Handys oder PDAs sowie für Mailserver. Die meisten Programme sind für die Bundesverwaltung kostenlos nutzbar, andere Produkte und Dienstleistungen können über einen Rahmenvertrag bezogen werden. Berechtigte finden alle Informationen im geschützten Bereich für IT-Sicherheitsbeauftragte auf der BSI-Webseite.

Welches Resümee ziehen Sie?

Eine nunmehr über zehnjährige erfolgreiche Abwehr von Angriffen beweist, dass die ergriffenen Maßnahmen wirksam und notwendig sind. In Anbetracht der sich ändernden IT-Landschaft und der Professionalisierung der Angriffe ist aber ein stetiger Verbesserungsprozess notwendig, der mittelfristig – orientiert an dem zunehmenden Bedrohungspotenzial – eine laufende Optimierung der Schutzmaßnahmen erforderlich macht.

IVBB/IVBV

Der Informationsverbund Berlin-Bonn (IVBB) wurde nach einem Beschluss des Bundeskabinetts 1998 als Weiterentwicklung des Bonner Behörden Netz gemeinsam mit der Deutschen Telekom als Kommunikationsplattform der Ministerien und anderer Verfassungsorgane in Betrieb genommen. Bei Inbetriebnahme dieses breitbandigen Netzes wurden die Dienste wie Telefonie, E-Mail oder Videokonferenzen integriert. Die IP-Service-Plattform hat sich zu einem äußerst wichtigen Baustein für die Nutzung des Internet aber auch für das gemeinsame Intranet der Bundesverwaltung entwickelt. 2003 erfolgte mit dem Informationsverbund der Bundesverwaltung (IVBV) ein weiterer Meilenstein in Hinblick auf ein gemeinsames Verwaltungsnetz der Bundesverwaltung. Es ermöglicht auch den Behörden, die nicht über ein eigenes Verwaltungsnetz verfügen, den Zugang zu den ressortübergreifenden Behördenverfahren und -diensten.

Vertrauen in die Cyberwelt: Aufklärung und Sensibilisierung

In unserer Gesellschaft besteht ein zunehmend hoher Bedarf an Informationen über Gefährdungen und Schutzmöglichkeiten von kompetenter, unabhängiger Stelle. Dabei müssen das Informationsangebot und die Dienstleistungen konkret am Bedarf der Zielgruppen in Verwaltung, Wirtschaft und Gesellschaft ausgerichtet werden. Dazu gehört auch, diese nicht zu „überfrachten", sondern durch gezielte Aufbereitung von Materialien zur Wissensvermehrung beizutragen. Nur so kann eine entsprechende Medienkompetenz erreicht und das Vertrauen in die Cyberwelt gestärkt werden.

Der Koalitionsvertrag der Bundesregierung verspricht eine Stärkung der IT-Sicherheit im öffentlichen und nicht-öffentlichen Bereich. Mehr Selbstschutz und die Nutzung sicherer IT-Produkte sind dabei wichtige Zielsetzungen. Auch das BSI wird in diesem Zusammenhang gestärkt.

Im Bereich Aufklärung und Sensibilisierung ist das BSI bereits langjährig tätig. Es stellt Informationsmaterialien und -angebote für Bürgerinnen und Bürger bereit, unter anderem durch das Internetportal www.bsi-fuer-buerger.de, durch den Newsletter „Sicher • Informiert" und auch durch das Service Center, bei dem Nutzerinnen und Nutzer telefonisch Hilfestellung und Informationen erhalten. Durch die Teilnahme an Messen und Informationsveranstaltungen pflegt das BSI den regelmäßigen Austausch mit den unterschiedlichen Zielgruppen, um das Informationsangebot noch stärker an deren aktuelle Bedürfnisse anpassen zu können.

Eine breite IT-Sicherheitskultur zu etablieren – das ist ein anspruchsvolles Ziel, das von einer einzigen Behörde nicht im Alleingang realisiert werden kann. Das BSI setzt bei seiner Kommunikation daher auch verstärkt auf den Austausch und die Zusammenarbeit mit Kooperationspartnern und Multiplikatoren, die sich ebenfalls intensiv mit dem Thema IT-Sicherheit befassen. Dies ermöglicht eine kompetente und umfassende Bearbeitung des Themenfeldes sowie dessen vielfältigen technischen, pädagogischen und psychologischen Aspekten.

Stimmen von Kooperationspartnern

AIRBUS Operations GmbH

„Airbus nutzt das Material des BSI schon seit Jahren, um seine Mitarbeiter mit Informationen und Security Tools zu unterstützen und zu informieren."

Peter Behrens, Koordinator klicksafe, Landeszentrale für Medien und Kommunikation, Ludwigshafen

„Die Initiative klicksafe ist Partner im deutschen Safer Internet Centre der Europäischen Union. Aufgabe von klicksafe ist die Durchführung einer breiten Medienkampagne sowie die Medienkompetenzförderung rund um das Thema Internet bei Eltern, Lehrern, Pädagogen, Kindern und Jugendlichen. Die Initiative ist bundes- und europaweit vernetzt und arbeitet mit Akteuren aus den Bereichen Politik, Wirtschaft, NGOs und Verbraucherschutz zusammen. Aufgrund seiner technischen Expertise im Bereich der Internetsicherheit und seiner Rolle als Cyber-Sicherheitsbehörde stellt das BSI einen wichtigen Partner für klicksafe dar, mit dem wir auch zukünftig im Rahmen der gemeinsamen Zielsetzungen für ein sicheres Internet kooperieren werden."

Prof. Dieter Kempf, Vorstandsvorsitzender „Deutschland sicher im Netz e.V." und Vorstandsvorsitzender DATEV eG

„Mit dem Bundesamt für Sicherheit in der Informationstechnik steht 'Deutschland sicher im Netz e.V.' (DsiN) ein kompetenter Kooperationspartner mit ausgezeichneter Expertise zur Seite. Internet-Sicherheit ist seit Jahren ein zentrales Thema der Arbeit des BSI. Durch diese Zusammenarbeit konnten beide Partner bereits in der Vergangenheit einen wesentlichen Beitrag zur Verbesserung der IT- und Internetsicherheit leisten. DsiN freut sich darauf, auch künftig wesentliche Aktivitäten zur Verbesserung der IT-Sicherheit mit dem BSI als Kooperationspartner aufgreifen zu können."

Kommunizieren – mobil und geschützt

Sichere Mobilkommunikation – neue Herausforderungen durch gesteigerte Funktionalität

Joachim Opfer, Fachbereichsleiter Abhörsicherheit im BSI

Die heutige Arbeitswelt ist gekennzeichnet von einer immer stärkeren Tendenz zum technikgestützten mobilen Arbeiten. Stichwort „Mobiles Büro“: Die moderne Informations- und Kommunikationstechnik ermöglicht auf Dienstreisen oder vom Heimarbeitsplatz aus einen vollen Fernzugriff auf Unternehmensdaten, Kalender und E-Mail-Postfächer. Nicht zuletzt auch als Vorsorge für einen etwaigen Pandemiefall stellt die Arbeit von unterwegs oder von Zuhause eine echte Alternative dar. Eine wichtige Voraussetzung dafür ist die stetige Weiterentwicklung vom Handy zum intelligenten Smartphone, das als „mobiles Büro in der Hosentasche“ dienen kann. Mobile Endgeräte werden längst nicht mehr nur zum Telefonieren und SMS-Versand verwendet, sie bieten inzwischen eine mobile Internetanbindung mit allen wesentlichen Anwendungen und Kommunikationsfunktionen eines vollwertigen mobilen Büros. Darüber hinaus können sie zumeist noch als Digitalkamera, GPS-Navigationsgerät oder Taschencomputer genutzt werden.

„Die zunehmende Verbreitung des mobilen Arbeitens macht die Smartphones besonders attraktiv für Angriffsversuche."

Joachim Opfer

Mobile Arbeitsplätze geschützt und verfügbar halten

Der große Leistungsumfang der Smartphones und die unbestreitbaren Vorteile des mobilen Arbeitens führen dazu, dass sich vielerorts Arbeitsprozesse so verändern, dass effektive Leistung ohne Smartphones gar nicht mehr vorstellbar ist. Damit wird die Gesellschaft zunehmend abhängiger. Abhängig von einer Absicherung der Daten gegen Einblicke Dritter sowie von der ständigen Verfügbarkeit und dem zuverlässigen Funktionieren des Mobile Office.

Die zunehmende Verbreitung des mobilen Arbeitens macht die Smartphones besonders attraktiv für Angriffsversuche. Dabei sind nicht nur die Endgeräte selbst betroffen, auch die Netzinfrastrukturen können angegriffen werden. Auf diese Weise entsteht ein extrem hohes Schadenspotenzial: Hohe Kosten auf Nutzerseite, der Verlust von Daten, Diensten, Funktionen und Erreichbarkeit und – daraus resultierend – ein negativer Einfluss auf die Produktivität von Unternehmen.

Die moderne Informationsgesellschaft ist also in hohem Maße abhängig von der Sicherheit und der Verfügbarkeit mobiler Arbeitsplätze. Großflächige Angriffe können sogar nachteilige Auswirkungen auf die gesamte Nationalökonomie nach sich ziehen.

Bedrohungen und Schadfunktionen machen vor Mobiltelefonen nicht halt

Um die auf dem PDA gespeicherten Daten bei Verlust oder Diebstahl des Gerätes zu schützen, darf die Bedienung des Gerätes nur nach Authentisierung des Nutzers – z. B. durch Eingabe einer PIN – möglich sein. Zusätzlich sollten die gespeicherten Daten grundsätzlich verschlüsselt abgespeichert werden. Fehlen diese Schutzmechanismen oder sind sie leicht überwindbar, hat der Dieb oder unehrliche Finder vollen Zugriff auf die gespeicherten Daten – und damit möglicherweise sogar Zugang zum stationären Unternehmensnetz oder -rechner. Selbst ohne Zugriff auf das Endgerät können die übertragenen Daten und Gespräche bei unzureichender Ende-zu-Ende-Verschlüsselung auf der Funkstrecke mitgehört werden. Dass die im GSM-Netz eingesetzte Standardverschlüsselung grundsätzlich überwindbar ist, ist theoretisch schon lange bekannt. Dennoch galt die Handyverschlüsselung bis vor kurzem für alltägliche Anwendungen als hinreichend sicher, denn das Brechen der Verschlüsselung erforderte den Einsatz von hochspezialisierten Superrechnern. Mittlerweile wurden die Entschlüsselungsverfahren jedoch so perfektioniert, dass auch versierte Hacker mit schmalem Budget GSM-Mobilfunkverbindungen abhören können.

Hat ein Angreifer physischen Zugriff oder Fernzugriff über eine ungesicherte Funkschnittstelle wie zum Beispiel Bluetooth, kann er das Endgerät mit Schadsoftware infizieren. Genau wie bei stationärer IT ist eine Infektion über das Internet möglich. Eine besonders

tückische Schadfunktion: Mobile Endgeräte lassen sich zur „Wanze in der Westentasche“ umfunktionieren, mit der dann unbemerkt Umgebungsgespräche abgehört werden können. Mobiltelefone lassen sich zudem über das Mobilfunknetz fernsteuern. Der IT-Administrator eines Unternehmens, der Hersteller des Endgerätes oder auch der Netzbetreiber kann die Geräte komfortabel mit regelmäßigen Softwareupdates versorgen oder auch neue Programme installieren. Diese Fähigkeiten können aber auch missbraucht werden, um in das Endgerät „einzubrechen“ und diese mit Schadsoftware zu infizieren. Diese Beispiele zeigen auf, dass mobile Endgeräte vielfältigen Gefahren ausgesetzt sind, denen durch wirksame Schutzmechanismen begegnet werden muss.

Das BSI bietet Lösungen

Das BSI leistet einen wesentlichen Beitrag dazu, mobile Kommunikation sicher zu gestalten. Es ist dafür zuständig, die Bundesverwaltung mit sicheren Geräten auszurüsten bzw. entsprechende Empfehlungen abzugeben. Dafür werden die Entwicklungen auf den Gebieten der Mobilfunkstandards, der Netztechnologie und der mobilen Endgeräte genauestens verfolgt und untersucht. Das BSI führt regelmäßig Studien zur Mobilfunksicherheit durch und veröffentlicht die Ergebnisse in Form von Broschüren auf seiner Website www.bsi.bund.de. Darin werden Gefährdungsszenarios systematisch untersucht und Konzepte für Schutzmechanismen entwickelt.

Darüber hinaus erstellt die Behörde Anforderungen und Sicherheitskonzepte für mobiles Arbeiten. Das Schutzprofil „Mobile Synchronisationsdienste“ dient dabei als Vorlage (= Lastenheft) für die Entwickler sicherer mobiler Lösungen.

Das BSI begleitet die Entwicklung von Sicherheitsprodukten für sicherheitskritische Anwendungen mit dem Ziel, diese für den Einsatz im Geheimschutzbereich zuzulassen. Kernaufgaben dabei sind die Durchführung von Sicherheitsevaluierungen und die Erteilung von Zulassungen, Einsatzempfehlungen und Sicherheitszertifikaten – aktuell zum Beispiel die Zulassung für abhörsichere Handys („Topsec Mobile“ von Rohde & Schwarz und „Secuvoice“ von Secusmart) sowie Einsatzempfehlung für einen sicheren mobilen PDA (SiMKo2 von T-Systems).

Abhörsichere Kommunikation

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 sollen 5000 sichere Mobiltelefone und mindestens 4000 sichere Smartphones in der Bundesverwaltung eingeführt werden. Das BSI ist verantwortlich für diese Maßnahme und koordiniert deren Umsetzung.

SiMKo2 als sicheres Smartphone für die Bundesverwaltung wurde erstmals auf der CeBIT 2009 der Öffentlichkeit vorgestellt. Das BSI hat für dieses Produkt eine Einsatzempfehlung für VS-NfD ausgesprochen. Alle Daten des Nutzers sind auf dem Gerät verschlüsselt abgelegt, die Datenübertragung erfolgt ebenfalls verschlüsselt. Die Software ist so abgesichert, dass ein Angreifer das Gerät weder aus der Ferne noch mit direktem Zugang zum Gerät manipulieren kann bzw. mit dem Gerät verarbeitete Daten mitlesen kann.

Mit Topsec Mobile und Secuvoice stehen nun zwei verschiedene Handys zum verschlüsselten abhörsicheren Telefonieren mit NfD-Zulassung zur Verfügung.

Garantiert abhörsicher!

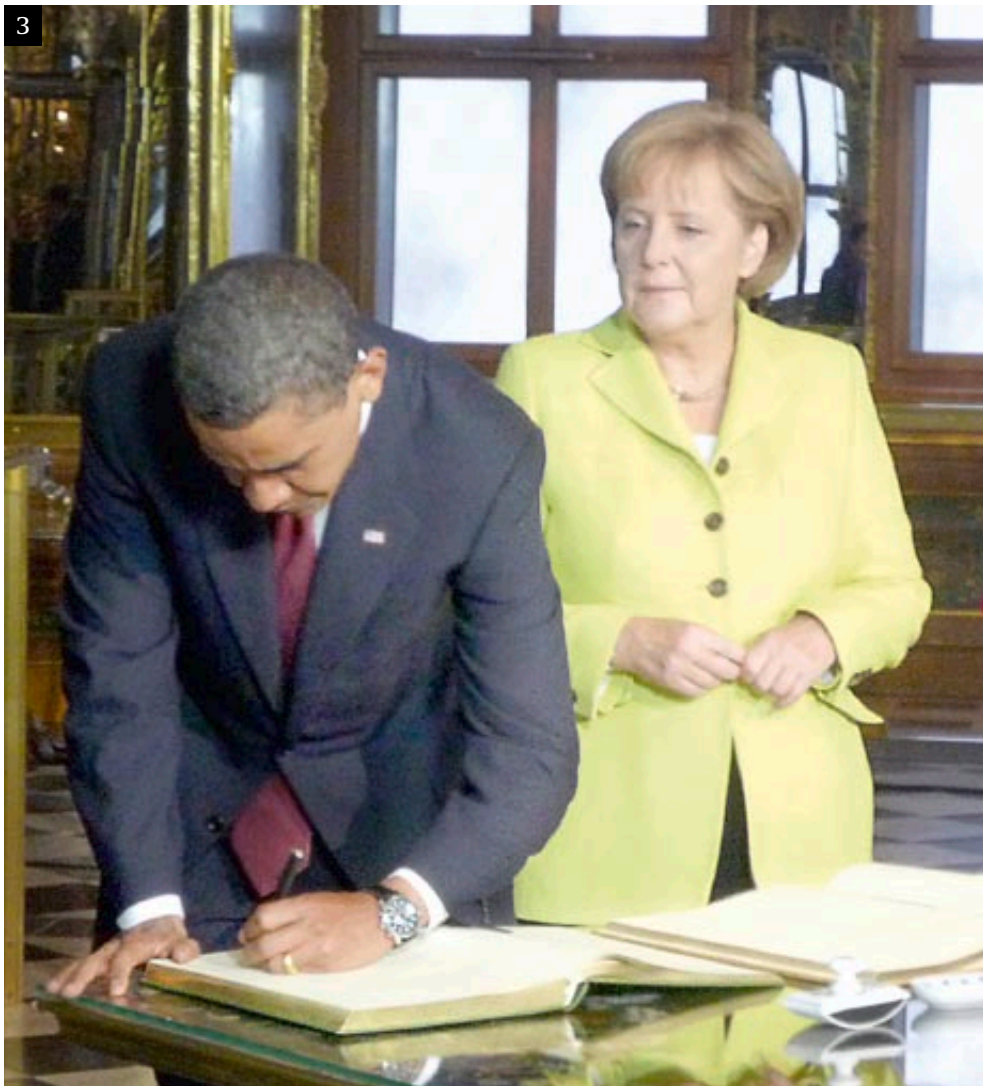
Lauschabwehr beim NATO-Gipfel in Baden-Baden und beim Besuch des US-Präsidenten Obama in Dresden

Das BSI bietet als Dienstleistung Lauschabwehrprüfungen in abhörgefährdeten Behörden an. Darüber hinaus werden aber auch Konferenzen und bilaterale Treffen auf höherer Ebene betreut, bei denen die Gespräche absolut vertraulich bleiben sollen. Aufgabe der Lauschabwehr-Prüftrupps ist, sicher zu stellen, dass keine Abhörgeräte vorhanden sind und dass auch auf anderen Wegen – beispielsweise über manipulierte oder versehentlich aktivierte Mobiltelefone – keine Gesprächsinformationen an Unbefugte gelangen. Herausragende Veranstaltungen im Jahr 2009, um die sich das BSI in dieser Hinsicht gekümmert hat, waren der NATO-Gipfel in Baden-Baden sowie der Besuch des US-Präsidenten Barack Obama in Dresden.

Ob große Konferenz oder Vier-Augen-Gespräch – das BSI sorgt für Vertraulichkeit

So unterschiedlich wie die Anlässe sind, müssen auch die entsprechenden Maßnahmen sein. Das zeigt ein Blick in die verschiedenen Räume und Größenordnungen der hochkarätigen Begegnungen. Während in Baden-Baden die Staats- und Regierungschefs der NATO in großer Runde zusammenkamen, bestand die Aufgabe in Dresden darin, ein Vier-Augen-Gespräch abzusichern. Dieses fand im historischen „Grünen Gewölbe“ statt, das sich im Erdgeschoss des Residenzschlosses hinter vergitterten Fenstern befindet. In dem für das Gespräch vorgesehenen Bronzenzimmer fand noch wenige Tage zuvor normaler Besucherbetrieb statt. Das gesamte Residenzschloss wurde deshalb während der Vorbereitungsarbeiten für die Öffentlichkeit geschlossen, so dass die Lauschabwehrprüfungen durch das BSI beginnen konnten.

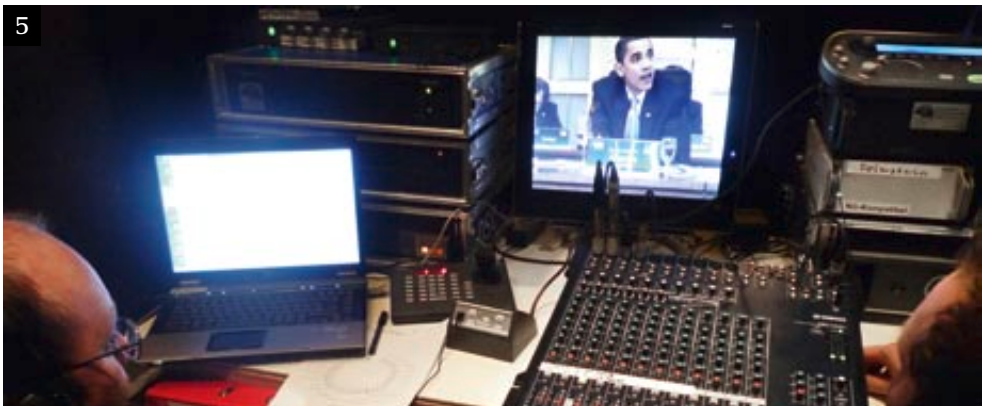
3



4


1


2


5

1. *Die Stühle, auf denen die Bundeskanzlerin und der US-Präsident beim Vier-Augen-Gespräch saßen, wurden einer Röntgenprüfung unterzogen.* **2.** *Im benachbarten Wappenzimmer, das ebenfalls für ein vertrauliches Gespräch mit größerem Teilnehmerkreis vorgesehen war, wurden unter anderem die zahlreichen Wandschränke auf illegale Abhörgeräte untersucht.* **3.** *Unmittelbar vor dem Gespräch trugen sich die Bundeskanzlerin und der US-Präsident in die Goldenen Bücher des Freistaates Sachsen und der Stadt Dresden ein.* **4.** *Während das vertrauliche Gespräch lief, wurde vom BSI-Messfahrzeug aus das Hochfrequenz-Spektrum auf illegale Abhörsender und aktive Mobiltelefone im Besprechungsraum untersucht.* **5.** *Zum NATO-Gipfel in Baden-Baden: Bei Veranstaltungen mit internationalem Teilnehmerkreis wird zum Zweck der Übersetzung und für Tonmitschnitte oft aufwändige Konferenztechnik eingesetzt. Je nach Art der Veranstaltung bzw. des Gesprächs gilt es sicherzustellen, dass keine vertraulichen Gesprächsinformationen von Unbefugten belauscht oder gar mitgeschnitten werden können.*

„Das Pilotprojekt EasyPASS soll Aufschluss über die Sicherheit, die Effizienz und die Praktikabilität einer biometriegestützen Grenzkontrolle geben.“

Markus Nuppeney

Sichere elektronische Identitäten

EasyPASS – Grenzkontrolle einfach und schnell mit dem elektronischen Reisepass

Markus Nuppeney, Projektverantwortlicher Hoheitliche Kontrollsysteme, BSI

Im Jahr 2006 wurden die technischen Spezifikationen für elektronische Reisepässe (ePässe) durch die Internationale Zivilluftfahrt-Organisation (ICAO) verabschiedet. Im Rahmen seiner internationalen Standardisierungsaktivitäten hat das BSI die Entwicklung dieser Spezifikationen maßgeblich beeinflusst – insbesondere die Ausgestaltung der elektronischen Sicherheitsmechanismen für ePässe.

Mittlerweile geben mehr als 60 Länder weltweit ePässe gemäß den ICAO-Standards heraus. Diese Pässe verfügen über einen integrierten, kontaktlos auslesbaren Chip, auf dem die elektronischen Sicherheitsmerkmale abgelegt sowie die personenbezogenen Daten und ein Lichtbild des Passinhabers in elektronischer Form gespeichert sind.

Sicher, effizient und komfortabel
Durch die zunehmende Verbreitung von ePässen ergeben sich nun auch neue Möglichkeiten für die Umsetzung von hoheitlichen Kontrollprozessen. So verspricht beispielsweise die Nutzung von ePässen im Rahmen der Grenzkontrolle diverse Vorteile und Optimierungsmöglichkeiten:

- **Erhöhung der Dokumentensicherheit**
  Durch die im ePass zusätzlich eingebrachten elektronischen Daten und Sicherheitsmerkmale können Dokumentenfälschungen und -missbrauch leicht und zuverlässig erkannt bzw. verhindert werden.
- **Effiziente Dokumentenprüfung**
  Der im ePass integrierte Chip ermöglicht schnelle und automatisierte Prüfverfahren, die etwa zur Durchsatzsteigerung bei Grenzkontrollen nutzbar sind.
- **Komfortable Nutzungsmöglichkeiten**
  Durch den ePass und das damit einhergehende Automatisierungspotenzial werden neue Nutzungsmöglichkeiten, beispielsweise self-service Grenzkontrollprozesse für ePass-Inhaber, ermöglicht.

Pilotprojekt EasyPASS für schnellere Grenzkontrollen
Um dieses Optimierungspotenzial in der Praxis auszuloten und für die realen Grenzkontrollabläufe zu erschließen, führt das BSI gemeinsam mit der Bundespolizei am Flughafen Frankfurt das Pilotprojekt EasyPASS durch. Mit der Konzeptionsphase für das Projekt wurde Ende 2007 begonnen; insbesondere soll dabei die Anwendung der biometrischen Gesichtserkennung auf Basis des ePasses im Rahmen eines (teil-)automatisierten Grenzkontrollprozesses untersucht werden. Ein Kernelement der Konzeption ist das Biometrie-Framework BioMiddle, welches gemeinsam vom BSI und der secunet Security Networks AG speziell für den Einsatz in hoheitlichen Biometrieanwendungen entwickelt wurde. BioMiddle wird bereits in unterschiedlichen hoheitlichen Szenarien erfolgreich eingesetzt und stellt auch im Kontext von EasyPASS die zentrale Integrationsplattform dar. Die modulare und auf internationalen Standards basierende Architektur der Middleware gewährleistet herstellerübergreifende Interoperabilität, so dass die gleichzeitige Nutzung von Hard- und Softwarekomponenten unterschiedlicher Anbieter ermöglicht wird und auch der Austausch von einzelnen Teilkomponenten einfach umzusetzen ist.

Nach der Konzeption erfolgte zeitnah die Entwicklung und Integration der einzelnen Systemkomponenten (Hard- und Software), so dass bereits im Sommer 2009 die

EasyPASS besteht aus den folgenden vier Teilprozessen:

1. **Optische Dokumentenprüfung**
   Bei der optischen Prüfung werden die auf der Datenseite des Passes sichtbaren Daten gescannt. In diesem Zusammenhang werden die optischen Sicherheitsmerkmale des Passes geprüft.
2. **Elektronische Dokumentenprüfung**
   Die elektronische Prüfung erfolgt anhand der auf dem Chip des Reisepasses gespeicherten Daten. Dazu wird dieser Chip nach entsprechender Authentisierung ausgelesen. In diesem Zusammenhang werden die elektronischen Sicherheitsmerkmale des Passes geprüft.
3. **Biometrischer Vergleich**
   Für die biometrische Prüfung erfolgt ein Vergleich des auf dem Chip des ePasses elektronisch gespeicherten Lichtbildes mit einem innerhalb der Personenschleuse aufgenommenen Live-Bild der Person.
4. **Fahndungsabfrage**
   Bei der Fahndungsabfrage wird beim zentralen polizeilichen Informationssystem eine Anfrage über die zu kontrollierende Person gestellt.

Neben den für den eigentlichen Grenzkontrollprozess erforderlichen Prüfungen finden zum Zweck der Evaluation im Hintergrund weitere biometrische Prüfungen mit Algorithmen verschiedener Anbieter statt.

Im Rahmen der technischen Auswertung zu EasyPASS stehen folgende Aspekte im Vordergrund:

- **Biometrische Leistungsfähigkeit**
  Im Rahmen der Bestimmung der biometrischen Leistungsfähigkeit ist insbesondere die Erkennungsgenauigkeit von Interesse – das heißt, wie gut die Reisenden anhand ihres Lichtbildes authentifiziert werden können. Außerdem wird die Qualität der im Prozess verwendeten Lichtbilder und die Anzahl der Aufnahmeversuche bestimmt.

- **Zeitbedarf**
  Wesentliches Ziel in diesem Kontext ist die Bestimmung der Dauer des gesamten automatisierten Kontrollprozesses. Um detaillierte Analysen bezüglich des Zeitbedarfs durchführen und Verbesserungspotenziale ermitteln zu können, wird im Rahmen der Pilotierung der Zeitbedarf für jeden einzelnen Prozessschritt erfasst.

- **Fehlerquellen und -häufigkeit**
  Zur Ermittlung von Fehlerquellen und Fehlerhäufigkeiten erfolgt im Rahmen der Pilotierung eine Fehlerprotokollierung für sämtliche Prozessschritte.

- **Nutzungs- und Dokumentenstatistik**
  Die Nutzungs- und Dokumentenstatistik soll Aufschluss darüber geben, wie hoch die Frequentierung der EasyPASS-Systeme ist und wie die Nutzergruppe bezüglich demografischer Kennzahlen (Alter, Geschlecht etc.) zusammengesetzt ist.

- **Benutzbarkeit und Akzeptanz**
  Neben den technischen Kennzahlen soll im Rahmen der Pilotierung auch eine Einschätzung zur Benutzbarkeit der Systeme und zur Akzeptanz durch die Anwender erfasst werden.

EasyPASS-Passagiersysteme (vier Personenschleusen inklusive Dokumentenleser und intelligentem Kamerasystem) am Flughafen Frankfurt aufgebaut und im Probebetrieb intensiv getestet werden konnten. Im Oktober 2009 erfolgte schließlich die offizielle Eröffnung durch das Bundesministerium des Innern – und damit der Start des Wirkbetriebs.

Weniger Wartezeit für den Reisenden

Die Teilnahme an EasyPASS ist für Bürger der Europäischen Union (EU), des Europäischen Wirtschaftsraums (EWR) und der Schweiz, die über einen ePass verfügen und volljährig sind, auf freiwilliger Basis und ohne vorherige Registrierung möglich. Beim EasyPASS-Verfahren betritt der Reisende nach selbständigem Auflegen seines ePasses auf einen Dokumentenleser eine der vier Personenschleusen. Darin wird sein Gesichtsbild über eine höhenadaptive Kamera aufgenommen und über eine entsprechende Gesichtserkennungssoftware mit dem im Chip des ePasses gespeicherten Lichtbild verglichen. Im Hintergrund erfolgen währenddessen die Echtheitsprüfung des Dokumentes und die polizeilichen Fahndungsmaßnahmen. Führen die Prüfungen zu keiner Beanstandung, öffnet sich die Schleuse und dem Reisenden wird der Grenzübertritt gewährt. Beamte der Bundespolizei überwachen den Prozess und können bei Bedarf eingreifen. Ebenso entscheiden sie anhand der Überprüfungsergebnisse, ob und welche Kontrollfolgemaßnahmen erforderlich sind.

Das Pilotprojekt EasyPASS soll Aufschluss über die Sicherheit, die Effizienz und die Praktikabilität einer biometriegestützten Grenzkontrolle geben. Gleichzeitig sollen die konventionellen Grenzkontrollen unterstützt und eine spürbare Entlastung mit deutlich kürzeren Wartezeiten für die Reisenden erreicht werden.

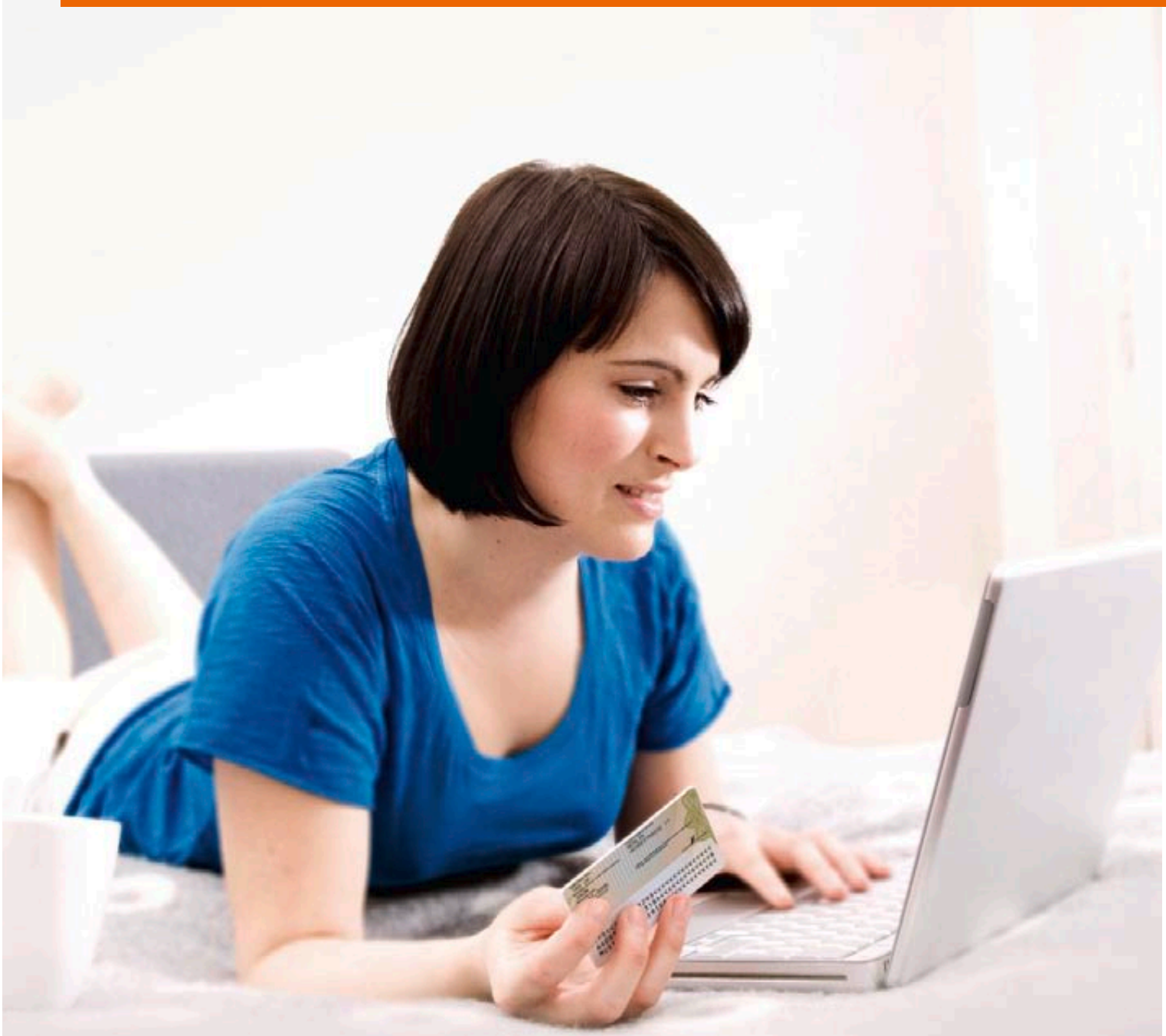
„Eine Erhöhung des Sicherheitsniveaus wird erzielt.“

Drei Fragen an Wolfgang Wurm, Präsident der Bundespolizeidirektion Flughafen Frankfurt/Main

Wie gestaltet sich die Zusammenarbeit von Bundespolizei und BSI?
EasyPASS ist ein Gemeinschaftsprojekt der Bundespolizei und des BSI im Auftrag des BMI. Im Zusammenhang mit der elektronischen Prüfung von hoheitlichen Dokumenten und dem Einsatz von biometrischen Systemen hat sich das BSI erneut als kompetenter und verlässlicher Partner der Bundespolizei erwiesen. Die konstruktive Zusammenarbeit hat maßgeblichen Anteil am erfolgreichen Start des Projektes.

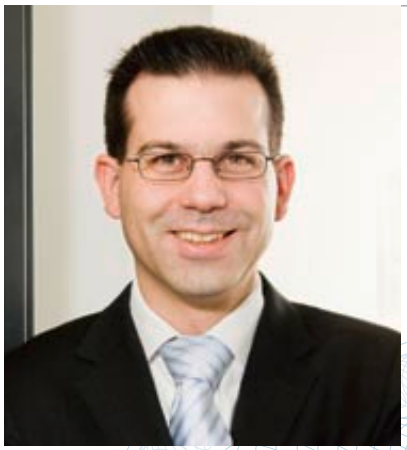
Welchen Nutzen bringt EasyPASS für die grenzpolizeiliche Praxis? Hat sich EasyPASS bereits bewährt?
Mit der Einführung der elektronischen Reisepässe wurden über den eingebrachten Chip weitere Sicherheitsmerkmale in das Reisedokument aufgenommen. EasyPASS als ein (teil-)automatisiertes Grenzkontrollsystem ist u. a. in der Lage, diese Sicherheitsmerkmale schnell und sicher zu überprüfen und damit eine Aussage zur Echtheit des Grenzübertrittspapiers zu treffen. Darüber hinaus erfolgt – automatisiert – eine Identitätsfeststellung sowie eine fahndungsmäßige Überprüfung. Die steigenden Passagierzahlen an deutschen Flughäfen erfordern eine Weiterentwicklung des bisherigen konventionellen Grenzkontrollverfahrens hin zu sicheren, nutzerfreundlichen und wirtschaftlichen Technologien. Mit einer durchschnittlichen Kontrolldauer von ca. 15 Sekunden gewährleistet EasyPASS bereits im Pilotbetrieb einen erfreulich hohen Passagierdurchsatz. Durch die implementierten Prüfverfahren wird gleichzeitig eine Erhöhung des Sicherheitsniveaus erzielt. Durch diese Funktionalität, aber auch durch den geringen Flächenverbrauch kann bisher benötigtes Kontrollpersonal reduziert und zielgerichtet in anderen Bereichen, zum Beispiel in der Grenzfahndung, eingesetzt werden. Reisende hingegen profitieren von spürbar kürzeren Wartezeiten an den Grenzkontrollstellen. Die stabile Funktionalität und die sehr geringe Rückweisungsquote lässt bereits zum jetzigen Zeitpunkt ein positives Ergebnis des Testlaufes erwarten.

Was sind die nächsten Schritte über die Pilotphase hinaus?
Nach Beendigung des EasyPASS-Pilotbetriebs wird das System auf Grundlage der gewonnenen Erkenntnisse hinsichtlich Funktionalität, Sicherheit, Nutzerfreundlichkeit sowie Wirtschaftlichkeit evaluiert. Erst dann können die Anforderungen für einen zukünftigen Roll-Out definiert und in die Planungen zur Implementierung (teil-)automatisierter Grenzkontrollsysteme einbezogen werden. Aufgrund der skizzierten, aller Voraussicht nach positiven Ergebnisse rechnen wir jedoch mit einem recht zeitnahen Roll-Out.



Sicheres Ausweisen im Internet mit dem neuen Personalausweis – ein weltweit einmaliges Projekt des BSI

Manuel Bach, Technischer Projektleiter Bürgerclient, BSI



„Der Spagat zwischen Datenschutz und Bedienungskomfort ist gelungen.“

Manuel Bach

Im Auftrag des Bundesministerium des Innern arbeitete das BSI in den Jahren 2008 und 2009 intensiv an einem Großprojekt, das ab November 2010 für weite Teile der deutschen Bevölkerung relevant wird: der Einführung des neuen Personalausweises. Neben einigen anderen Neuerungen gegenüber dem alten Ausweis (Scheckkartenformat, kontaktlose RFID-Schnittstelle, biometrisches Lichtbild und optional Speicherung von zwei Fingerabdrücken) bietet der neue Personalausweis dank eines integrierten Computerchips Funktionen, die dem Bürger bei der Nutzung des Internet völlig neue Möglichkeiten erschließen werden.

SICHERER IDENTITÄTSNACHWEIS

Ähnlich wie in der „Offline-Welt“, in der ein Bürger durch Vorzeigen seines Personalausweises seine Identität nachweist (z. B. wenn er bei der Post ein Paket abholt), kann er dies in naher Zukunft auch online tun. Das bietet sowohl für ihn als auch für die Anbieter von Dienstleistungen oder Waren im Internet enorme Vorteile. Ein Internetanbieter kann auf diese Weise sicher gehen, dass niemand mit gefälschten Identitätsdaten ein Nutzerkonto erstellt. Das Versenden von Ware auf Rechnung etwa wird für einen Händler somit wesentlich risikoärmer. Auch für den Bürger ergeben sich zahlreiche Vorteile. Wer z. B. derzeit bei einer Direktbank Geld anlegen möchte, kann zwar ein entsprechendes Konto online eröffnen und auch den anzulegenden Betrag online überweisen, muss sich aber in der Regel zusätzlich noch persönlich auf einem Postamt seiner Wahl per Postident-Verfahren mit seinem Personalausweis identifizieren. Das ist mühsam für den Kunden – und teuer für die Bank. In Zukunft kann der Bürger den neuen Personalausweis nutzen, um seine persönlichen Daten sicher online im Internet zu übertragen.

INFORMATIONEN JE NACH BEDARF REDUZIEREN – DURCH DIE FUNKTIONEN ELEKTRONISCHER ALTERSNACHWEIS UND PASSWORT-ERSATZ

Häufig geht es im Internet lediglich darum, nachzuweisen, ob man das für einen bestimmten Vorgang nötige Mindestalter besitzt. Name und Adresse sind für den Anbieter in diesem Fall irrelevant; er muss aus Gründen des

Der nPA gewährleistet die sichere Übertragung der persönlichen Daten im Internet.

Der Eigentümer des nPA hat volle Kontrolle über seine Daten.

Jugendschutzes aber dafür Sorge tragen, dass Minderjährige keinen Zugriff auf sein Angebot erhalten. Auch hierfür bietet der neue Personalausweis eine geeignete Funktion: den elektronischen Altersnachweis. Prinzipiell kann zwar auch das exakte Geburtsdatum übermittelt werden, oft ist aber lediglich der Nachweis nötig, ob eine Person älter als 16 oder 18 Jahre ist. Auch eine solche datenschutzfreundliche Ja-/Nein-Information lässt sich mit dem neuen Personalausweis übermitteln.

Schließlich lässt sich der neue Ausweis auch dazu verwenden, Benutzername und Passwort zu ersetzen – selbst dann, wenn der Nutzer dem Internetanbieter keinerlei Personendaten übermitteln möchte. So ist es etwa in vielen Webforen üblich, sich einen Nutzernamen auszudenken. Wer sich dahinter verbirgt, ist nicht einmal dem Betreiber des Forums bekannt. Mit dem neuen Personalausweis kann man sich völlig anonym in einem Forum registrieren lassen und einloggen. Dazu wird durch den Personalausweischip – im Verbund mit einem vom Diensteanbieter zusammen mit dessen Berechtigungszertifikat gesendeten Schlüssel – eine sogenannte sektorspezifische ID generiert. Anhand dieser kann der Diensteanbieter den Ausweisinhaber beim nächsten Einloggen wiedererkennen. Diese ID enthält aber keine weiteren Informationen zur Person wie Name oder Adresse. Dabei generiert der Personalausweis für unterschiedliche Diensteanbieter auch unterschiedliche sektorspezifische IDs. Sollte der Nutzer also beispielsweise einen anonymen Account bei einem Webdiskussionsforum und einen weiteren bei einem Online-Spiele-Portal besitzen, so haben die beiden Betreiber dieser Webangebote keine Möglichkeit, gemeinsam herauszufinden, dass es sich um denselben Bürger handelt. Auch dann nicht, wenn sie ihre Datenbanken (sei es legal oder illegal) miteinander abgleichen.

SICHERE DATENÜBERMITTLUNG MIT DEM „BÜRGERCLIENT“

Für all diese Anwendungen benötigt man neben dem neuen Personalausweis und einem Computer mit Internetverbindung zwei weitere Dinge: einen geeigneten kontaktlosen Kartenleser sowie eine spezielle Software, den sogenannten „Bürgerclient“. Der Kartenleser lässt sich für eine geringe Summe erwerben und soll perspektivisch sogar standardmäßig in Rechnern eingebaut werden, den Bürgerclient stellt die Bundesregierung dem Bürger kostenlos als Versionen für die Betriebssy-

steme Windows, Mac OS und Linux zur Verfügung. Sind die benötigten Komponenten vorhanden und installiert, ist der Ablauf immer derselbe: Möchte der Bürger sich beispielsweise auf einem Webportal (etwa bei seinem E-Mail-Anbieter) einloggen, ruft er die entsprechende Webseite mit seinem Browser auf und klickt auf „Einloggen mit dem Personalausweis“. Danach öffnet sich ein Bildschirmfenster des Bürgerclients, in dem nicht nur angezeigt wird, welche Daten der Diensteanbieter abfragen möchte (der Bürger kann dabei frei entscheiden, welche Berechtigungen er erteilt), sondern auch, mit welchem Anbieter der Bürger es genau zu tun hat. Auch der Diensteanbieter weist sich also gegenüber dem Bürger aus. Dabei ist die Echtheit auch dieser Daten vom Staat bestätigt – der Diensteanbieter erhält hierzu vom Bundesverwaltungsamt ein elektronisches Berechtigungszertifikat. Anschließend legt der Nutzer seinen Ausweis auf das Lesegerät, gibt seine sechsstellige Personalausweis-PIN ein (diese lässt sich übrigens vom Bürger jederzeit ändern) – und bereits nach wenigen Sekunden ist der Login-Vorgang abgeschlossen.

Eine weitere Funktion des neuen Personalausweises ist die Möglichkeit zur Erstellung qualifizierter elektronischer Signaturen. Mit Hilfe des Bürgerclients und eines geeigneten Kartenlesers kann ein Bürger damit beliebige Daten (z. B. E-Mails oder PDF-Formulare) rechtsverbindlich elektronisch unterschreiben. Im Gegensatz zum elektronischen Identitätsnachweis ist diese Funktion allerdings nicht in der Personalausweisgebühr enthalten, sondern lediglich auf dem Ausweis vorbereitet. Ein geeignetes Signaturzertifikat kann der Bürger bei einem Anbieter seiner Wahl online erwerben. Alternativ kann er statt des Personalausweises auch alle anderen im deutschen Markt gängigen Signaturkarten zusammen mit dem Bürgerclient verwenden.

GELUNGENER SPAGAT ZWISCHEN DATENSCHUTZ UND BEDIENUNGSKOMFORT

Im Laufe des Personalausweisprojektes wurden vom BSI nicht nur die Sicherheitseigenschaften des Ausweises selbst technisch spezifiziert, auch die Softwareinfrastruktur („eCard-API-Framework“), der Bürgerclient, die Kartenleser, die Erfassungsgeräte bei den Meldestellen und viele weitere nötige Komponenten basieren auf technischen Richtlinien des BSI. Das Gesamtkonzept stößt dabei nicht nur bei den Diensteanbietern auf großes Interesse, sondern erhält sogar Unterstützung von führenden Datenschützern. Denn im Vergleich zu den eID-Lösungen anderer Länder, bei denen oftmals pauschal der komplette Personendatensatz abgefragt wird, hat der Eigentümer des hiesigen neuen Personalausweises die volle Kontrolle über seine Daten. Er kann von Fall zu Fall neu entscheiden, welche Daten er in welchem Umfang übermitteln möchte. Darüber hinaus wird ihm vom Bürgerclient eindeutig angezeigt, mit welchem Diensteanbieter er es zu tun hat. Die Identität des Diensteanbieters wurde zuvor durch das Bundesverwaltungsamt überprüft. Damit leisten der neue Personalausweis und der Bürgerclient einen wichtigen Beitrag zur Bekämpfung der im Internet leider alltäglichen Betrügereien – und schützen den Bürger darüber hinaus vor der Sammlung personenbezogener Daten durch Firmen, die diese Daten für die eigentlich beabsichtigte Transaktion in Wirklichkeit gar nicht benötigen. Fazit: Der Spagat zwischen Datenschutz und Bedienungskomfort ist gelungen.

Anwendungstests

Mittels praktischer Tests wird die Anwendung des elektronischen Identitätsnachweises für den Zugang zu E-Business- und E-Government-Diensten im Internet sowie an Automaten vorbereitet, getestet und ausgewertet. Die Testphase findet im Zeitraum vom 1. Oktober 2009 bis 30. Oktober 2010 statt. Im Juni 2009 wurden aus zahlreich registrierten Firmen, Institutionen und Behörden 30 Interessenten für den zentral koordinierten Teil dieses Tests ausgewählt, in dem ein besonderes Augenmerk auf die Praxistauglichkeit, Handhabbarkeit und Akzeptanz des elektronischen Identitätsnachweises des künftigen Personalausweises gelegt wird. Ziel ist es, eine große Anzahl attraktiver Einsatzmöglichkeiten für den neuen Personalausweis zu schaffen und diese anschließend – ab dem 1. November 2010 – den Bürgerinnen und Bürgern auch für die praktische Nutzung zur Verfügung zu stellen.

Herausforderungen gemeinsam angehen

SICHERHEIT IN DER INFORMATIONSTECHNIK – DAS MUSS GELERNT SEIN!

Mit steigender Bedrohungslage nimmt auch die Nachfrage nach qualifizierten IT-Sicherheitsfachkräften in Wirtschaft und Verwaltung zu. In der Aus- und Fortbildung auf der Ebene der Bundesverwaltung übernimmt das BSI eine aktive Rolle und trägt wesentlich dazu bei, Prozesse von heute und morgen sicherer zu gestalten. Auch im Bereich der Hochschulen ist das BSI bei der Wissensvermittlung zur IT-Sicherheit selbstverständlich engagiert und als fachliche Kompetenz etabliert.

Zertifikat für IT-Sicherheit

Im Jahr 2009 absolvierten 46 Teilnehmer den Basiskurs, insgesamt wurden 31 Zertifikate erteilt. Am Aufbaukurs A nahmen zwölf Teilnehmer teil. Sieben Zertifikate konnten hier vergeben werden. 2009 erreichte erstmalig ein Teilnehmer die höchste Stufe der Ausbildung. Das Zertifikat „IT-Sicherheitsbeauftragter in der öffentlichen Verwaltung“ ist befristet, kann jedoch durch regelmäßige Fortbildungen und die Teilnahme an Workshops seine Gültigkeit behalten.

Sichere Verwaltung mit dem Zertifikat „IT-Sicherheitsbeauftragter in der öffentlichen Verwaltung“

Der Umsetzungsplan Bund fordert von allen Behörden, IT-Sicherheitsbeauftragte zu bestellen, IT-Sicherheitskonzepte zu erstellen und vor allem zeitnah auf Sicherheitsempfehlungen zu reagieren. Die IT- Sicherheitsbeauftragten in der öffentlichen Verwaltung sollen – unterstützt von der jeweiligen Behördenleitung – die notwendigen Maßnahmen des Sicherheitsprozesses initiieren und überwachen. Sämtliche Aktivitäten zur IT-Sicherheit müssen professionell organisiert sein, die BSI-Standards haben sich dabei als „best practices“ für Aufbau und Betrieb eines IT-Sicherheitsmanagements bewährt.

In Zusammenarbeit mit der Bundesakademie für öffentliche Verwaltung (BAköV) bietet das BSI Aus- und Fortbildungen mit differenziertem, dreistufigem Abschluss „Zertifizierter IT-Sicherheitsbeauftragter in der öffentlichen Verwaltung“ an. Die Lehrinhalte werden vom BSI stets dem aktuellen Wissensstand über Sicherheitsrisiken und Sicherheitsmaßnahmen angepasst. Die Ausbildung erfolgt in thematisch gegliederten Blöcken, die entsprechend den Vorkenntnissen der Schulungsteilnehmer modular gewählt werden können. Bestandteile der Abschlussprüfung sind eine Projektarbeit, deren Präsentation in einem Kolloquium und eine erfolgreiche Prüfung. In den Prüfungen sind Fragen zur IT-Sicherheit im Multiple-Choice-Verfahren zu beantworten.

Über 100 IT-Sicherheitsbeauftragte aus der öffentlichen Verwaltung treffen sich einmal jährlich zum Austausch.

Markus Ullmann vom BSI (rechts) betreut die Bachelor-Arbeit von Ranbir Singh Anand, Informatik-Student an der Hochschule Bonn-Rhein-Sieg.

Das Jobprofil „IT-Sicherheitsbeauftragter in der öffentlichen Verwaltung“ mit Zertifikat schafft Struktur, Kompetenz und Anerkennung und somit beste Voraussetzungen, IT-Sicherheit in den Behörden gewährleisten zu können. Die Kommunikation zwischen Sicherheitsberatung und IT-Sicherheitsverantwortlichen erfolgt „auf Augenhöhe“, indem dieselbe Sprache und dasselbe „Sicherheitsverständnis“ angewendet werden. In IT-Krisen kann so unmittelbar – ohne jegliche Informations- und Reibungsverluste – reagiert werden.

Kooperation zum gegenseitigen Nutzen

Seit 2001 besteht eine Kooperation des BSI mit der Hochschule Bonn-Rhein-Sieg. Mitarbeiter des BSI unterstützen den Fachbereich Informatik der Hochschule nebenberuflich durch die Übernahme von Lehrveranstaltungen im Bereich der Informationssicherheit. Im Jahr 2009 wurde die Zusammenarbeit mit der Ernennung von Markus Ullmann, Referatsleiter „Neue Technologien und wissenschaftliche Grundlagen“ im BSI, zum Honorarprofessor der Hochschule Bonn-Rhein-Sieg weiter gefestigt.

Die Zusammenarbeit markiert eine erfolgreiche Kooperation zum beiderseitigen Nutzen: Studierende profitieren durch die praxisnahen Vorlesungen, die das Lehrangebot in der Informationssicherheit an der Hochschule Bonn-Rhein-Sieg erheblich erweitern. Für das BSI wiederum entsteht durch die Verwendung öffentlich zugänglicher BSI-Inhalte in der Lehre ein zusätzlicher Multiplikatoreffekt. Des Weiteren ist es durch die Lehrtätigkeiten möglich, Studierende durch Praktika sowie Bachelor- oder Masterarbeiten gezielt zum gegenseitigen Nutzen in die Arbeit des BSI einzubinden. Studierende können das BSI und seine Arbeit und darüber hinaus die Behörde als potentiellen Arbeitgeber kennen lernen. Denn bei steigender Marktnachfrage an Absolventen im Bereich der MINT-Fächer (Mathematik, Informatik, Naturwissenschaften und Technik) gewinnen frühzeitige Kontakte zu Studierenden für das BSI immer mehr an Bedeutung – insbesondere zu Zeiten, in denen die Absolventenzahl rückläufig ist.

Vorrangiges Ziel der Zusammenarbeit ist es aber, die Lehre in der Informationssicherheit stärker zu institutionalisieren und vermehrt auch in der angewandten Forschung im Bereich der Informationssicherheit zu kooperieren.

IT-Sicherheit – eine internationale Aufgabe

Die grenzenlose Vernetzung der Kommunikations- und Informationssysteme macht international kooperatives Handeln unentbehrlich. Der globalen Herausforderung Informationssicherheit stellt sich das BSI sowohl durch aktive Mitarbeit in Gremien – so zum Beispiel der EU, NATO, OECD und ISO – als auch durch bi- und multilaterale Zusammenarbeit mit anderen Staaten.

Das internationale Engagement des BSI ist geprägt von seiner Rolle als nationale IT-Sicherheitsbehörde und weltweit anerkanntes IT-Sicherheitskompetenzzentrum. Durch seine technisch-operative Kompetenz, die erfolgreiche Zusammenarbeit mit der Industrie und die Einbindung in internationale Kooperationen ist die Expertise des BSI vielfach gefragt – in Europa etwa im Rahmen von Konsultationen und Experten-Workshops der EU-Kommission, bei der Entwicklung der IT-Sicherheitsarchitektur des Satellitensystems Galileo oder als Partner und Verwaltungsratsmitglied der ENISA, der European Network and Information Security Agency.

Darüber hinaus unterhält das BSI einen wertvollen Erfahrungsaustausch auf Leitungs- und Fachebene zu zahlreichen Behörden und Ministerien in aller Welt.

Herausforderungen tatsächlich und sachlich angehen

Gastbeitrag von Patrick Pailloux, Generaldirektor der Agence nationale de la sécurité des systèmes d'information (ANSSI), Frankreich

„Das Internet ist heute ein Teil des täglichen Lebens aller Europäer. Aber zur gleichen Zeit, wie sich innovative Anwendungen entwickelten und das Konzept der Informationsgesellschaft Gestalt annahm, hat die böswillige Nutzung des Internets ein exponentielles Wachstum erfahren. Und das in einem Ausmaß, dass sie die Chancen, die die Informationstechnik für uns bereit hält, aufs Spiel setzt. Ein weltweites politisches Bewusstsein dahingehend keimt bereits auf, und gleichzeitig entsteht der Wille, die Herausforderungen tatsächlich und sachlich anzugehen. Es ist bemerkenswert und gleichzeitig beruhigend festzustellen, dass Deutsche und Franzosen im Hinblick auf Cyber-Sicherheit die gleiche strategische Vision teilen. Dies hat zu ähnlichen Schlussfolgerungen geführt, die sich in den drei folgenden Dimensionen äußern: Zunächst ist es die Bekräftigung des Führungsanspruchs der nationalen Strukturen, die für die Sicherheit der Informationssysteme verantwortlich zeichnen. Des Weiteren wird eine hochgradige Dringlichkeit in der Umsetzung der Cyber-Sicherheit gesehen – insbesondere durch Überwachung der sensitivsten Netze. Schlussendlich ist die Entwicklung von Sicherheitsprodukten zu beschleunigen.

In unseren Ländern wurden diese Aspekte auf politischer Ebene konkretisiert: in Frankreich am 7. Juli 2009 durch die Veröffentlichung des Errichtungserlasses der nationalen Behörde für die Sicherheit der Informationssysteme. Die Errichtung erfolgte im Rahmen der neuen französischen Strategie im Hinblick auf Verteidigung und nationale Sicherheit, die der Verteidigung gegen IT-Attacken eine herausragende Dringlichkeit beimisst. In Deutschland trat am 19. August des gleichen Jahres die Novellierung des BSI-Gesetzes in Kraft, die dem BSI weitergehende Aufgaben und Befugnisse einräumt.

In der Praxis finden sich im neu definierten Auftrag unserer beider Behörden zahlreiche Konvergenzpunkte. Unser Aktionsradius deckt die Gesamtheit der Informationsgesellschaft ab: Jenseits des Schutzes klassifizierter Informationen – seit Langem in unserer Historie verankert – richten wir unsere Aufmerksamkeit verstärkt auf die Allgemeinheit. Unser Expertenwissen auf dem Gebiet der IT-Sicherheit bringen wir ein in die Verwaltung, bei den Betreibern kritischer Infrastrukturen wie auch in die Gesamtheit der wirtschaftlichen Akteure und in die breite Öffentlichkeit als einen Teil unseres prioritären Auftrags.

Über die Hilfestellung hinaus müssen wir unsere Fachkompetenz nutzen, um den Regierungsstellen und den wirtschaftlichen Akteuren aktiv Dienstleistungen und vertrauenswürdige Sicherheitsprodukte zur Verfügung zu stellen. Uns obliegt es auch, innovative Lösungen zu entwickeln und einzubringen und uns nicht mehr – wie es in Frankreich in der Vergangenheit der Fall war – auf eine Rolle als kritischer Zuschauer zu beschränken. Angesichts einer gesteigerten Bedrohung wird unser Einsatz und unsere aktive Beteiligung immer wichtiger. Pragmatische und wirtschaftlich erschwingliche Lösungen für die sich uns stellenden Probleme zu finden, ist eine zwingende Notwendigkeit.

Insgesamt setzt wirkungsvolles Handeln einen Austausch von Informationen, ein Teilen von Erfahrung und ein Zusammenarbeiten unter Verbündeten voraus. Dies sind nicht nur Worte – Taten sind eine unausweichliche Verpflichtung. Ein Aspekt ist nachdrücklich zu betonen: Die Bedrohung heute ist global. Das Internet hebt die Vorstellung von Distanz und Grenze auf. Angesichts dieser Entwicklung ist es nunmehr wesentlich und unausweichlich zu kooperieren, um eben dieser Bedrohung die Stirn zu bieten.

Auf dem Gebiet der Cyber-Sicherheit muss die deutsch-französische Bindung ein positives Beispiel sein und bleiben. Sie wird Motor für die Weiterentwicklung der IT-Sicherheit in der Europäischen Union sein.“

„Wir brauchen das Know-how des BSI in Europa“

Interview mit Dr. Udo Helmbrecht

Dr. Udo Helmbrecht ist Executive Director der European Network and Information Security Agency (ENISA) mit Sitz in Heraklion/Kreta und war von 2003 bis 2009 Präsident des BSI.

Dr. Helmbrecht, in welchen Bereichen sehen Sie Deutschland auf EU-Ebene besonders gefordert, und welchen Beitrag erwarten Sie vom BSI zur Stärkung der IT-Sicherheit in Europa?

Das BSI hat bisher schon einen großen Teil zur Erhöhung des europäischen Sicherheitsniveaus beigetragen. Ich denke da nur an die vielfältigen grenzüberschreitenden Kontakte, die geknüpft wurden. Aber auch die umfangreiche Mitarbeit in vielen Projekten, beispielsweise im STORK²-Projekt. Wir brauchen diesen Erfahrungsschatz und das Know-how des BSI in Europa. Ich wünsche mir, dass dieser Wissenstransfer und die Mitarbeit des BSI in vielen internationalen Foren und Gremien weiter ausgebaut werden kann, insbesondere das Engagement im ENISA Verwaltungsrat, in dem Deutschland durch das BSI vertreten wird. Das BSI hat beispielgebende Wirkung für die Europäische Union. Sehen Sie zum Beispiel nur einmal nach Frankreich: dort wurde im letzten Jahr eine ähnliche Sicherheitsagentur, die ANSSI (Agence nationale de la sécurité des systèmes d'information) eingerichtet.

Was sind die aktuellen Schwerpunkte der ENISA?

Das Arbeitsprogramm von ENISA in 2010 sieht drei große Themenbereiche vor: die Widerstandsfähigkeit von Netzen (resilience) einschließlich der kritischen IT-Infrastrukturen (ciritical IT infrastructure protection),

verstärkte Formen der Kooperation wie beispielsweise CERTs und die Adressierung aufkommender und zukünftiger Risiken (emerging risks). Außerdem haben wir in diesem Jahr sogenannte vorbereitende Programme in Angriff genommen: erstens, das Thema Vertrauen und Persönlichkeitsrechte im Internet (privacy and trust) einschließlich digitaler Identitäten (eID) und zweitens, Anreize und Hindernisse für Multistakeholder – Kooperationsmodelle im Bereich der Netzwerk- und Informationssicherheit.

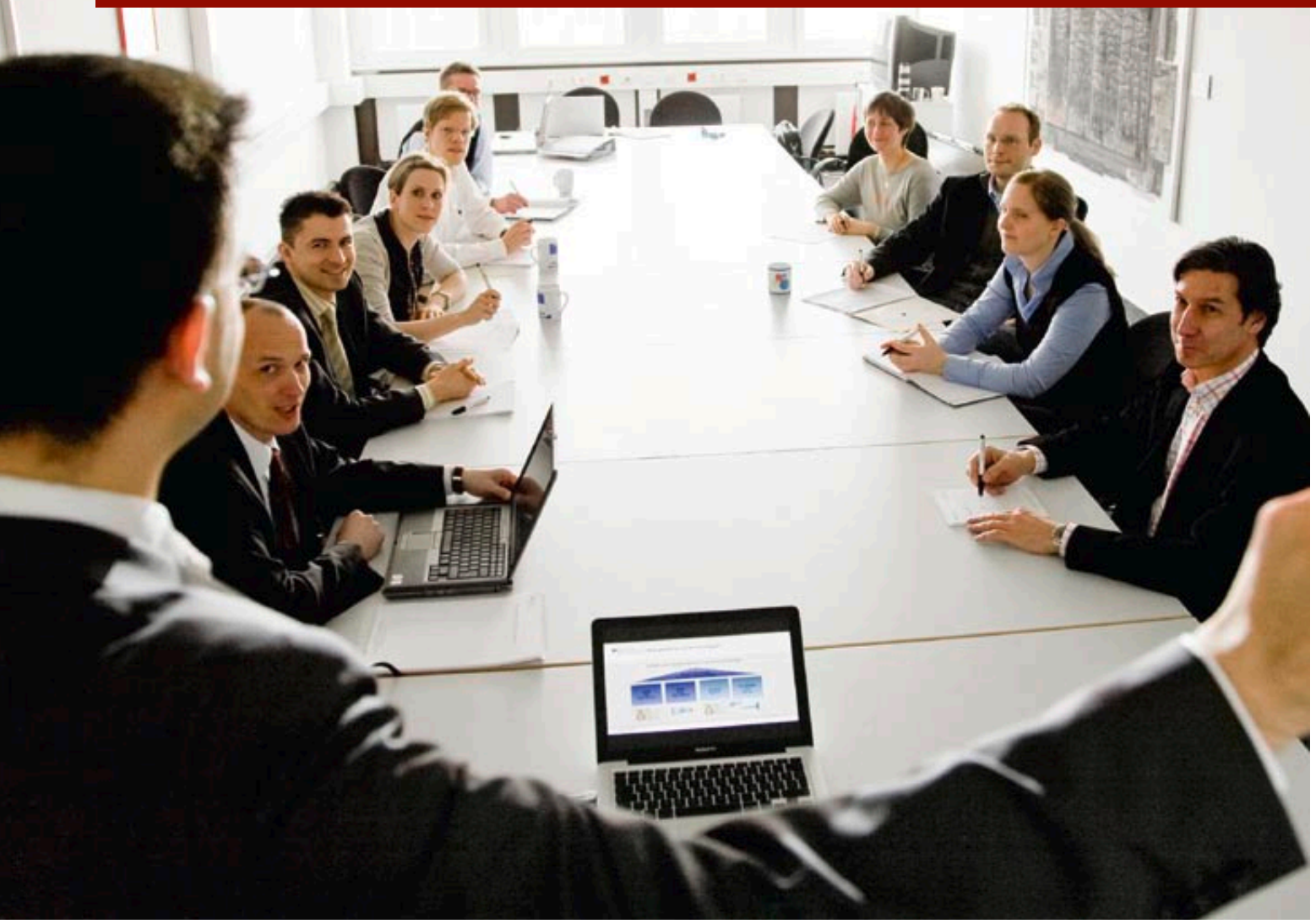
Wie ist die Zusammenarbeit mit den Mitgliedstaaten?

ENISA bringt als Kompetenzzentrum alle relevanten Stakeholder zusammen und stärkt den Austausch von Erfahrungen und Informationen. Wir positionieren uns als Schrittmacher für mehr IT-Sicherheit, um in enger Partnerschaft europäische Lösungen aufzeigen. Freilich gibt es Mitgliedstaaten, die in einigen Bereichen schon größere Fortschritte erzielt haben. Wir erwarten von diesen die Bereitschaft zum Wissenstransfer – beispielsweise in die neuen Mitgliedsstaaten. Denn uns allen ist bewusst, dass Sicherheit nicht an Grenzen halt macht und jeder Know-how-Transfer letztlich der eigenen Sicherheit dient. Ich bin sehr positiv gestimmt, dass das weiterhin und auch in verstärktem Maße geschehen wird. Beispiele gibt es hierfür schon genug, so zum Beispiel im CERT/CSIRT[3] Bereich. Es ist unser Ziel, dass es in jedem Mitgliedsstaat ein Regierungs-CERT gibt. Somit kann Deutschland durch ein verbessertes IT-Sicherheitsniveau auf europäischer Ebene von der Kooperation mit ENISA profitieren.

Was wünschen Sie sich für die IT-Sicherheit in Europa?

Über den weiteren Ausbau eines qualitativ hochwertigen Dialoges mit den Mitgliedsstaaten, den EU-Institutionen und allen weiteren Akteuren der Informationsgesellschaft muss ENISA die zukünftigen technischen Herausforderungen der Informations- und Kommunikationstechnologie in das Arbeitsprogramm aufnehmen. Dabei darf ENISA keine Aktivitäten der Mitgliedsstaaten duplizieren, noch in Konkurrenz dazu treten. Vielmehr muss ENISA dort beraten und unterstützen, wo im europäischen Verbund entweder für das einzelne Mitgliedsland oder die Union insgesamt ein Mehrwert entsteht. Die Arbeitsergebnisse, die letztlich eine Anstrengung aller Partner sind, müssen in den Mitgliedsstaaten sichtbar werden. Dazu bitte ich auch um die Mithilfe aller.

[2] STORK (Secure Identity Across Borders Linked): www.eid-stork.eu
[3] Computer Emergency Response Team/ Computer Security Incident Response Team



Herausforderungen gemeinsam angehen

Herz und Hirn des BSI: Unsere Mitarbeiter

IT-Sicherheit aktiv mitgestalten

Der entscheidende Erfolgsfaktor für die Arbeit des BSI sind seine Mitarbeiter. Nicht nur als Beruf, sondern auch als Berufung – so empfinden viele Kolleginnen und Kollegen ihre Tätigkeit im Bundesamt für Sicherheit in der Informationstechnik. Das Zukunftsthema IT-Sicherheit aktiv mitgestalten zu können, bedeutet für sie Herausforderung und Chance gleichermaßen. Im BSI finden Arbeitnehmer sehr gute Rahmenbedingungen vor, so etwa ein hohes Maß an Eigenverantwortung, State-of-the-art-Technik und exzellente Fortbildungsmöglichkeiten – gepaart mit einem positiven Arbeitsklima und der Aussicht auf einen gesicherten Arbeitsplatz. Hinzu kommt ein intensiver Kontakt auf internationaler Ebene und zur Privatwirtschaft.

Informationen über die Arbeit im BSI und über Stellenangebote finden Sie unter www.bsi.bund.de.

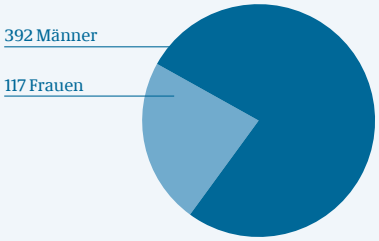
„Das Arbeitsklima ist sehr kollegial. Erfahrene und junge Kollegen arbeiten gut zusammen.“

Semra Agirtas

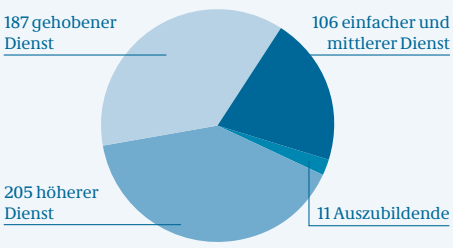
Semra Agirtas, Sachbearbeiterin „Akkreditierung und Qualitätsmanagement des Zertifizierungs- und Zulassungsschemas“

„Die Themen und Aufgaben, die das BSI betreut, empfinde ich als spannend. Hier kommt es nicht darauf an, einem Unternehmen zu mehr wirtschaftlichem Erfolg zu verhelfen, sondern den Bürgern, der Verwaltung und somit der gesamten Gesellschaft mit Standards, Richtlinien, Hinweisen oder Warnungen eine mehr als nützliche Dienstleistung anzubieten. Mich motiviert an meiner Tätigkeit ganz besonders, dass sie Teil einer größeren Sache ist, die zumeist die ganze Bundesrepublik betrifft, interessiert und auch voranbringt. Ich finde es aufregend, mit Themen wie elektronischer Gesundheitskarte, De-Mail oder Digitalfunk die Zukunft mit zu gestalten und meinen Teil zu der sich immer weiter verändernden Technologie und Gesellschaft beizutragen. Im BSI stimmt einfach das Komplettpaket. Aufgaben und Themen sind sehr abwechslungsreich, mein Arbeitsplatz ist modern und auf meine Bedürfnisse eingestellt. Das Arbeitsklima ist sehr kollegial. Erfahrene und junge Kollegen arbeiten gut zusammen, und ein ‚Wir-Gefühl‘ entsteht auch durch verschiedene gemeinschaftliche Veranstaltungen. Außerdem gibt es zahlreiche Angebote, mit denen man auch einmal über den eigenen Tellerrand hinaus blicken kann. Die Weiterbildungsmaßnahmen eröffnen mir Perspektiven und zeigen mir, dass ich als Mitarbeiter geschätzt werde. Im BSI kann man seine Zukunft planen, denn es werden Konzepte gefördert und gestaltet, die es einer Frau ermöglichen, Beruf und Familie zu vereinen.“

Statistik – Mitarbeiter (Stand: Ende 2009)



Mitarbeiter (Laufbahngruppen)



Wir setzen auf Nachwuchs!

Seit 2008 fördert das BSI Bachelor-Studenten mit einer Studienbeihilfe und garantiert ihnen im Anschluss an ihr Studium eine Festanstellung.

„Im BSI gibt es kurze Entscheidungswege und eine kundenorientierte Denkweise.“

Dr. Uwe Kraus

Dr. Uwe Kraus, Fachbereichsleiter „Kryptotechnik“

„Ich freue mich, mein Wissen und Können als Ingenieur und Diplomwirtschaftsinformatiker seit 2004 bei einem der Top-IT-Arbeitgeber einbringen zu können. Nach einer zweijährigen Tätigkeit als Referent habe ich ab November 2006 das Referat „Evaluierung in Kryptosystemen“ geleitet und bin seit April 2010 Fachbereichsleiter Kryptotechnik. Besonders die technisch abwechslungsreichen und komplexen Themengebiete im Bereich der IT-Sicherheit empfinde ich als eine kontinuierliche Motivation. So umfassen die Aufgaben der Evaluierung und Bewertung von IT-Sicherheitsprodukten, insbesondere für den Bereich der Verschlusssachenverarbeitung, die Prüfung unterschiedlicher Produktkategorien wie beispielsweise softwarebasierte Verschlüsselungslösungen für Festplatten und E-Mails bis hin zu hoch komplexen taktischen Funksystemen und Satelliten. Die Zusammenarbeit mit hochqualifizierten und motivierten Fachkräften prägt dabei ein positives Arbeitsklima und trägt erheblich dazu bei, erfolgreiche Ergebnisse zu erzielen. Hinzu kommt die für eine Behörde untypische, unbürokratische Arbeitsweise im BSI, die sich in kurzen Entscheidungswegen und einer kundenorientierten Denkweise äußert.“

„Thematisch sind wir am Puls der Zeit.“

Matthias Intemann

Matthias Intemann, Referent „Zertifizierung“

„Im Rahmen meiner Tätigkeit in der Zertifizierung von Produkten beim BSI habe ich die Chance, spannende Bereiche der IT-Sicherheit mit zu gestalten. Die Vielzahl der Kommunikationspartner und Produkte, mit denen man im Laufe der Zeit zu tun hat, bietet eine große Abwechslung: Immer wieder sind neue Herausforderungen zu finden. Langeweile gibt es nicht. Thematisch sind wir am Puls der Zeit. Die Vielseitigkeit drückt sich auch in der Art der Tätigkeiten aus, die vom Leiten von Projekten, über Beratung bis zur Bewertung von Inhalten reicht. Die Zusammenarbeit mit fachlich äußerst kompetenten Kollegen, auch über Zuständigkeiten hinaus, sowie mit externen Know-how-Trägern macht die Arbeit besonders spannend. Gerade der fundierte Austausch hilft dabei, sich weiter zu entwickeln. Die guten Weiterbildungsmöglichkeiten im BSI unterstützen hierbei natürlich auch. Selbst in Zeiten hoher Auslastung wird der allgemeine Qualitätsanspruch an die Leistungen aufrecht erhalten, so dass automatisch effizient gearbeitet wird. Qualitätsmanagement und Prozessoptimierung, die in ein professionelles Umfeld gehören, sind eine Selbstverständlichkeit. Gerade in Gesprächen mit externen Kontakten wird immer wieder klar, dass das BSI eine allgemein akzeptierte und geschätzte Behörde ist. Das Gefühl, der IT-Sicherheit im Allgemeinen kompetent förderlich zu sein, vermittelt darüber hinaus noch die Befriedigung einer sinnvollen Tätigkeit.“

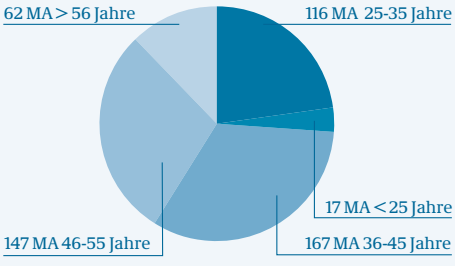
„Man lernt bei Verhandlungen die Sichtweisen anderer Nationen kennen.“

Dr. Dörte Rappe

Dr. Dörte Rappe, Referentin „Leitungsstab, Innenrevision“

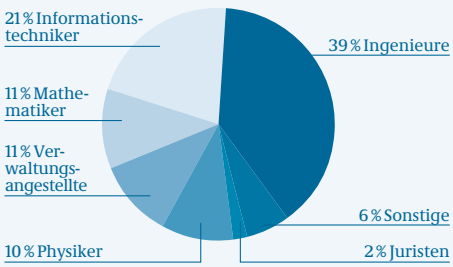
„Mit der Arbeit im BSI habe ich meinen Traumjob gefunden, da die Tätigkeit ausgesprochen abwechslungsreich und interessant ist. Es gibt viele nette Kollegen, die man auch abseits des beruflichen Alltags bei gemeinsamen Aktivitäten besser kennen lernen kann. Durch Teilnahme an internationalen Arbeitsgruppen und Konferenzen erhält man die Möglichkeit, die Welt und politische Sichtweisen kennenzulernen sowie andere Wissenschaftler zu treffen, sich mit ihnen auszutauschen und zu diskutieren. Bei Verhandlungen lernt man die Sichtweisen anderer Nationen kennen und die deutschen Interessen zu vertreten. Im Gegensatz zur Universität erfährt man bei der Arbeit im BSI auch von den ‚wirklichen‘ Probleme in der Anwendung und erhält so ganz neue Sichtweisen. Ich finde es dabei besonders faszinierend, mich mit dem Bereich Kryptographie nicht nur theoretisch, sondern auch praktisch auseinanderzusetzen und dabei herauszufinden, wie politische und fachliche Interessen von Anwendern optimal miteinander vereinbart werden können. Durch zahlreiche Weiterbildungsangebote – sowohl fachlicher als auch allgemeiner Natur – erschließen sich uns unglaublich viele inhaltlich interessante Bereiche innerhalb des Hauses. Durch die Möglichkeit, für eine feste Zeit in der Behörde zu „rotieren“, lernt man nie aus, und es wird nicht langweilig. Außerdem lässt sich auf diese Weise am besten der Bereich entdecken, der ideal zu den eigenen Interessen und Fähigkeiten passt. Darüber hinaus sind in einer Behörde natürlich die flexiblen Arbeitszeiten sowie die Möglichkeit, Familie und Beruf vereinbaren zu können, interessant.“

Altersstruktur Mitarbeiter



Beruflicher Hintergrund

(nur höherer und gehobener Dienst)



Das BSI ist top!

Bereits zum wiederholten Mal in Folge ist das BSI unter Deutschlands Top-Arbeitgebern im IT-Bereich vertreten: als beliebteste Behörde im öffentlichen Sektor.

... und das passierte noch 2008/2009

2008/2009 im Überblick

Januar

16. – 18. Januar

Omnicard

Das BSI nimmt mit Vorträgen am führenden Fachkongress für die Smart-Card-Branche teil.

24. Januar

CAST-Workshop

Das BSI beteiligt sich am CAST-Workshop in Darmstadt zum Thema Digitale Signatur.

31. Januar

5 Jahre www.bsi-fuer-buerger.de

Seit dem 31. Januar 2003 informiert das BSI Bürgerinnen und Bürger auf seinem Portal über die Gefahren im Internet (Foto).

Februar

11. Februar

Workshop Aufklärung und Sensibilisierung im Zeichen der IT-Sicherheit

Anlässlich des EU-Aktionstages „Safer Internet Day“ treffen sich Experten aus Wirtschaft, Wissenschaft und Verwaltung auf Einladung des BSI zum Workshop „Aufklärung und Sensibilisierung im Zeichen der IT-Sicherheit“.

20. Februar

Virtualisierung und IT-Grundschutz

„Virtualisierung und IT-Grundschutz“: In Zusammenarbeit mit der Networkers AG veranstaltet das BSI den 1. IT-Grundschutztag 2008.

März

4. – 9. März

CeBIT 2008

BSI-Experten informieren auf der CeBIT 2008 unter anderem über IT-Grundschutz, IT-Frühwarnsysteme, CERT-Bund, hoheitliche Dokumente und IT-Sicherheitszertifizierung.

April

8. – 10. April
RSA Konferenz

In San Francisco präsentiert das BSI auf dem von TeleTrusT betreuten deutschen Gemeinschaftsstand seine Tätigkeitsschwerpunkte im Bereich IT-Sicherheit.

9. April
2. IT-Grundschutztag

Beim 2. IT-Grundschutztag 2008 beschäftigen sich rund 120 Teilnehmer mit den Sicherheitsaspekten des Microsoft-Betriebssystems Windows Vista.

22. – 23. April
3. interdisziplinäres Symposium

Zum 3. interdisziplinären Symposium des BSI und der Arbeitsgruppe Identitätsschutz im Internet (a-i3) erscheinen Vertreter aus Unternehmen, Wissenschaft, Politik und Verbänden.

24. April
Girls' Day

Das BSI beteiligt sich mit Vorträgen und Präsentationen an dem bundesweiten Aktionstag für Berufsbildung.

Mai

28. – 31. Mai
LinuxTag in Berlin

Das BSI präsentiert seine Lösungen im Bereich OSS, die neben Freier Software für Linux auch Freie Sicherheitslösungen für Windows umfassen.

Juni

17. – 18. Juni
OECD-Konferenz zur Zukunft der Internet-Ökonomie

Bei der OECD-Konferenz zur Zukunft der Internet-Ökonomie in Seoul, Korea, stellt BSI-Präsident Dr. Udo Helmbrecht IT- und Internetsicherheitsaspekte des geplanten elektronischen Personalausweises und der Bürger-Portale vor.

Juli

7. Juli

Call for Papers

Start des Call for Papers für den 11. Deutschen IT-Sicherheitskongress.

August

23. – 24. August

„Einladung zum Staatsbesuch“ in Berlin

Die Bundesregierung öffnet die Türen für interessierte Bürgerinnen und Bürger. Das BSI informiert im BMI über das Service-Portfolio für Privatanwender.

September

1. – 2. September

3. Jahrestagung für IT-Sicherheitsbeauftragte

Das BSI und die Bundesakademie für die öffentliche Verwaltung (BakÖV) organisieren die 3. Jahrestagung für IT-Sicherheitsbeauftragte der Bundesbehörden.

8. – 13. September

Informatik 2008

Mit Vorträgen und einem Informationsstand nimmt das BSI an der 38. Jahrestagung der Gesellschaft für Informatik teil.

23. – 25. September

9th International Common Criteria Conference (ICCC)

Das BSI ist mit Vorträgen in Korea dabei.

23. September

3. IT-Grundschutztag

Das BSI und das Informatikzentrum der Sparkassenorganisation (SIZ) laden zum 3. IT-Grundschutztag (Foto).

Oktober

7. – 9. Oktober
10. Information Security Solutions Europe (ISSE)

Das BSI beteiligt sich an der 10. Information Security Solutions Europe (ISSE) Konferenz in Madrid.

7. – 10. Oktober
Security-Messe

Das BSI beteiligt sich mit einem Ausstellungsstand und Fachvorträgen an der Security-Messe in Essen.

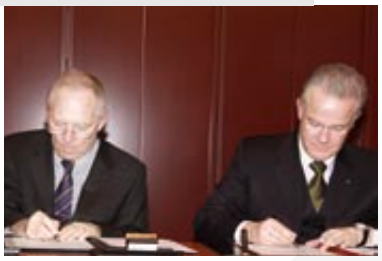
21. – 24. Oktober
Systems 2008

Das BSI übernimmt die Schirmherrschaft der IT-Security Area und präsentiert eine Vortragsreihe und einen Messestand (Foto).

24. Oktober
Deutscher IT-Sicherheitspreis

Der mit insgesamt 200.000 Euro dotierte Deutsche IT-Sicherheitspreis der Horst-Görtz-Stiftung wird unter der Schirmherrschaft des BSI und unter Mitwirkung in der Jury verliehen.

November



3. November
4. IT-Grundschutztag

Vorträge und Diskussionen zu Informationssicherheit und Datenschutz stehen im Mittelpunkt des 4. IT-Grundschutztages in Berlin.

4. – 5. November
Moderner Staat

Auf der wichtigsten Kongressmesse für die öffentliche Verwaltung Moderner Staat in Berlin fungiert das BSI als „Partner IT-Sicherheit".

10. November
Kooperationsabkommen

Bundesinnenminister Wolfgang Schäuble und Hans-Jörg Bullinger, Präsident der Fraunhofer-Gesellschaft, unterzeichnen ein Kooperationsabkommen über die Zusammenarbeit im Bereich der IT-Sicherheit. Das BSI und die Fraunhofer SIT werden die Partnerschaft umsetzen (Foto).

12. November
5. IT-Grundschutztag

Aufgrund der großen Nachfrage führt das BSI eine weitere Veranstaltung mit dem Informatikzentrum der Sparkassen-Organisation (SIZ) in Bonn durch.

20. November
3. Nationaler IT-Gipfel

Der neue elektronische Personalausweis ist eines der zentralen Themen des 3. Nationalen IT-Gipfels in Darmstadt. Das BSI präsentiert Arbeiten an Fingerabdruck-Sensoren mit Lebendfinger-Erkennung und anderen biometrischen Systemen.

28. November
Auditorentreffen

Über 200 Auditoren informieren sich über aktuelle Entwicklungen rund um die Themen IT-Grundschutz und Zertifizierung beim jährlichen Auditorentreffen in Bonn.

Dezember

2. Dezember
ZertiFA 2008

Das BSI nimmt mit Vorträgen an der ZertiFA 2008 in Berlin teil.

Januar

20. – 22. Januar

Omnicard 2009

Das BSI stellt in Berlin Innovationen und Dienstleistungen im Feld der Kartentechnologie und -anwendung vor.

Februar

10. Februar

Safer Internet Day 2009

Das BSI beantwortet in einer Telefonaktion Anfragen von Bürgern rund um das Thema „Surfen– aber sicher!“.

12. Februar

1. IT-Grundschutz-Tag

Das BSI veranstaltet mit dem Fraunhofer-SIT und dem Center for Advanced Security Research Darmstadt (CASED) den ersten IT-Grundschutz-Tag des Jahres.

März

3. März

Bericht zur Lage der IT-Sicherheit in Deutschland 2009

IT-Bedrohungslage auf anhaltend hohem Niveau: Das BSI veröffentlicht den Bericht zur Lage der IT-Sicherheit in Deutschland 2009.

3. – 8. März

CeBIT 2009

Auf der weltgrößten Computermesse CeBIT nimmt das BSI mit einem Stand, mehreren Vorträgen und Präsentationen teil.

23. – 24. März

Interdisziplinäres Symposium

a-i3 und das BSI informieren und diskutieren beim interdisziplinären Symposium zum Thema Identitätsschutz in E-Government und E-Business.

April

20. – 24. April

RSA Conference in San Francisco

Das BSI ist als Aussteller auf dem Gemeinschaftsstand, der vom BMWi, dem AUMA und dem TeleTrusT getragen wird, vertreten.

23. April

Girls' Day

Mädchen-Zukunftstag: Erneut beteiligt sich das BSI am alljährlichen Girls' Day.

Mai

12. – 14. Mai

11. Deutscher IT-Sicherheitskongress

„Sichere Wege in der vernetzten Welt": Rund 500 Teilnehmer aus Wirtschaft, Verwaltung und Wissenschaft tauschen sich auf dem 11. Deutschen IT-Sicherheitskongress über aktuelle Trends und Perspektiven in der IT-Sicherheit aus.

Juni

18. Juni

3. Berliner Gespräch des Münchner Kreises

Das BSI informiert beim 3. Berliner Gespräch des Münchner Kreises zur technischen Umsetzung des geplanten elektronischen Personalausweises.

23. Juni

15 Jahre IT-Grundschutz

Das BSI lädt zu einer Jubiläumsveranstaltung mit renommierten Grundschutz-Experten nach Bonn ein.

24. – 27. Juni

LinuxTag 2009

In Berlin zeigt das BSI seine aktuellen IT-Sicherheitslösungen auf Basis von Open Source Software, darunter Freie Software für Linux sowie für Windows und Mac OS X.

Juli

2. Juli

Initiative für Sicherheitserweiterungen im Domain Name System

Initiative für mehr Internet-Sicherheit: Auftakt der gemeinsamen Initiative für Sicherheitserweiterungen im Domain Name System von DENIC, eco und BSI in Frankfurt. (vgl. S. 29)

August

20. August

BSI-Gesetz

Das neue BSI-Gesetz tritt in Kraft.

23. – 24. August

Tag der offenen Tür der Bundesregierung

BSI für Bürger: DaS Service-Angebot für Bürgerinnen und Bürger zeigt das BSI beim Tag der offenen Tür der Bundesregierung im BMI.

30. August

Tag der offenen Tür im alten Bundesviertel

Das BSI nimmt erstmals am Tag der offenen Tür im alten Bundesviertel teil und präsentiert sich an seinem Bonner Standort allen interessierten Bürgerinnen und Bürgern.

September

10. September

Bonner Firmenlauf

Kolleginnen und Kollegen des BSI nehmen für einen guten Zweck am Bonner Firmenlauf teil.

11. – 12. September

Workshop on Factoring Large Integers

Das BSI ist Mitorganisator des Workshop on Factoring Large Integers an der Ruhr-Universität in Bochum.

22. September

2. IT-Grundschutztag

Der 2. IT-Grundschutztag findet in Bonn statt. Partner ist das Informatikzentrum der Sparkassenorganisation (SIZ).

22. – 23. September

Jahrestagung der IT-Sicherheitsbeauftragten

Die Jahrestagung der IT-Sicherheitsbeauftragten des Bundes findet unter Vorsitz des BSI und der BaköV in Brühl statt.

22. – 24. September

10. Internationale Common Criteria Conference

Das BSI beteiligt sich an der 10. Internationalen Common Criteria Conference (ICCC) in Tromsø, Norwegen (Foto).

Oktober

13. – 15. Oktober
it-sa

Das BSI ist mit einem Stand und Vorträgen auf der Nachfolgemesse der Systems, der it-sa in Nürnberg, vertreten.

14. Oktober
3. IT-Grundschutz-Tag

Der 3. IT-Grundschutz-Tag findet im Rahmen der it-sa Messe in Nürnberg statt.

16. Oktober
Neue Leitung im BSI

Michael Hange wird neuer BSI-Präsident und tritt die Nachfolge von Dr. Udo Helmbrecht an. Horst Flätgen wird Vizepräsident.

23. – 25. Oktober
IT-Talentegipfel

Im Rahmen der Nachwuchsförderung nimmt das BSI am IT-Talentegipfel auf Burg Liebenzell teil.

27. Oktober
Public-IT-Security

BSI-Präsident Michael Hange eröffnet die neue Kongressmesse Public-IT-Security (PITS) in Berlin.

November

19. November
4. IT-Grundschutztag

Das BSI und das Horst Görtz Institut richten den 4. IT-Grundschutztag des Jahres in Bochum aus.

24. – 25. November
Moderner Staat 2009

Moderner Staat 2009 in Berlin: Das BSI ist als Aussteller auf der Verwaltungsmesse dabei.

27. November
Auditorentreffen

Rund 200 Auditoren, die ISO 27001-Audits auf der Basis von IT-Grundschutz durchführen, versammeln sich zum jährlichen Auditorentreffen des BSI in Bonn (Foto).

Dezember

1. Dezember
ZertiFa 2009

Mit diversen Vorträgen nimmt das BSI an der ZertiFa 2009 in Berlin teil und hat den Konferenzvorsitz inne.

2. Dezember
Neuer Präsident

Michael Hange wird als neuer Präsident des BSI offiziell durch Staatssekretär Dr. Hans Bernhard Beus, zugleich IT-Beauftragter der Bundesregierung, in sein Amt eingeführt (Foto).

8. Dezember
4. Nationaler IT-Gipfel

Beim 4. Nationalen IT-Gipfel vereinbaren das BSI und der Verband der deutschen Internetwirtschaft eco e.V. gemeinsame Aktivitäten bei der Bekämpfung von Botnetzen (vgl. S. 28f).

Organisationsplan

April 2010

Präsident Michael Hange

Vizepräsident Horst Flätgen

Leitungsstab
Innenrevision

Stab Internationale Beziehungen

Pressesprecher

Abteilung 1
Dr. Hartmut Isselhorst

Fachbereich 11
Sicherheit in Anwendungen und Kritischen Infrastrukturen

Kommunikationssicherheit in Geschäftsprozessen
Kritische Infrastrukturen und IT-Sicherheitsrevision
VS- und IT-Sicherheitsberatung
IT-Sicherheitsmanagement und IT-Grundschutz
Hochverfügbarkeit in kritischen Geschäftsprozessen

Fachbereich 12
Sicherheit in Netzen

CERT-Bund
Internetsicherheit
Sicherheit in Betriebssystemen
IT-Penetrationszentrum
Abwehr von Internetangriffen
Regierungsnetze

Abteilung 2
Dr. Gerhard Schabhüser

Fachbereich 21
Kryptotechnik

IT-Sicherheitsarchitekturen und -plattformen
Entwicklung von Kryptokomponenten
Entwicklung von Kryptosystemen
Evaluierung von Kryptosystemen
Krypto- und IT-Sicherheitsadministration

Fachbereich 22
Abhörsicherheit

Mobilfunksicherheit
Abstrahlsicherheit
Grundlagen der Lauschabwehr
Lauschabwehrprüfungen
Materielle Sicherungstechnik

Kompetenzbereich Kryptographie

Entwicklung und Evaluierung kryptographischer Verfahren

Abteilung 3
Bernd Kowalski

Fachbereich 31
Neue Technologien und Konformitätsprojekte

Neue Technologien und wissenschaftliche Grundlagen
Hoheitliche Dokumente und elektronische Ausweise
Industriekooperation

Fachbereich 32
Zertifizierung, Zulassung und Konformitätsprüfungen

Information und Kommunikation, Öffentlichkeitsarbeit
Zertifizierung
Zulassung und Prüfstandards
Akkreditierung und Qualitätsmanagement

Abteilung Z
Horst Samsel

Organisation, Personal, Haushalt
Interne Serviceleistungen, Projektbegleitung
Objekt- und Geheimschutz

IT-Stab

IT-Organisation/ -Planung
IT-Betrieb

Bildnachweis

adpic, ANSSI, BEIT Systemhaus, Bitkom, BMI, BSI, Bundespolizeidirektion Frankfurt/Main, Dataport, Deutsche Messe Hannover, Eric Lichtenscheidt, Fotolia, Girls' Day, Infineon, insafe, LinuxTag/Messe Berlin, Norbert Luckhardt (kes), OpenLimit, Secumedia Verlag, Shutterstock, SIGNAL IDUNA, T-Systems/HTC, trendence, www.omnicard.de

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 Communication Group

Druck
Das Druckhaus Bernd Brümmer, Alfter

Stand
Mai 2010

Artikelnummer
BSI-JB10/601

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