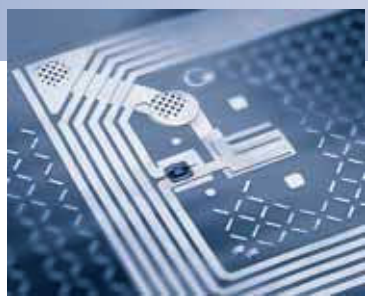
Bundesamt
für Sicherheit in der
Informationstechnik



Jahresbericht 2005

Bundesamt
für Sicherheit in der
Informationstechnik
www.bsi.bund.de

Information
- Internet-Sicherheit für alle Zielgruppen
- Spezielle Themen der Informationstechnik
- Webportal für Bürger, Wirtschaft und Verwaltung
- Hotline und Service Center für Bürger
- Veröffentlichungen von Fachthemen und Sicherheitshinweisen
- Präsentation der Arbeitsergebnisse bei Fachmessen und -kongressen

Beratung
- Risiken im Internet und bei bestimmten IT-Technologien
- Sicherheit für IT-Plattformen und -Infrastrukturen für Bundesbehörden
- Penetrationstests
- Grundschutz als Methodik und Werkzeug für sichere IT-Infrastrukturen
- Risikobewertung und Sicherung Kritischer Infrastrukturen

Entwicklung
- Kryptoverfahren, Biometrische Verfahren
- IT-Sicherheitslösungen (z.B. Kryptogeräte für den staatlichen Geheimschutz)
- Testwerkzeuge und Messmittel für Konformitätsprüfungen und für die Abhörsicherheit

Zentrale Serviceleistungen und Betrieb
- Schlüsselmittelherstellung/-verteilung und Root-CA (Bund)
- Warn- und Alarmdienste, CERT-Bund
- Technische Koordination des IVBB

Prüfvorschriften
- Schutzprofile für IT-Komponenten und -Produkte
- Technische Richtlinien für Komponenten in IT-Projekten der Bundesbehörden
- Schutzprofile und Technische Richtlinien von allgemeiner Bedeutung

Prüfung, Bewertung, Zertifizierung und Zulassung
- Evaluierung und Zertifizierung der Sicherheit von IT-Komponenten und -Systemen
- Zulassung von Systemen für die elektronische Verschlusssachenbearbeitung
- Abnahme- und Typmusterprüfung von IT-Sicherheitskomponenten

Akkreditierung
- Anerkennung und Qualitätssicherung von Prüfstellen und Auditoren

Spezielle Technische Messungen und Abnahmen
- Abstrahlprüfungen für Kommunikationseinrichtungen
- Prüfung und Abnahme von TK-Anlagen
- Lauschabwehrprüfungen
- Prüfungen der materiellen Sicherheit

Sichere Informationstechnik für unsere Gesellschaft

Die Abhängigkeit der Gesellschaft von der Informationstechnik (IT) wird zunehmend größer und ihr Schutz damit immer wichtiger. Diese Aufgabe übernimmt in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI). 1991 gegründet gehört das BSI zum Geschäftsbereich des Bundesministeriums des Innern. Es ist operativ für den Bund, kooperativ für die Wirtschaft und informativ für den Bürger tätig. Oberstes Ziel des BSI ist hierbei der Schutz von Information und Kommunikation. Das BSI verfolgt dabei drei strategische Ziele:

- **Prävention:** *Informationsinfrastrukturen angemessen schützen*
- **Reaktion:** *Wirkungsvoll bei IT-Vorfällen handeln*
- **Nachhaltigkeit:** *IT-Sicherheitstechnologie und -kompetenz fördern*

Wer sind wir?
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist der zentrale IT-Sicherheitsdienstleister des Bundes. Wir sind für IT-Sicherheit in Deutschland verantwortlich. Grundlagen unserer Arbeit sind Fachkompetenz und Neutralität.

Was wollen wir erreichen?
Unser Ziel ist der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft. Mit unserer Unterstützung soll IT-Sicherheit als wichtiges Thema wahrgenommen und eigenverantwortlich umgesetzt werden. Wir wollen bewirken, dass Sicherheitsaspekte schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden.

Wer sind unsere Kunden?
Mit unserem Angebot wenden wir uns an die Nutzer und Hersteller von Informationstechnik. Das sind heute in erster Linie öffentliche Verwaltungen in Bund, Ländern und Kommunen, aber auch Unternehmen und Privatanwender.

Was sind unsere Aufgaben?
Wir setzen uns verantwortungsvoll mit allen Fragen der IT-Sicherheit auseinander. Wir untersuchen und bewerten bestehende Sicherheitsrisiken und schätzen vorausschauend die Auswirkungen neuer Entwicklungen ab. Auf Grundlage dieses Wissens bieten wir unseren Kunden Dienstleistungen in den vier Kernbereichen Information, Beratung, Entwicklung und Zertifizierung an.

- **Information:** Wir informieren zu allen wichtigen Themen der IT-Sicherheit.
- **Beratung:** Wir beraten in Fragen der IT-Sicherheit und unterstützen Sie bei der Umsetzung geeigneter Maßnahmen.
- **Entwicklung:** Wir konzipieren und entwickeln IT-Sicherheitsanwendungen und -produkte.
- **Zertifizierung:** Wir prüfen, bewerten und zertifizieren IT-Systeme hinsichtlich ihrer Sicherheitseigenschaften. Die Zulassung von IT-Systemen für die Verarbeitung geheimer Informationen gehört ebenfalls zu unseren Aufgaben.

Wie arbeiten wir?
Im Miteinander von Spezialisten und Generalisten arbeiten wir teamorientiert und kollegial. Dabei sind die fachlichen Zuständigkeiten transparent gestaltet. Wir leben einen kooperativen Führungsstil, der durch Vertrauen und gegenseitigen Respekt getragen wird. Unsere Arbeit zeichnet sich durch Qualität, Unabhängigkeit und Dienstleistungsorientierung aus. Unsere Fachkompetenz entwickeln wir durch kontinuierliche Weiterbildung stetig fort. Mit Hilfe moderner Kommunikationstechniken tauschen wir das erworbene Wissen untereinander aus. Dadurch können wir schnell und zielgerichtet auf die ständig wachsenden Herausforderungen der IT-Sicherheit reagieren.

Was liegt vor uns?
Der Ausbau und die Sicherung des hohen Qualitätsstandards unserer Arbeit ist für uns eine permanente Herausforderung. Durch den ständigen nationalen und internationalen Austausch greifen wir neue Entwicklungen umgehend auf und bauen die IT-Sicherheit in Deutschland damit konsequent aus.
Wir werden die Zusammenarbeit auf allen Ebenen weiter verbessern und unsere eigene Arbeit noch effizienter ausrichten.
Wir wollen unsere Dienstleistungen in der Öffentlichkeit bekannter machen und unsere Kunden noch gezielter ansprechen.

15 Jahre IT-Sicherheit für unsere Gesellschaft

Liebe Mitbürgerinnen und Mitbürger,

am 1. Januar 1991 nahm das Bundesamt für Sicherheit in der Informationstechnik seine Arbeit auf. Mit der Gründung einer Fachbehörde für alle Fragen der IT-Sicherheit verfolgte die Bundesregierung schon früh das Ziel, die Etablierung der Informationstechnik durch die Gewährleistung ihrer Sicherheit in allen Bereichen der Gesellschaft nachhaltig zu fördern. Die Bedeutung, die der Informationstechnologie gegenwärtig zukommt, zeichnete sich seinerzeit jedoch allenfalls schemenhaft ab. Mittlerweile findet sich kaum noch ein Lebensbereich, der nicht auf funktionierende Informationstechnik angewiesen ist. Ob Wirtschaft, Verwaltung oder Privatnutzer – Fragen der IT-Sicherheit betreffen heute jeden.

Die Informations- und Kommunikationsgesellschaft steht vor gewaltigen Herausforderungen. Denn Vernetzung und mobile Kommunikation erleichtern nicht nur den Austausch von Informationen. Sie tragen auch Risiken für Staat und Gesellschaft in sich. Auch die für unser Zusammenleben grundlegenden Kritischen Infrastrukturen werden durch den Einsatz von Informationstechnik anfälliger für Angriffe in böser Absicht. Und so ist der Schutz der Informationstechnik eine zentrale Aufgabe der Innenpolitik, die aber nur in engem Austausch mit der Privatwirtschaft gelöst werden kann. Im Koalitionsvertrag hat sich die Bundesregierung dazu verpflichtet, einen Nationalen Plan zum Schutz der Informationsinfrastrukturen umzusetzen.

Die Innere Sicherheit unseres Landes hängt immer stärker von der Sicherheit unserer IT-Systeme ab. Deshalb werden die Arbeitsschwerpunkte des Bundesamtes für Sicherheit in der Informationstechnik in ganz besonderer Weise von der allgemeinen Sicherheitslage bestimmt. Denn es muss auf Veränderungen schnell und angemessen reagieren. Inzwischen ist das BSI nicht nur eine Sicherheitsbehörde des Bundes. Es bietet auch Dienstleistungen für die Privatwirtschaft an und entwickelt sich immer stärker zu einem Ansprechpartner für die gesamte Gesellschaft.

Ich freue mich, dem Bundesamt für Sicherheit in der Informationstechnik zu 15 Jahren hervorragender Facharbeit gratulieren zu können, und danke allen Mitarbeiterinnen und Mitarbeitern für ihren Beitrag zu diesem Erfolg.

Bonn, im April 2006

Dr. Wolfgang Schäuble, MdB
Bundesminister des Innern

Das BSI: eine operativ tätige Sicherheitsbehörde

Liebe Leserinnen und Leser,

im vergangen Jahr haben neue Gefahren wie Phishing und Bot-Netze viel Aufsehen erregt. Sie haben gezeigt, dass ungenügend geschützte IT-Systeme und mangelhaftes Wissen unangenehme Folgen haben können. Dieser Trend wird sich fortsetzen. Computerviren haben den Anfang gemacht, Dialer folgten, heute ist es Phishing und morgen wird es die Internettelefonie betreffen. Welche Gefahren in den nächsten Jahren auf uns zukommen werden, kann niemand abschätzen. Doch fest steht: Die Gefährdungen werden zunehmen. Das hat auch der Mitte des Jahres erschienene Bericht des BSI zur „Lage der IT-Sicherheit 2005“ deutlich gemacht. Auf diese Situation müssen wir alle vorbereitet sein.

Die Politik nimmt diese Aufgabe sehr ernst und hat in 2005 ein Zeichen gesetzt. Im August hat die Bundesregierung den Nationalen Plan zum Schutz der Informationsinfrastrukturen beschlossen. Darin ist festgehalten, wie die IT-Infrastrukturen geschützt werden sollen, die das öffentliche Leben aufrecht erhalten.

Kooperationen ausbauen und die deutsche IT-Sicherheitsindustrie stärken – so heißt der Weg zu sicheren IT-Infrastrukturen und mehr IT-Sicherheit in Deutschland. Damit verbunden ist eine deutliche Erweiterung der Aufgaben, die das BSI künftig wahrnehmen wird.

Nicht mehr nur der technische Sachverstand und die Empfehlungen des BSI werden in Zukunft gefragt sein, sondern auch die Unterstützung durch das BSI in der Praxis – informativ für den Bürger, kooperativ mit der Wirtschaft und operativ für die Verwaltung. Damit entwickelt sich das BSI zu einer operativ tätigen Sicherheitsbehörde.

Inzwischen arbeiten rund 450 Mitarbeiterinnen und Mitarbeiter im BSI. Über 60 IT-Sicherheitsexperten wurden im vergangenen Jahr neu eingestellt. Mit diesem Know-how und dem Engagement aller hat sich das BSI im Jahr 2005 seiner besonderen Verantwortung gestellt und wird dies auch weiterhin mit Erfolg tun.

Bonn, im April 2006

Dr. Udo Helmbrecht
Präsident des Bundesamtes für Sicherheit
in der Informationstechnik

1 Das BSI im Dialog mit Bürgern und Fachwelt

1.1 Internet-Sicherheit für alle

Das Thema IT-Sicherheit beherrscht nicht nur den Arbeitsplatz vor dem Computerbildschirm, sondern hält zunehmend Einzug in alltägliche Abläufe eines jeden Menschen, sei es im Auto, in der Arztpraxis oder bei einer Passkontrolle am Flughafen.

Für IT-Sicherheit zu sorgen, das bedeutet auch: für das Thema zu sensibilisieren und zielgruppengerecht darüber aufzuklären. Das BSI nimmt diese Verantwortung unter anderem durch die Bereitstellung seiner vielfältigen Informationsangebote wahr.

Die BSI-Homepage www.bsi.bund.de wendet sich in erster Linie an IT-Experten. Wie alle Internetauftritte des BSI wurde sie gemäß der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie Informationstechnik-Verordnung – BITV) vom 17. Juli 2002 gestaltet. Für die IT-Fachleute ist neben den aktuellen Warnhinweisen und den allgemeinen Informationen über das BSI besonders der umfangreiche Themenfundus interessant. Unter der Rubrik „Publikationen“ werden die meisten BSI-Veröffentlichungen in der Vollversion zum Download zur Verfügung gestellt.

Ein besonderes Merkmal: der neutrale Blickwinkel auf die Themen. Als repräsentatives Beispiel für das Jahr 2005 kann die VoIPSEC-Studie (Voice over IP) genannt werden, die sich mit Sicherheitsaspekten einer Technik auseinandersetzt, die in den vergangenen Jahren zu einer echten Alternative zur klassischen Telefonie gereift ist. *(Siehe auch Kapitel „Neue Herausforderungen: Spam, Phishing, Bot-Netze, VoIP“)*

Von der Biometrie bis zur Zertifizierung – das Internetangebot www.bsi.bund.de öffnet den Weg zu vielen Fachinformationen, Materialien, Terminhinweisen und Publikationen. Ein besonderes Angebot: der BSI-Newsletter, der fünfmal im Jahr erscheint und Informationen zu Veröffentlichungen, Veranstaltungen und aktuellen Zertifikaten enthält.

Schwerpunktthema: elektronischer Pass

Die Kernthemen des BSI wie IT-Grundschutz, Zertifizierung/Akkreditierung, Internetsicherheit und Schutz Kritischer Infrastrukturen wurden im Onlineangebot 2005 um die Schwerpunkte ePass und Biometrie ergänzt. Ausführlich werden technische Grundlagen biometrischer Verfahren und die Projekte des BSI auf diesem Gebiet dargestellt. *(Siehe auch Kapitel „Technologiefeld Biometrie“)*

Informieren, aufklären, sensibilisieren

Das Bürgerportal des BSI (www.bsi-fuerbuerger.de) ist speziell auf die Bedürfnisse von Privatnutzern zugeschnitten. Einsteiger und Fortgeschrittene finden Informationen und viele Tipps rund ums Internet und den PC. Die komplexe Thematik IT-Sicherheit wird auch für den Technik-Laien verständlich erklärt.

Thematische Schwerpunkte wie Kinderschutz oder Browser-Sicherheit setzt der monatliche „Brennpunkt“. Ganz praktische Hilfe bieten die kostenlos herunter ladbaren Schutzprogramme in der Tool-Box.

Wer regelmäßig über aktuelle Sicherheitstipps informiert werden möchte, sollte auch den 14-tägig erscheinenden Newsletter SICHER INFORMIERT abonnieren. Einfach unter www.bsi-fuer-buerger.de anmelden. Über 28.000 Nutzer nehmen dieses Angebot bereits gerne wahr und täglich kommen viele neue hinzu.

Lob für das Bürgerportal des BSI gab es 2005 reichlich. Der WDR bewertete unter mehreren Internetseiten zum Thema IT-Sicherheit die Website www.bsi-fuer-buerger.de klar mit einem „Empfehlenswert“, der zweitbesten Note auf der Skala. Die Zeitschrift „Computerbild“ erteilte in ihrer Märzausgabe die Note „sehr gut“.

Extra für die Fragen der vielen privaten Nutzer von PC und Internet eingerichtet: die Website: www.bsi-fuer-buerger.de (links). „Argus“, in der griechischen Mythologie ein Hund mit tausend Augen, ist das Symbol für dieses Internetangebot. Die CD (oben), die z.B. bei Messeauftritten des BSI erhältlich ist, informiert grundlegend über Sicherheit im World Wide Web.

So verwundert es nicht, dass sich die Bürger-CD des BSI, die den Inhalt des Bürgerportals spiegelt, auch auf dem Familientag der Beschäftigten der Airbus Deutschland GmbH in Hamburg größter Beliebtheit erfreute. Hans Werner, IT-Security Officer bei Airbus Deutschland, über das Give-away-Highlight des IT Security Stands: „Wir möchten das Angebot des BSI für Bürger nutzen, um unsere Mitarbeiter und ihre Familien für das wichtige Thema der IT-Sicherheit zu sensibilisieren.“

Eine ähnlich starke Nachfrage erlebten die Mitarbeiter des BSI am Tag der Offenen Tür der Bundesregierung im Bundesministerium des Innern. Die drängendsten Fragen der Besucher des BSI-Standes drehten sich um Schadprogramme und Datensicherheit.

Umlagert – der Stand des BSI beim Tag der Offenen Tür der Bundesregierung im Bundesministerium des Innern (BMI) stieß auf großes Interesse der Besucher.

Girls' Day

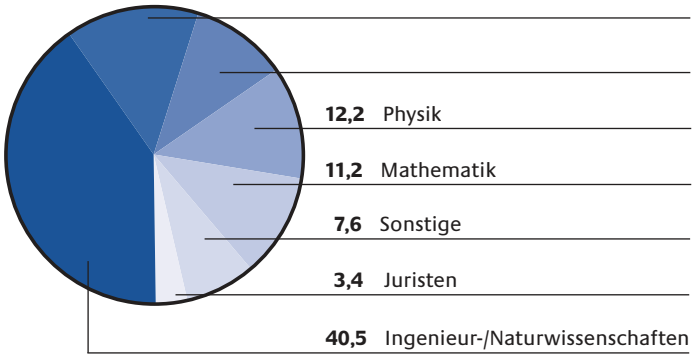
Am bundesweiten Mädchen-Zukunftstag, dem sogenannten „Girls' Day" (28.4.2005), hatten Schülerinnen aus dem Raum Bonn Gelegenheit, das BSI kennen zu lernen. Zahlreiche Schülerinnen nutzten die Möglichkeit, eine Sicherheitsbehörde von innen zu sehen.

BSI im Gespräch

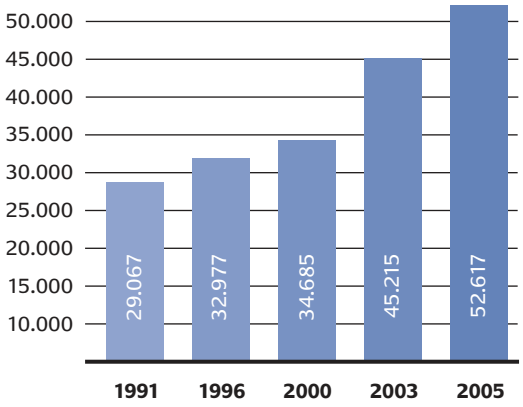
Ein Angebot, das sich an Entscheider in Wirtschaft, Verwaltung und Wissenschaft wendet, ist „BSI im Gespräch". In Berlin diskutierten die Teilnehmer des Events im kleinen Kreis das Thema „IT-Sicherheit im Fahrzeug". Ziel der Veranstaltung „BSI im Gespräch" ist es, mit hochrangigen Repräsentanten eines Sachgebiets einen meinungsbildenden Dialog anzustoßen, der absehbare Zukunftsthemen umreißt.

Drei Beispiele für kompetente Fachinformationswerke aus dem BSI: Die abgebildeten Publikationen sind über den Bundesanzeiger-Verlag (Postfach 10 05 34, D-50445 Köln, Fax: 0221-97 66 82 78, E-Mail: vertrieb@bundesanzeiger.de) erhältlich. Die Sammlung „E-Goverment-Handbuch" kostet 98 Euro, „IT-Sicherheitsmanagement und IT-Grundschutz" ist zum Preis von 39,80 Euro erhältlich und das Standardwerk zur IT-Sicherheit „IT-Grundschutzkataloge" (früher: „IT-Grundschutzhandbuch") kostet 152 Euro.

Fachrichtungen im BSI
nur höherer und gehobener Dienst, in Prozent



Haushaltszahlen 1991 bis 2005
in Tausend Euro



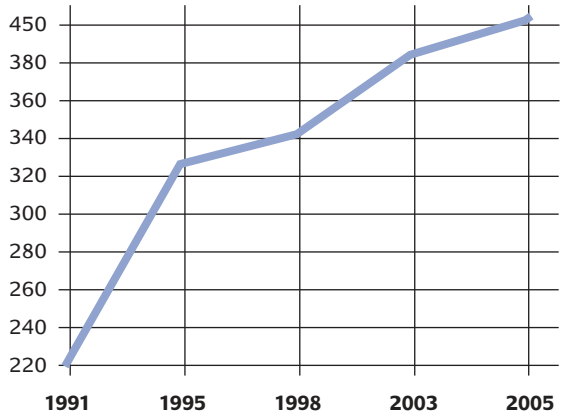
1.2 Das BSI: Status quo und Ausblick

Seit 15 Jahren setzt sich das BSI nachhaltig für sichere Informationstechnik in Deutschland ein. Dabei hat sich die Behörde mit Sitz in Bonn, die dem Geschäftsbereich des Bundesministeriums des Innern zugeordnet ist, stetig fortentwickelt. Im Jahre 2005 fiel der Startschuss für eine neue operative Ausrichtung. Das BSI soll weitere Aufgaben übernehmen.

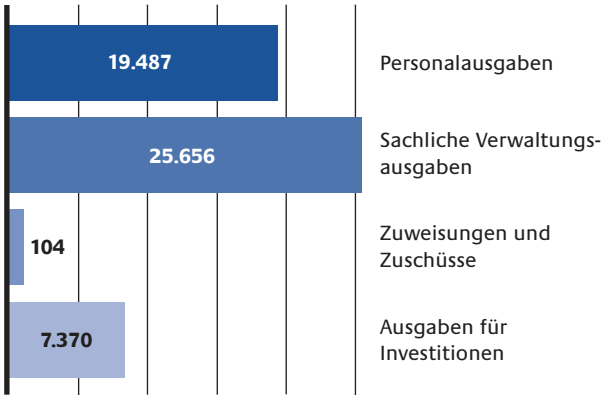
Das BSI in Zahlen

Der Gesamthaushalt des BSI erreichte im Jahr 2005 ein Volumen von 52,62 Mio Euro. Gegenüber dem Vorjahreszeitraum entsprach dies einem Zuwachs von 2,9 Prozent. Auf Personalausgaben entfielen 19,49 Mio Euro. Die Ausgaben für Investitionen betrugen 7,37 Mio Euro. Zusammen mit den im Jahre 2005 neu geschaffenen 35 Stellen arbeiten im BSI nunmehr insgesamt 450 Mitarbeiterinnen und Mitarbeiter. Neben den Naturwissenschaftlern, die nach wie vor die größte Gruppe darstellen, ist entsprechend dem breiten Aufgabenspektrum des BSI auch die Arbeit von Juristen, Verwaltungs-, Wirtschafts- und Sozialwissenschaftlern unverzichtbar. Denn so vielfältig das Thema IT-Sicherheit ist, so vielfältig sind auch die fachlichen Perspektiven, aus denen heraus es betrachtet werden muss. Eine Entwicklung, die mit dem technischen Fortschritt und dem Einzug des Themas IT-Sicherheit in den Alltag der Menschen weiter voran geschritten ist. Die Mitarbeiter des BSI überraschte es wenig, dass ihr Haus im „Absolventenbarometer 2005 – IT Edition“ der Unternehmensberatung trendence als Top-Arbeitsgeber eingestuft wurde. Das BSI erreichte Platz 8 von insgesamt 105 Unternehmen. Damit zählt die Fachbehörde zu den beliebtesten Arbeitgebern unter examensnahen Studierenden der IT-Branche und rangiert somit auf der gleichen Ebene mit Firmen wie Siemens, IBM und Microsoft.

Mitarbeiterzahlen 1991 bis 2005



Ausgaben nach Sachgebieten 2005
in Tausend Euro



Neue operative Ausrichtung

Mit seiner Eröffnungsrede zum 9. Deutschen IT-Sicherheitskongress *(siehe auch Kapitel „Fachmessen und Kongresse“)* gab der ehemalige Bundesinnenminister Otto Schily am 10. Mai 2005 den Startschuss für die neue Ausrichtung, mit der das Amt zusätzliche Aufgaben innerhalb der Bundesverwaltung übernimmt. Schily betonte, das Bewusstsein für die große Bedeutung der IT-Sicherheit müsse in gleichem Maße wachsen, wie sich immer mehr Bereiche in Wirtschaft und Gesellschaft auf IT stützten. Primäres Ziel des stärkeren Engagements des BSI ist es, Informationsinfrastrukturen angemessen zu schützen und wirkungsvoll bei IT-Sicherheitsvorfällen zu handeln: kooperativ mit der Wirtschaft, informativ für den Bürger und operativ für die Verwaltung. Gerade auf Bundesebene richten sich die Anstrengungen des BSI darauf, mit gutem Beispiel voranzugehen und eine Stärkung des Bewusstseins für IT-Sicherheit zu forcieren. Mit dem „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ (NPSI) hat die Bundesregierung im Juli 2005 eine umfassende IT-Sicherheitsstrategie für Deutschland beschlossen. *(Siehe auch Kapitel „Lagebericht IT-Sicherheit 2005“)* Für die Umsetzung des NPSI ist das BSI als nationale IT-Sicherheitsbehörde und zentraler IT-Sicherheitsdienstleister von entscheidender Bedeutung.

Zentrale Anlaufstelle: CERT-Bund

Bereits heute ist das Computer-Emergency-Response-Team des Bundes (CERT-Bund – www.bsi.bund.de/certbund) bei sicherheitsrelevanten Vorfällen in IT-Systemen der Bundesverwaltung die zentrale Anlaufstelle. Zu seinen Aufgaben zählen unter anderem der präventive Hinweis auf Schwachstellen in Hardware- und Softwareprodukten, die Warnung und Alarmierung bei besonderen IT-Bedrohungslagen und die Empfehlung von reaktiven Maßnahmen zur Schadensbegrenzung oder -beseitigung. CERT-Bund steht in erster Linie den Bundesbehörden zur Verfügung. Zu seinen Dienstleistungen gehört auch eine 24-Stunden-Rufbereitschaft, die bei akuten IT-Gefährdungen der Bundesverwaltung greift. Anfragen von anderen Behörden sowie Privatpersonen oder privaten Institutionen werden im Rahmen verfügbarer Ressourcen bearbeitet.

1.3 Fachmessen und Kongresse

Messeveranstaltungen und Fachkongresse bieten dem BSI immer wieder Gelegenheit, mit IT-Experten aber auch Privatnutzern Kontakt aufzunehmen. Informationsangebote zu platzieren, Produkte des eigenen Hauses zu präsentieren und schließlich in puncto IT-Sicherheitsfragen aufzuklären und zu sensibilisieren – das sind die Ziele des BSI.

Das „Who-is-Who" der deutschen IT-Sicherheitsszene traf sich 2005 beim 9. Deutschen IT-Sicherheitskongress des BSI vom 10. bis 12. Mai in Bonn-Bad Godesberg. Unter dem Motto „IT-Sicherheit geht alle an" traten rund 500 Experten aus Wirtschaft, Wissenschaft und Verwaltung drei Tage lang in den Dialog und diskutierten aktuelle Themen der IT-Sicherheit.

Der damalige Bundesinnenminister Otto Schily betonte in seiner Eröffnungsrede die Bedeutung eines stärkeren öffentlichen Bewusstseins für das Thema IT-Sicherheit und unterstrich den effektiven Anteil, den das BSI bereits heute leiste. Schwerpunkte der über 30 Programmbeiträge waren unter anderem biometrische Verfahren und die neuen EU-Reisepässe sowie die elektronische Gesundheitskarte. Traditionell begleitet wurde der Kongress durch eine Ausstellung im Foyer. In diesem Jahr standen bei den ausgestellten Produkten und Dienstleistungen kryptografische Lösungen im Vordergrund. Bei der abschließenden Podiumsdiskussion zum Thema „Biometrie – eine neue Bürgertechnologie" hatten die Kongressteilnehmer Gelegenheit zu einem konstruktiven Austausch ihrer Positionen.

Präsent auf der CeBIT

Auf der CeBIT 2005 (10. bis 16. März, Hannover) befand sich der Messestand des BSI erstmals in Halle 7, der IT-Security Area. Reges Interesse beim Messepublikum fanden besonders das Golden Reader Tool (GRT), die Sichere Inter-Netzwerkarchitektur (SINA), IT-Grundschutz und die IT-Sicherheitszertifizierung nach Common Criteria (CC). Stark nachgefragt wurde auch die CD-ROM, die alle Informationen der BSI-Internetseiten enthält. Im Public-Sector-Parc der Halle 9 präsentierte sich das BSI mit Informationen zu CERT-Bund und zur Virtuellen Poststelle. Auf großes Interesse stießen die Vortragsreihen von BSI-Experten im Convention Center und auf dem Forum E-Government.

Bei der größten Computermesse der Welt, der CeBIT in Hannover, ist das BSI in jedem Jahr mit einem repräsentativen Stand vertreten.

Gut gefüllt – der 9. Deutsche Sicherheitskongress des BSI im Mai 2005 stieß auf großes Interesse in der Fachöffentlichkeit. Rechts: Blick in den Großen Saal der Godesberger Stadthalle. Ein Tagungsband ist beim SecuMedia Verlag zum Preis von 49,10 Euro zuzüglich Versand erhältlich (ISBN 3-922746-95-3, 368 Seiten oder via http://buchshop.secumedia.de).

Der „Deutsche IT-Sicherheitspreis“ auf der „Systems“

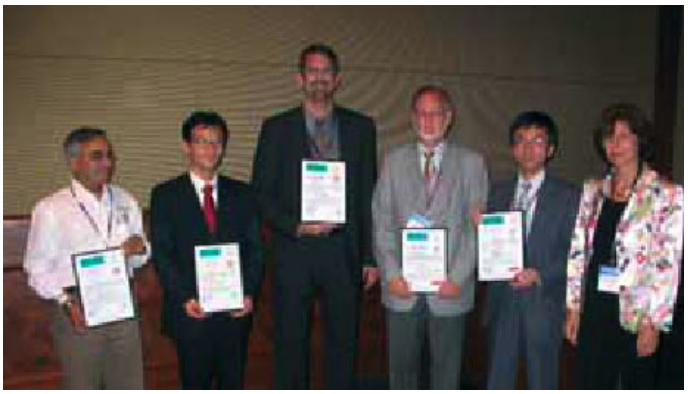
Seit mehreren Jahren unterstützt das BSI als ideeller Träger der IT-Security Area die Fachmesse „Systems“ (24. bis 28. Oktober in München). Neben dem Messestand war das BSI mit einem umfangreichen Vortragsprogramm präsent. Themen waren zum Beispiel SINA, das Golden Reader Tool, die Basis für interoperable elektronische Reisepässe, und das Computer Emergency Response Team.

Ein Novum auf der Messe: Im Forum Blau wurde der „Deutsche IT-Sicherheitspreis“ ausgelobt. Der hochdotierte Preis, dessen Schirmherr Dr. Udo Helmbrecht ist, wird von der Horst-Görtz-Stiftung verliehen und 2006 erstmals vergeben. Ziel ist es, einen Beitrag zur Stärkung der Innovationskraft der deutschen Wirtschaft zu prämiieren.

BSI-Präsident Dr. Udo Helmbrecht zusammen mit Horst Görtz, Gründer der Horst-Görtz-Stiftung

Moderner Staat

Aktuelle Arbeiten des BSI spielten auf dem Kongress „Moderner Staat“ vom 29. bis 30. November in Berlin eine tragende Rolle. Das BSI war als „Partner IT-Sicherheit“ mit einem Messestand und einer 90-minütigen Vortragsveranstaltung vertreten. Die interessierten Zuhörer ließen sich von Mitarbeitern des BSI zu den Themen Virtuelle Poststelle (VPS), IT-Grundschutz und Zertifizierung sowie geprüfte IT-Sicherheit informieren.



ICCC-Konferenz, September 2005, Tokio. BSI-Zertifikate gingen u.a. an Sony, Sharp, Infineon, Philips, Microsoft und Novell.

Auch international präsent

Auf internationalem Parkett konnte das BSI seine Themen im Jahre 2005 besonders bei der International Common Criteria Conference (ICCC), die vom 28. bis 29. September in Tokio stattfand, sowie bei der Information Security Solutions Europe (ISSE, 27. bis 29. September) in Budapest platzieren. Auf der sechsten ICCC war das BSI mit einem Informationsstand vertreten, um die mehr als 500 Besucher über seine Zertifizierungsstelle zu informieren. Wieder nutzte das BSI die ICCC, um Zertifikate offiziell an mehrere Hersteller, darunter Sony Corporation, Sharp Corporation, Infineon Technologies AG, Phillips Semiconductors GmbH, Microsoft Corporation und Novell-SUSE LINUX Products GmbH (Sponsor IBM), zu überreichen.

1.4 Kommunikation und Kooperation

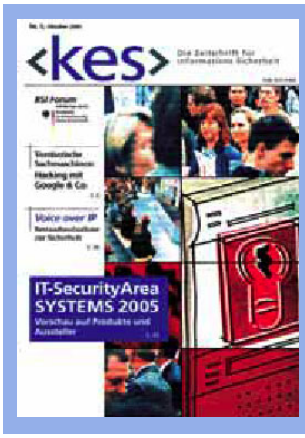
Das BSI nutzt viele Wege, um seine Sicherheitshinweise und Fachthemen in der Öffentlichkeit bekannt zu machen. Sein nachhaltiger Einsatz als kompetente und wirtschaftlich unabhängige Instanz ist ein wichtiger Beitrag zu einer Stärkung der Sicherheitskultur in der Informationstechnik.

Der erste „Lagebericht IT-Sicherheit“, der Erkenntnisse und Erfahrungen des BSI bündelt und auf die derzeit größten Bedrohungen hinweist, ist ein herausragender Beleg für diese Arbeit. *(Siehe auch Kapitel „Lagebericht IT-Sicherheit 2005“)*

Die Partnerschaft ist beschlossen und besiegelt. BSI-Präsident Dr. Udo Helmbrecht (rechts) mit York von Heimburg, dem Vorstand der IDG Communications Verlag AG.

Einen ebenso wichtigen Beitrag für eine „Kultur der Sicherheit“ leisten die Kooperationspartner des BSI. Neben bestehenden Kooperationen, wie mit dem Heise-Sicherheitsportal, dem Internetportal www.freenet.de oder Fujitsu Siemens Computers, bietet seit Mai 2005 das „Webzine“ tecCHANNEL einen Kommunikationskanal für aktuelle Informationen aus dem BSI. Diese Zusammenarbeit bekräftigte BSI-Präsident Dr. Udo Helmbrecht bei einem Treffen mit dem Vorstand der IDG Communications Verlag AG, York von Heimburg, auf dem 9. Deutschen IT-Sicherheitskongress.

Durch die Kooperation mit dem deutschen Partner des „Safer Internet“-Programms der EU, dem Internetportal „klicksafe“ (www.klicksafe.de), unterstützt das BSI eine nationale Sensibilisierungskampagne zur Förderung der Medienkompetenz im Internet. Das BSI stellt den Projektbetreibern aktuelle Informationen zu Fragen der Internetsicherheit zur Verfügung.



<kes>: IT-Sicherheit auf hohem Niveau

Das BSI-Forum in der <kes> ist das offizielle Verlautbarungsorgan des BSI (auch elektronisch auf www.bsi.bund.de verfügbar). Das Forum erscheint als Teil der sechs Mal jährlich publizierten <kes>, der führenden Zeitschrift für Informationssicherheit. Es enthält aktuelle Fachbeiträge rund um das Thema IT-Sicherheit und wendet sich in erster Linie an IT-Experten.
Wer sich eingehender mit aktuellen Themen wie E-Government oder IT-Grundschutz beschäftigen möchte, findet diese in der BSI-Schriftenreihe, die im Bundesanzeiger Verlag erscheint, anspruchsvoll aufbereitet. *(Siehe auch Kapitel „Internet-Sicherheit für alle“)*

1.5 Bündnis für elektronische Signaturen

Bereits im Jahre 1997 hat der Gesetzgeber mit der Verabschiedung des Signaturgesetzes erstmals die Voraussetzungen für den Einsatz rechtsverbindlicher elektronischer Signaturen geschaffen. Auf Initiative der Bundesregierung hat sich am 3. April 2003 in Berlin das Signaturbündnis konstituiert. Sein Ziel: diesem für Wirtschaft und Staat wichtigen Thema neue Impulse zu geben.

Das BSI war von Anfang an eng in alle technischen Arbeitsgruppen des Signaturbündnisses eingebunden. Ziel war die Schaffung einer stabilen Grundlage für interoperable Infrastrukturen auf der Basis gemeinsam akzeptierter Standards. Die im Ergebnis erarbeiteten Signaturbündnis-Spezifikationen finden u.a. Beachtung bei der Umsetzung der Chipkartenprojekte der Bundesregierung (eCard-Strategie). Auch hat die im Signaturbündnis vertretene Privatwirtschaft die Einhaltung der Signaturbündnis-Spezifikationen zugesagt. Im Jahr 2005 übernahm das BSI zusätzlich die Aufgaben einer Geschäftsstelle des Signaturbündnisses.

Partner aus der Wirtschaft

Bis Ende 2005 traten dem Signaturbündnis, zu dessen Gründungsmitgliedern u.a. das Bundesministerium des Innern (BMI), das Bundesministerium für Wirtschaft und Arbeit (BMWA), das Bundesministerium der Finanzen (BMF) sowie namhafte Partner aus Wirtschaft und Industrie gehören, weitere 36 Mitglieder bei. Damit sind Ende 2005 ca. 50 Mitglieder im Signaturbündnis vertreten.

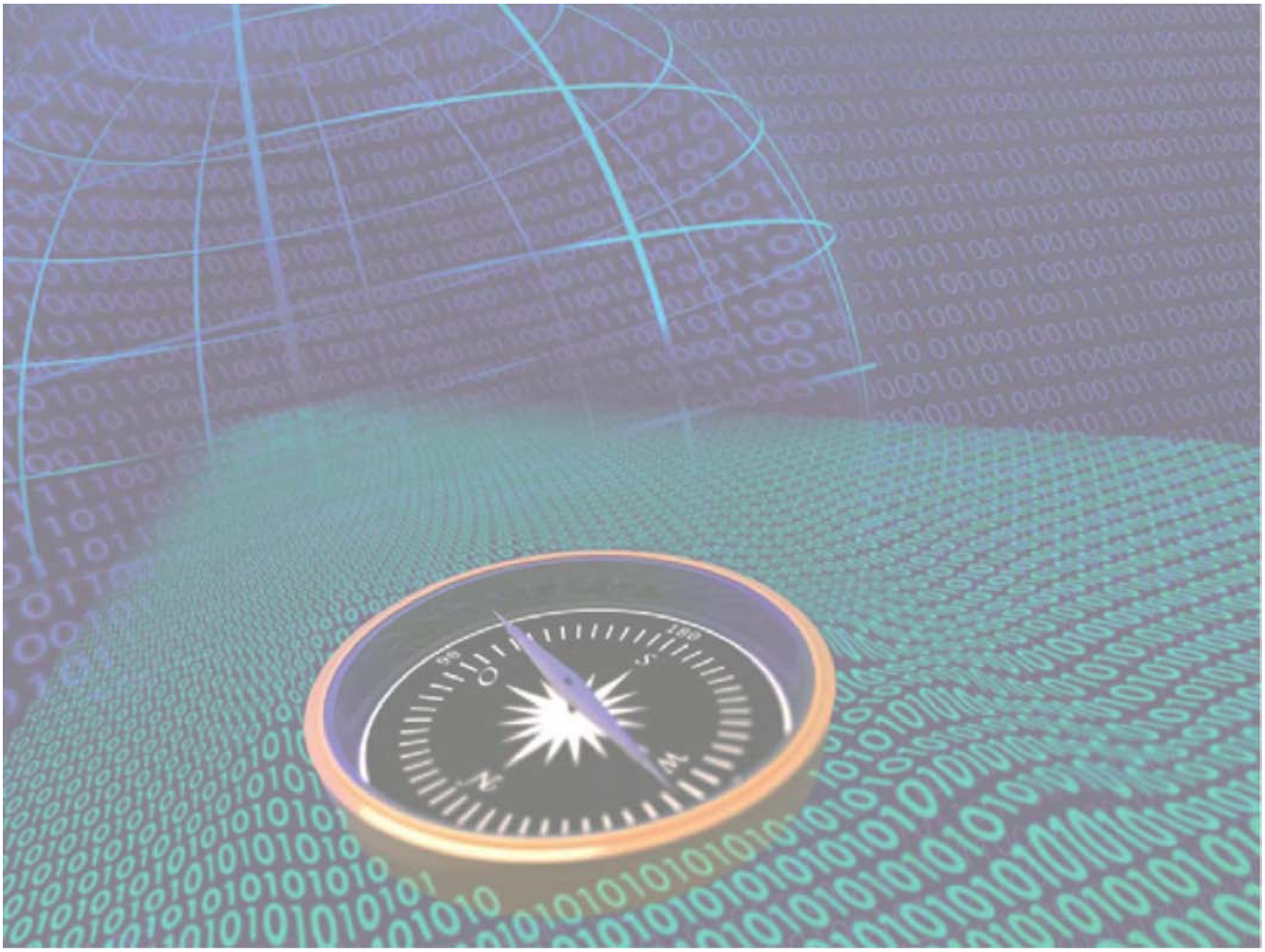
Die Vision des Bündnisses ist einfach: Der Bürger soll mit jeder beliebigen Chipkarte und jedem Kartenleser eine Vielzahl von – idealerweise alle – verfügbaren Anwendungen im Bereich eCommerce und eGovernment nutzen können.

Um diese Vision Realität werden zu lassen, setzt das Signaturbündnis auf Netzwerkeffekte durch die Einbindung vorhandener Karteninfrastrukturen, ausgereifte eCommerce/ eBusiness-Anwendungen sowie einen intensiven Dialog zwischen Staat und Wirtschaft.

Internationale Standards

Hauptanliegen des BSI war es, die 2003 zwischen den Mitgliedern vereinbarten Konvergenzziele bis Ende 2005 zu erreichen – bis auf die Klärung weniger Detailfragen konnte dies auch verwirklicht werden.

Um die gemeinsame Arbeit zu sichern und technische, rechtliche und wirtschaftliche Rahmenbedingungen zu optimieren, haben sich die Mitglieder des Signaturbündnisses im Dezember 2005 mit der Frage der inhaltlichen und organisatorischen Neuausrichtung des Signaturbündnisses befasst. Kommende Schwerpunkte aus der Sicht des BSI sind dabei die Aufstellung von Regeln zur Zertifizierung bündniskonformer Produkte, die internationale Standardisierung sowie die Tätigkeit des BSI als Geschäftsstelle des Signaturbündnisses.



2 Sicherheit aktiv gestalten – Service für Unternehmen und Verwaltung

2.1 Lagebericht It-Sicherheit 2005

Informationstechnik ermöglicht nicht nur neue und effizientere Dienstleistungen, sie bringt leider auch neue Gefährdungen mit sich. Der Bericht des BSI „Die Lage der IT-Sicherheit in Deutschland 2005“ stellt dies sehr eindringlich dar. Damit die Informationstechnik auch weiterhin ein verlässliches Arbeitsmittel bleibt, müssen rechtzeitig wirksame Sicherheitsmaßnahmen ergriffen werden.

Der BSI-Bericht „Die Lage der IT-Sicherheit in Deutschland 2005“ macht den Ernst der Situation deutlich: In der zweiten Jahreshälfte 2004 wurden mehr als 1.400 neue IT-Schwachstellen entdeckt – ein Anstieg von 13 Prozent im Vergleich zum ersten Halbjahr. Noch dramatischer sieht die Lage bei den IT-Schädlingen aus. Mehr als 7.300 neue Wurm- und Virenvarianten wurden im gleichen Zeitraum registriert. Das entspricht einem Anstieg von rund zwei Dritteln gegenüber dem ersten Halbjahr. Trojanische Pferde machten ein Drittel der 50 häufigsten Internetschädlinge im zweiten Halbjahr 2004 aus. Der Anteil von Spamnachrichten beträgt inzwischen 60 bis 90 Prozent am gesamten E-Mail-Verkehr. Auch die zunehmenden Phishing-Attacken gefährden die Sicherheit des Internets.

Der BSI-Lagebericht IT-Sicherheit 2005 stellt die aktuelle Lage der IT-Sicherheit in Deutschland dar und gibt einen Überblick über die anstehenden Herausforderungen. Der Lagebericht ist in Deutsch und Englisch von der Website des BSI als pdf-Dokument downloadbar.

Deutschland 2005: Wie sicher ist die Informationstechnik?

BSI-Präsident Dr. Udo Helmbrecht rief bei der Präsentation des Lageberichtes am 18.08.2005 in Berlin zu mehr Wachsamkeit auf: „Auch wenn der Schutz unserer IT-Systeme heute gewährleistet ist, müssen wir uns für die Zukunft noch besser wappnen.“ So hat bisher nur rund die Hälfte der IT-Verantwortlichen in Unternehmen eine schriftlich fixierte Strategie zum Schutz der Informationstechnik. Trotz des hohen Spamaufkommens sind Antispam-Maßnahmen in Unternehmen und Verwaltung in Deutschland noch nicht flächendeckend realisiert. Mindestens neun Prozent der Organisationen sind der Spamflut ungeschützt ausgesetzt. *(Siehe auch Kapitel „Neue Herausforderungen: Spam, Phishing, Bot-Netze, VoIP“)*

Die Angreifer werden immer schneller. Der Zeitraum zwischen dem Bekanntwerden und dem Ausnutzen einer Schwachstelle (Exploit) liegt derzeit bei 6,4 Tagen und wird weiter sinken – bis hin zu Zero-Day-Exploits. Es zeichnet sich darüber hinaus ein Trend hin zur Professionalisierung und Kommerzialisierung der Internetkriminalität ab. Statt isolierter Computerhacker steht hinter gezielten Angriffen vermehrt die organisierte Kriminalität. Hacker und Virenautoren arbeiten mit Kriminellen zusammen. Finanzielle Interessen sind dabei die ausschlaggebende Antriebskraft.

IT-Sicherheit braucht höheren Stellenwert

Dabei ist die IT-Sicherheitskompetenz in den gesellschaftlichen Gruppen wenig ausgeprägt. Obwohl Bürgerinnen und Bürger zunehmend von Informationstechnik abhängen – sei es am Arbeitsplatz, beim digitalen Zahlungsverkehr oder in der Kommunikation – räumen nur wenige sicherer Informationstechnik in der Praxis den erforderlichen Stellenwert ein. Ähnliches gilt für Wirtschaft und Verwaltung. Die Darstellung der momentanen Lage zeigt, dass es gute Gründe gibt, der IT-Sicherheit einen hohen Stellenwert zuzuschreiben. Doch es gilt auch künftig, vermehrt auftretende Gefahren im Blick zu behalten. Das zielgerichtete Ausnutzen von Schwachstellen in IT-Systemen ist dabei ein zentrales Problemfeld.

Welche Motivationen können bei solchen Angriffen ausschlaggebend sein? In einer Welt der zunehmenden Vernetzung globaler Märkte erfährt die Sicherheit ihrer IT-Systeme für Wirtschaftsunternehmen große Bedeutung. Das Ausspionieren von Ausschreibungen, Verträgen oder Preisinformationen zur Erzielung von Wettbewerbsvorteilen der Konkurrenz aus In- und Ausland wird zunehmen. Angriffe auf IT-Systeme hatten im vergangenen Jahr einen zunehmend wirtschaftlichen Hintergrund. Ziel war vor allem das Ausspionieren von Kreditkarteninformationen und anderen sensitiven Finanzdaten. Für die Zukunft ist anzunehmen, dass sich diese Entwicklung weiter verstärkt. Verwendeten Programmierer von Schadsoftware bislang vor allem englischsprachige E-Mails, um Computerwürmer zu verbreiten, so sind inzwischen vermehrt deutschsprachige Texte zu finden. Diese Regionalisierung führt zu einer wachsenden Verbreitung solcher Schadprogramme auch in Deutschland.

Der Lagebericht des BSI verweist auf Schwachstellen und Bedrohungen, er zeigt Trends auf und bewertet Entwicklungen. Doch das BSI will nicht nur den Status quo beschreiben. Es geht auch darum zu zeigen, welche Möglichkeiten es gibt, um die Sicherheit der IT nachhaltig zu verbessern. Deshalb stellt der Bericht dar, welche Aktivitäten sich eignen, damit Schwachstellen und Bedrohungen von IT-Systemen zukünftig keine noch größeren Probleme darstellen, als sie es heute schon sind. Nur mit einer neuen, von allen Gruppen gemeinsam getragenen Sicherheitskultur lassen sich die Rahmenbedingungen für sichere und zuverlässige Informationstechnik entscheidend verbessern. Deshalb hat die Bundesregierung den Nationalen Plan zum Schutz der Informationsinfrastrukturen initiiert. Das BSI wird als zentrale deutsche IT-Sicherheitsbehörde dazu einen wesentlichen Beitrag leisten.

Plan zum Schutz der Informationsinfrastrukturen

Ein angemessenes Maß an IT-Sicherheit erreicht man nur mit durchdachten und umfassenden Konzepten, nicht mit isolierten Einzelmaßnahmen. Was für Unternehmen und Behörden gilt, lässt sich auch auf die gesamte Nation übertragen. Deshalb hat die Bundesregierung eine IT-Sicherheitsstrategie für Deutschland – den Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) – beschlossen. Dieser wurde unter Federführung des Bundesministerium des Innern unter enger Mitwirkung des BSI erstellt.

Sicherheit fängt im Alltag an – Tipps zum Schutz vor Betrug und Manipulation am Geldautomaten hält das BSI auf seiner Website bereit: www.bsi-fuer-buerger.de/geld/10_04.htm

Der NPSI verfolgt drei strategische Ziele:

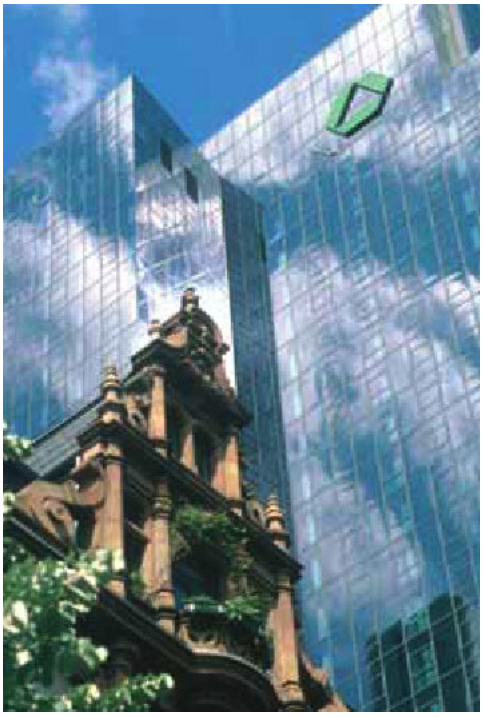
1. Prävention: Informationsinfrastrukturen angemessen schützen
Wie schützt man Informationsinfrastrukturen angemessen vor Gefahren und Angriffen? Hier geht es um Handlungsfelder von der Sensibilisierung der Mitarbeiter über den Einsatz sicherer Produkte bis hin zur kryptografischen Absicherung von IT-Netzen.

2. Reaktion: Wirkungsvoll bei IT-Sicherheitsvorfällen handeln
Zur effizienten Reaktion werden vor allem zwei Dinge benötigt: Ein korrektes und gut aufbereitetes Lagebild und durchdachte und eingeübte Krisenreaktionskonzepte sowie Notfallpläne. Das gilt sowohl für Unternehmen und Behörden, als auch auf nationaler Ebene.

3. Nachhaltigkeit: Deutsche IT-Sicherheitskompetenz stärken – international Standards setzen
Deutschland benötigt neben dem politischen Willen und der Bereitschaft aller Verantwortlichen zur Stärkung der IT-Sicherheit Fachkompetenz sowie vertrauenswürdige Dienstleistungen und IT-Sicherheitsprodukte. Dies beinhaltet auch die Vermittlung von IT-Sicherheitskompetenz in Schule und Ausbildung sowie die Förderung von Forschung und Entwicklung in diesen Bereichen. Gemeinsam mit europäischen Partnern werden vertrauenswürdige IT-Sicherheitslösungen entwickelt. Das BSI wird dabei als nationale IT-Sicherheitsbehörde die IT-Sicherheit aktiv mitgestalten.

Diese strategischen Ziele werden durch 15 Einzelziele für die verschiedenen gesellschaftlichen Gruppen, von Verwaltung und Wirtschaft über Wissenschaft und Medien bis hin zu den Bürgerinnen und Bürgern konkretisiert und im Rahmen von Umsetzungsplänen, zunächst für die Bundesverwaltung und für die privatwirtschaftlichen Betreiber Kritischer Infrastrukturen, mit Leben gefüllt. Das BSI ist intensiv in die Um-

setzung des NPSI eingebunden. Dabei wird es seine Beratungsleistungen für Behörden weiter ausbauen und aktiv an der Gestaltung der IT-Sicherheit in Behörden und Großvorhaben des Bundes mitwirken. Das Lagezentrum des BSI wird zu dem Krisenreaktionszentrum IT des Bundes ausgebaut, ein Frühwarnsystem für IT-Sicherheitsvorfälle ist in der Entwicklung. *(Siehe Kapitel „Krisenmanagement: erkennen, reagieren, schützen“)*
Zur Vermeidung und zur schnellen Beherrschung von IT-Krisen verstärkt das BSI die Zusammenarbeit mit den Betreibern Kritischer Infrastrukturen.



Kritische Infrastrukturen: auch Geldinstitute gehören dazu. Richtlinien und Materialen für die IT-Sicherheit von Banken sind beim BSI zu bekommen.

Konkrete Hilfen für Betreiber Kritischer Infrastrukturen

Im Rahmen seiner Arbeiten zum Schutz der Informationsinfrastrukturen hat das BSI 2005 bereits konkrete Hilfsmittel für Unternehmen, die zu den Kritischen Infrastrukturen zählen, veröffentlicht. Zwei dieser Hilfsmittel sind die Beispielrichtlinie „IT-Sicherheit im KRITIS-Unternehmen“ sowie „Audit-Materialien zum Standort-Kurzcheck in Kritischen Infrastrukturen“. Die Beispielrichtlinie ist das Resultat der Zusammenarbeit mit einem international operierenden Unternehmen aus der Mineralölbranche. Die von dem Unternehmen in der Praxis angewandte IT-Sicherheits-Richtlinie wurde durch das BSI überarbeitet und mit dem Grundschutzhandbuch des BSI abgeglichen. Sie bietet nun jedem Unternehmen die Möglichkeit, die Effektivität seiner eigenen IT-Sicherheitsmaßnahmen zu prüfen und gegebenenfalls anzupassen und damit zu verbessern. Ausgehend von den guten Erfahrungen des Unternehmens, mit dem die Beispielrichtlinie erstellt wurde, bietet das BSI auf Basis der Regeln der Beispielrichtlinie Audit-Materialien für einen so genannten Standort-Sicherheitscheck an. Sie sollen dabei helfen, die Umsetzung der Beispielrichtlinie zu überprüfen und den Status der IT-Sicherheit im Unternehmen transparent darzustellen. Indem das BSI die Hilfsmittel auch in englischer Sprache zur Verfügung stellt, wird den speziellen Belangen international agierender Unternehmen aus dem Bereich der Kritischen Infrastrukturen gezielt Rechnung getragen.

2.2 Krisenmanagement: Erkennen, reagieren, schützen

Trotz effizienter Schutzmaßnahmen sind IT-Sicherheitsvorfälle nicht immer zu vermeiden. Insbesondere, wenn eine große Anzahl von Institutionen betroffen ist oder lokal begrenzte Ursachen weitreichende Folgeschäden verursachen, gelten bestimmte Verhaltensregeln für ein IT-Krisenreaktionszentrum.

Ein IT-Krisenreaktionszentrum muss bei einer „Nationalen Krise“ im Bereich Informationssicherheit oder einer ähnlich weit reichenden Störung

- diese frühzeitig erkennen,
- noch nicht betroffene Nutzer rechtzeitig warnen oder sogar alarmieren,
- durch abgestimmte und eingeübte Reaktionen den Schaden möglichst minimieren
- und schnell wieder in den sicheren Regelbetrieb übergehen können.

Bei IT-Sicherheitsvorfällen von nationaler Bedeutung ist durch aufbereitete Informationen und kompetente Analysen die Entscheidungs- und Handlungsfähigkeit der Bundesregierung sicherzustellen. Dabei sind IT-Verantwortliche in Behörden und Wirtschaft zu unterstützen.

Das ist Aufgabe des sich im Aufbau befindlichen Nationalen IT-Krisenreaktionszentrums des Bundes beim BMI. Es wertet eingehende Meldungen über IT-Sicherheitsvorfälle aus, informiert und warnt verschiedene Zielgruppen (Bundesverwaltung, Wirtschaft, Bürger) und koordiniert technische Maßnahmen zur Bewältigung des Vorfalls. Bei größeren IT-Krisen wird das Lagezentrum sofort personell verstärkt und zum IT-Krisenreaktionszentrum des Bundes erweitert. Das BSI alarmiert dann auch das übergeordnete „Koordinierungsgremium IT-Sicherheit“ im BMI und versorgt es mit fachkompetent aufbereiteten und zielführenden Informationen. Dieses Gremium trifft Maßnahmen, die außerhalb der eigentlichen fachlichen Zuständigkeit des BSI liegen.

Das Lagezentrum

Der erste Schritt zum IT-Krisenreaktionszentrum war die Einrichtung des Lage- und Analysezentrums beim BSI, das an sieben Tagen acht Stunden täglich besetzt und aktiv im Einsatz ist. Damit ist eine Voraussetzung geschaffen, dass Vorzeichen auf IT-Angriffe und IT-Vorfälle auch an Wochenenden und Feiertagen rechtzeitig erkannt werden. Mit der Entwicklung von speziellen technischen Sensoren für die Erkennung von Anomalien im Internetdatenverkehr und weiteren Projekten zur Einbindung von Wirtschaft und Verwaltung in ein Nationales Frühwarnsystem ist der Grundstock zum Nationalen IT-Krisenreaktionszentrum gelegt. Der weitere Ausbau wird so zügig wie möglich vorangetrieben.

Das BSI selbst hat eine Reihe von Projekten zur Informationsgewinnung, Frühwarnung und Alarmierung entwickelt sowie die Erstellung von Tools unterstützt. Sie bilden integrale Bestandteile der Krisenreaktion. Mit seinen Erfahrungen und den entwickelten Tools ist das BSI auf die Aufgabe eines nationalen IT-Krisenreaktionszentrums des Bundes bestens vorbereitet.

Insbesondere sind zu nennen:

▸ SIRIOS – Trouble-Ticket-System zur Bearbeitung von Vorfällen im Verbund der CERTs

Das als Open-Source-Software (OSS) entwickelte System ermöglicht die strukturierte Ablage von Daten zu Sicherheitsvorfällen, Schwachstellen und Kontaktmöglichkeiten. Sie sind die Grundlage für eine qualitativ hochwertige, zuverlässige und schnelle Bearbeitung von Anfragen. Der Zugriff auf diese Daten wird über ein flexibles Rechtemodell auf Benutzerebene in einer Client-Server-Architektur zur Verfügung gestellt. Vom System unterstützte Workflows können individuell frei gestaltet werden. Mit standardisierten Formaten fördert das System den Informationsaustausch und die Kooperation zwischen IT-Sicherheitsteams. SIRIOS wird als Basis für eine gemeinsame Dokumentation und Statistik verwendet.

▸ WID-Portal – Portal des Warn- und Informationsdienstes

IT-Nutzer und IT-Verantwortliche brauchen Informationen und schnelle Warnmeldungen über neu gemeldete Sicherheitslücken in IT-Systemen. Das WID-Portal bietet die Möglichkeit, Informationen individuell in Form eines personalisierten Newsletters zusammenzustellen, der sich an technischen Systemen und dem bewerteten Risiko der Sicherheitslücken orientiert. Das WID-Portal enthält ein Archiv der gemeldeten Schwachstellen einschließlich der Verweise auf Programme, mit denen die Sicherheitslücken geschlossen werden können.

▸ CBAS – CERT-Bund Alarmierungssystem

In kritischen Situationen, insbesondere bei laufenden Angriffen auf die Informationstechnik oder auch bei der Umsetzung dringend notwendiger IT-Sicherheitsmaßnahmen, müssen technisches Personal und Entscheider zuverlässig erreicht werden. Die Alarmierung erfolgt durch ein vom BSI entwickeltes mandantenfähiges Alarmierungssystem.

▸ Bürger-CERT

Auch die Bürger brauchen Informationen und insbesondere Warnungen vor neuen Risiken und erkannten Bedrohungen. In Zusammenarbeit mit dem Mcert, dem Computer-Notfallteam für kleine und mittelständische Unternehmen, bereitete das BSI im Jahre 2005 den Betrieb eines „Bürger-CERT“ vor, das private Internetnutzer mit wichtigen Informationen versorgt. Der Startschuss für das Bürger-CERT fällt im Frühjahr 2006.

Viren, Würmer und Trojanische Pferde

Das BSI hat mit namhaften Herstellern von Virenschutzprogrammen gesprochen, um auf dem Gebiet „IT-Frühwarnung“ noch intensiver zusammen zu arbeiten. Ziel ist der Aufbau eines Informationsnetzwerks, das es ermöglicht, beim Auftreten neuer Schadprogramme zeitnah gesicherte Informationen zwischen vertrauenswürdigen Partnern auszutauschen. Wer so schnell wie es geht Detailinformationen über ein Schadprogramm hat (Betreffzeile oder Namen von E-Mail-Anhängen bzw. ihre Größe), kann den Zeitraum zwischen detaillierter Analyse eines Schadprogramms und der Entwicklung von Signaturen, mit denen sich auf dem PC automatisch Schadprogramme erkennen und abwehren lassen, wesentlich verkürzen.

Wächter im Netz

Das BSI beschäftigt sich mit der Möglichkeit, unter Berücksichtigung des Datenschutzes Protokolldaten über den Internetverkehr zu gewinnen und statistisch auszuwerten, um vor Anomalien so früh wie möglich warnen zu können.
Die erforderlichen Sensoren lassen sich in zwei Gruppen einteilen:

- Sensoren, die den Datenverkehr in Teilbereichen des Internets mitlesen,
- Sensoren, die etwa bei öffentlichen Web-Seiten die Betreiber mit Informationen über die Kommunikationsbeziehungen und Antwortzeiten versorgen.

Entwickelt werden technische Sensoren, die an ausgesuchten Punkten des Internets platziert werden, statistische Auswertungen ermöglichen und das Frühwarnsystem automatisch alarmieren, sobald eine Veränderung im „Grundrauschen“ des Internets als Anomalie erkannt wird und eine fachliche Analyse der Beobachtungen erforderlich erscheint.

Informationsverbund Berlin-Bonn (IVBB)

Der IVBB wird permanent durch ein Frühwarnsystem (NAGIOS) beobachtet. Die Nutzer sind an strategischen Knoten über einen Messrechner an ihren Anschlüssen direkt mit einbezogen. Damit ist sofort ersichtlich, ob die Störung einen Dienst oder den Anschluss eines Nutzers betrifft.

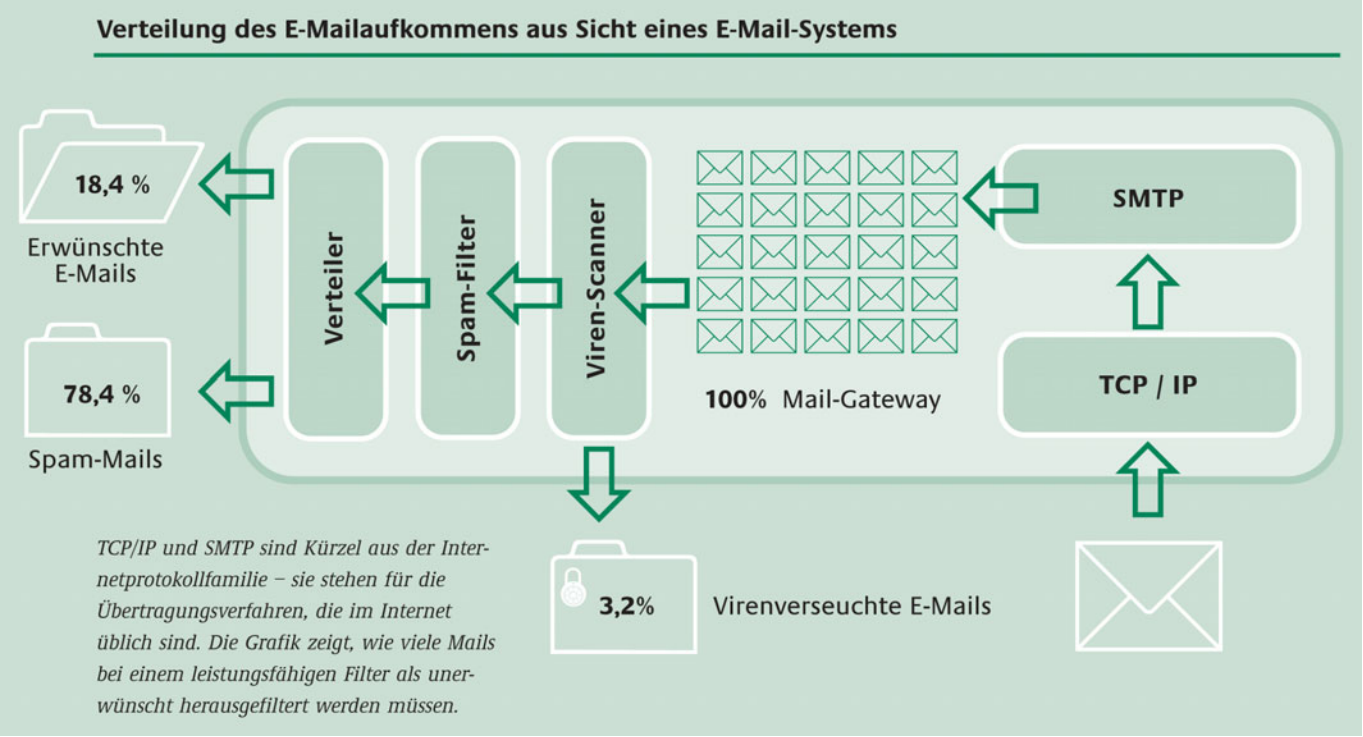
Der Messrechner fragt in regelmäßigen Abständen Dienste des IVBB ab und ermittelt aus den gemessenen Daten die Antwortzeit und die Verfügbarkeit der überwachten Anwendungen. Das aktuelle Lagebild der Prozesse und Anschlüsse kann im Lage- und Analysezentrum im BSI online über ein Webinterface abgerufen werden.

Der Informationsverbund Berlin-Bonn (IVBB) in Aktion: Videokonferenz zwischen den Standorten Bonn und Berlin des Bundesministeriums für Bildung und Forschung (BMBF).

2.3 Neue Herausforderungen: Spam, Phishing, Bot-Netze, VoIP

Das Internet erlaubt einen unkomplizierten globalen Informationsaustausch. Doch der einfache Zugang, die Freiheit, die das weltweite Netz bietet, hat ihren Preis: Internetdienste werden immer häufiger missbraucht.

Studien belegen, dass der Anteil an Spam-Mails weltweit bereits mehr als 60 Prozent am normalen Mail-Verkehr beträgt. Da stellt sich mancher ernsthaft die Frage, ob der Verzicht auf E-Mails nicht effektiver wäre. Doch bereits heute werden ganze Geschäftsabläufe per Mail abgewickelt. Also kann der Verzicht nicht praktikabel sein. Gebraucht werden zuverlässige Dienste und eine wirksame Abwehr gegen immer ausgefeiltere Spam-Versendetechniken.



Die Anti-Spam-Aktivitäten des BSI

Das BSI konzentrierte sich im Jahr 2005 vor allem darauf, die konkrete Bedrohungslage für Deutschland zu ermitteln. Überprüft wurde die Aussagekraft internationaler Studien für den deutschen Markt. Dabei konnte das BSI davon ausgehen, dass die deutschen Anwender vor den gleichen Problemen stehen, wie sie auch international auftreten. Die Einzelheiten waren jedoch unbekannt. Es gab weder Zahlen darüber, welches Spam-Aufkommen in Deutschland verarbeitet wird, noch war klar, welche Gegenmaßnahmen flächendeckend eingesetzt werden.

Antworten auf diese Fragen brachten intensive Gespräche mit Experten und eine Umfrage im Internet. Unter den Experten waren nationale Provider, international tätige Großunternehmen und eine Auswahl interessierter Organisationen. Diskutiert wurden auch internationale Ansätze zur Spam-Abwehr. Die Umfrage veranstaltete das BSI gemeinsam mit dem Institut für Internetsicherheit der FH-Gelsenkirchen.

Folgende Ergebnisse ragen heraus:

- Aufgrund des Datenrücklaufs waren statistische Aussagen zu ca. 40 Millionen E-Mail-Accounts und rund 2,3 Milliarden E-Mails im Monat möglich.
- Unter der Annahme, alle E-Mails werden angenommen, sind
  - ca. 18 Prozent als erwünscht und
  - ca. 82 Prozent als unerwünscht oder fehlerbehaftet erkannt worden.
- Antispam-Mechanismen werden umfangreich eingesetzt.
- 30 Prozent der Teilnehmer konnten bereits DDoS-Angriffe feststellen.
- Kritische Geschäftsprozesse werden von 45 Prozent der Befragten über E-Mail abgewickelt.
- Die meisten der Befragten gehen davon aus, dass die Bedrohung durch Spam und Viren weiter wachsen wird.

Detaillierte Ergebnisse der Umfrage stehen im Institut für Internetsicherheit (www.internetsicherheit.de) zum Download zur Verfügung.

Aus den Expertengesprächen und der Umfrage ging hervor, dass die Anwender unterschiedliche Ansätze zur Spam-Abwehr wählen. Das hat technische und organisatorische Ursachen. Die meisten setzen verschiedene Antispam-Maßnahmen in Kombination ein. Mit unterschiedlichem Erfolg werden auch neuere Verfahren implementiert. Ein weiteres Ergebnis: Als zur Zeit wenig zuverlässig sehen die Befragten Verfahren zur Authentifizierung von Absendern an (was auch an dem geringen Verbreitungsgrad liegen kann).

Die dynamischen Internetzugänge, wie sie überwiegend von unerfahrenen Heimanwendern genutzt werden, gelten übereinstimmend als die häufigste Quelle von Spam-Mails. Dies gilt national wie international.

Alle Befragten begrüßten Ansätze zur Spam-Abwehr, die stark auf eine internationale Zusammenarbeit von Organisationen ausgelegt sind. Unter anderem gibt es gemeinsame Anstrengungen, die Prozesse zur Bearbeitung von Beschwerden abzustimmen und zu standardisieren. Dieser Abuse-Managementprozess dient dem Ziel, Spam-Mails möglichst frühzeitig und nahe am Absender zu identifizieren.

Unerwünschte E-Mails gibt es in vielen Formen. Darunter kann kommerzielle oder nicht-kommerzielle Werbung verstanden werden, Malware, Phishing, Kettenbriefe oder Rufschädigung. Juristen und Techniker besitzen eine unterschiedliche Sichtweise zum Begriff Spam. Die im März 2005 veröffentlichte BSI-Studie „Antispam-Strategien – Unerwünschte E-Mails erkennen und abwehren.“ beschreibt auf über 140 Seiten ausführlich Möglichkeiten einer effektiven Spam-Abwehr und erfasst technische, rechtliche, wirtschaftliche und organisatorische Aspekte.
(Download: www.bsi.bund.de/literat/studien/antispam/antispam.pdf)

Die Studie kommt unter anderem zu dem Ergebnis, dass es wirtschaftlicher ist, Antispam-Maßnahmen einzusetzen als darauf zu verzichten, auch wenn es den E-Mail-Verkehr verlangsamt. Sicher konfigurierte Systeme sind Teil einer erfolgreichen Antispam-Strategie und verringern das Spam-Aufkommen insgesamt.

Spam-Mails sind ein komplexes, internationales Phänomen, das nicht einfach durch technische Maßnahmen abzustellen ist. Der Versand wird immer wieder neue Wege finden. Dadurch ist die Sicherheit in der Informationstechnik bedroht. Nur durch international greifende, flexible Antispam-Strategien lässt sich das Bedrohungspotential verringern. Die derzeit verfügbaren technischen Möglichkeiten bieten eine gute Basis.

„Spam"-Mails kosten jedes Unternehmen Zeit und Geld. Ohne Schutzmaßnahmen wäre der Mailverkehr oft nicht mehr nutzbar. Der Band „Antispam-Strategien" zeigt Lösungen. Zu beziehen beim Bundesanzeiger-Verlag Köln (32 Euro)

Phishing

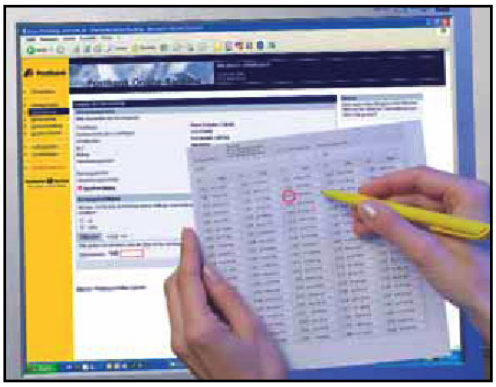
Im Jahr 2005 schwappte die Phishing-Welle auch nach Deutschland über. Beim Phishing versucht der Mail-Absender, in krimineller Absicht an vertrauliche Zugangsdaten von Online-Konten (Name, Kontonummer, PIN, TAN) zu gelangen, um mit diesen Daten die Konten plündern zu können. Zum Einsatz kommen entweder gefälschte Web-Auftritte von Geldinstituten, auf die der Kunde mit gefälschten E-Mails gelockt wird, oder sogenannte Trojanische Pferde, die beim Online-Banking unbemerkt Eingaben mitprotokollieren und über den normalen Internet-Verkehr an einen Server übertragen.

Anfangs waren die E-Mails noch auf Englisch oder in einem sehr mangelhaftem Deutsch abgefasst. Sie konnten so rasch als Fälschung erkannt werden. Die kriminellen „Phisher" haben die Qualität sowohl der E-Mails als auch der gefälschten Internet-Seiten inzwischen verbessert, so dass sie oft nur schwer von den Originalen zu unterscheiden sind.

Das BSI hat bei der Bekämpfung von Phishing hauptsächlich eine präventive Aufgabe. In erster Linie geht es um die Aufklärung der Bürger. Neue gefälschte Bank-Domains sind möglichst rasch abzuschalten. Das BSI arbeitet dabei erfolgreich mit den Strafverfolgungsbehörden zusammen.

Aufgrund des PIN-TAN-Verfahrens, das die deutschen Geldinstitute einsetzen, hält sich der Schaden in Deutschland gegenwärtig in Grenzen. Er dürfte im Jahre 2005 noch im einstelligen Millionenbereich liegen. In anderen Ländern, wo beim Internetbanking das Passwort genügt, geht der Schaden mittlerweile in den dreistelligen Millionenbereich, Tendenz steigend. Damit die Schadenshöhe in Deutschland nicht diese Ausmaße annimmt, haben die Banken sich verbesserte Verfahren wie iTAN (indizierte TAN) oder mTAN (mobile TAN per SMS) einfallen lassen.

Erfolgreich können aber alle diese Verfahren nur sein, wenn der einzelne Bürger bei seinen Online-Geschäften sicherheitsbewusst handelt und besonders E-Mails auf deren Wahrheitsgehalt prüft.



Zwei Beispiele für die neuen Sicherheitsstrategien der Geldinstitute: TAN-Nummern für den elektronischen Geldverkehr können nur verwendet werden, wenn die zugeteilte Nummer im Internet mit der auf der TAN-Liste übereinstimmt (iTAN). Oder jede TAN wird per SMS neu aufs Handy übertragen (mTAN).

Nur wenn das Zahlungssystem sicher ist, lassen sich bequem von zu Hause über das Internet Waren bestellen und Rechnungen begleichen.

Bot-Netze

Bot-Netze haben sich in der jüngsten Vergangenheit zu einer ernsthaften Bedrohung im Internet entwickelt. „Bot“ kommt von Robot und bezeichnet ein Programm, das selbstständig Befehle ausführt. Es wird auf den Computer eines Unwissenden geschleust, von einem Dritten gesteuert und für dessen Zwecke missbraucht. Ein Bot-Netz ist ein fernsteuerbares Netz von miteinander über das Internet verbundenen PCs, das in der Hand von Cyber-Kriminellen für ihre Zwecke genutzt werden kann.

Schadprogramme infizieren den einzelnen Computer, unterwerfen ihn der fremden Kontrolle und binden ihn in das Bot-Netz ein. Er weist keinen sichtbaren Schaden auf, aber er wartet auf Anweisungen von außen, die ihn für die Zwecke der Cyber-Piraten aktivieren. Kriminelle nutzen fremde Computer für Straftaten, der Besitzer des Rechners wird zum Mittäter, ohne es zu wissen.

Bot-Netze werden meistens für die Verbreitung von Spam-Mails oder für sogenannte „Denial of Service"-Attacken verwendet. Zur zentralen Fernsteuerung wird bei den derzeitigen Bot-Netzen zumeist das Internet Relay Chat Protokoll (IRC) eingesetzt.

Bot-Netze können aus Tausenden einzelner Rechner bestehen, deren zusammengefasste Kapazität die Bandbreite der meisten herkömmlichen Internetzugänge bei weitem übertrifft. Ein entsprechend großes Bot-Netz kann Internetserver durch riesige Datenmengen spielend lahm legen. Dazu kommt: Bot-Netze setzen sich meist aus „gekaperten" Heim-PCs zusammen. Das IP-Adressenspektrum ist dann so breit, dass die attackierten Anbieter sich nur bedingt schützen können.

Mit Hilfe eigener Infrastruktur und Software hat das BSI im Jahr 2005 damit begonnen, Bot-Netze zu erfassen und ihre Vorgehensweisen zu untersuchen. Dazu setzen die Techniker u.a. Internetsimulationen ein, die den Schadprogrammen das Vorhandensein einer vollständigen Internetumgebung vortäuschen, um ihre Vorgehensweise und Funktionalitäten analysieren zu können.

IT-Sicherheit von Anfang an – das sollten Erwachsene mit Kindern von Beginn an üben.

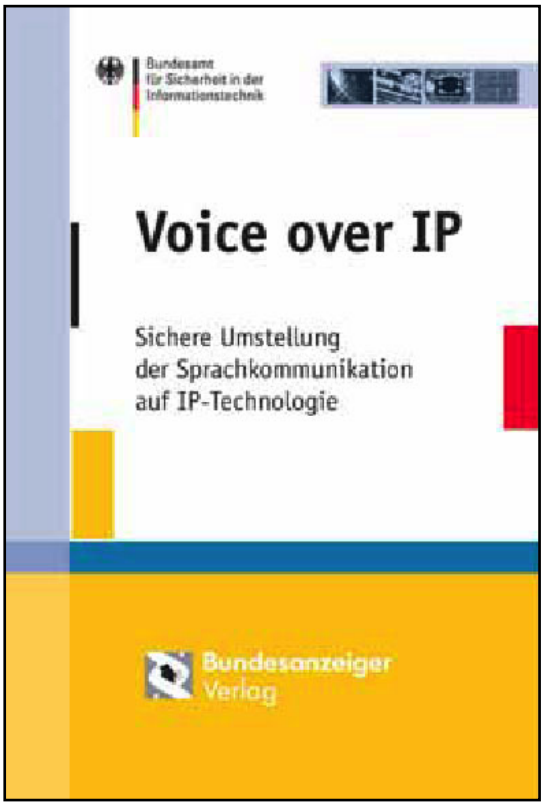
Voice over IP

VoIP hat die meisten technischen Kinderkrankheiten hinter sich und wächst nach und nach zu einer mehr als ernst zu nehmenden Konkurrenz zu traditionellen TK-Anlagen heran. Im Gegensatz zur leitungsgebundenen Vermittlung werden bei VoIP-Systemen die Gespräche über die aus der Datenwelt bekannten paketorientierten Vermittlung übertragen.

Dies hat zur Folge, dass die Gefährdungen aus der traditionellen TK-Welt mitgeschleppt und die aus der IP-Welt vererbt werden. Die von den Herstellern propagierten Einsparpotentiale durch die Konvergenz der beiden Systeme halten bei äquivalenter sicherheitstechnischer Betrachtung kaum stand. Nur durch einen substantiellen Mehraufwand sind VoIP-Systeme so verfügbar zu machen wie TK-Anlagen. Ähnliches gilt für Integrität und Vertraulichkeit. Auch diese beiden Faktoren, die zum Gerüst der Sicherheit gehören, bedürfen für den sicheren Einsatz von VoIP-Systemen einer detaillierten Untersuchung. Nur mittelbis langfristig werden Kosteneinsparungen durch die Konvergenz der Systeme möglich sein. Die größte Herausforderung ist nicht die Technik der Sprachübertragung über ursprünglich für Daten konzipierte Netze, sondern die Sicherheit.

Das bedeutet: Es geht nicht ohne ein Sicherheitskonzept, das den Schutzbedarf definiert und die Risiken analysiert. Nur auf diese Weise lässt sich ein der jeweiligen Institution angemessenes Sicherheitsniveau generieren. Was nutzt es, wenn eine größere Kosteneinsparung erzielt wurde, die Institution aber nicht mehr telefonieren kann (Verlust der Verfügbarkeit), ausspioniert wird (Verlust der Vertraulichkeit) oder ruiniert ist (Verlust der Integrität)? Sicherheit ist nicht umsonst und am Ende zählt nur eines: die Sicherheit und Zufriedenheit des Kunden!

Um sowohl Anwendern, Herstellern als auch Betreibern bei der Implementierung von VoIP eine Hilfestellung zu geben, hat das BSI 2005 eine Studie (www.bsi.bund.de/literat/studien/VoIP) erstellt. Sie beleuchtet alle sicherheitstechnischen Aspekte von VoIP. Frühzeitiges Einplanen der sicherheitstechnischen Belange zahlt sich am Ende immer aus!



Die Übertragung von Sprache über IP-Netze, das „Voice-over-IP“, ist einer der am schnellsten wachsenden Bereiche in der Telekommunikation. Bisher separat betriebene Telekommunikations- und IT-Netzinfrastrukturbereiche können unter Einsparung erheblicher Kosten zusammengefasst werden. Doch jede neue Technologie birgt neben Chancen auch Risiken. Dieses Handbuch gibt Tipps und erläutert Sicherheitsmaßnahmen. Zu beziehen beim Bundesanzeiger-Verlag (32 Euro).

2.4 VPS – Sichere Kommunikation zwischen Bürgern und Behörden

Die unter Federführung des BSI entwickelte BundOnline-Basiskomponente „Virtuelle Poststelle“ (VPS) ermöglicht den benutzerfreundlichen und sicheren Austausch elektronischer Daten zwischen Bürgern und Behörden. Als zentrale Kryptokomponente lässt sie sich sowohl in bestehende oder im Rahmen von E-Government neu entwickelte Fachverfahren integrieren als auch in Form eines eigenständigen Mail-Gateways betreiben. In beiden Funktionen befindet sich die VPS derzeit bereits bei zahlreichen Behörden im Einsatz.

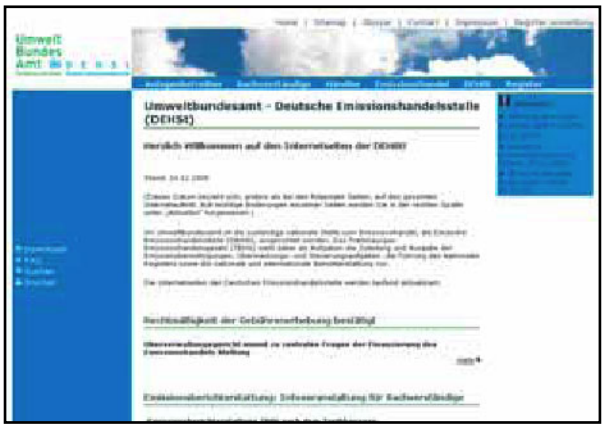
Die Vertraulichkeit eines Nachrichtenaustausches über das Internet ist nur dann gewährleistet, wenn die übertragenen Informationen zuvor mit einem kryptografischen Verfahren hinreichender Stärke verschlüsselt wurden. Soll dem Nachrichtenaustausch darüber hinaus auch eine rechtsverbindliche Form zukommen, wie etwa beim E-Business, E-Government oder Internet-Banking, müssen sich sowohl Absender als auch Empfänger der Nachrichten über die Identität ihres jeweiligen Kommunikationspartners stets vollkommen sicher sein können. Außerdem muss sichergestellt werden, dass die Nachrichten nicht unbemerkt verändert werden können. Verschlüsselung und Authentizität sind daher unabdingbare Voraussetzung für sicheres E-Government. Die Virtuelle Poststelle führt die genannten Funktionen an zentraler Stelle weitgehend automatisiert aus und entlastet hierdurch den Endanwender von diesen Aufgaben.

Die Formate der im Rahmen von E-Government ausgetauschten Daten können sehr unterschiedlich sein: sie reichen von unstrukturierten E-Mail-Texten mit beliebigen Anhängen bis hin zu wohlformatierten Datensequenzen, wie sie sich etwa beim Ausfüllen eines Web-Formulars ergeben und welche sich unmittelbar in den Workflow eines Fachverfahrens übernehmen lassen. Entsprechend dieser unterschiedlichen Anforderungen ist die VPS in zwei Teilkomponenten untergliedert, welche wahlweise einzeln und unabhängig voneinander oder auch gemeinsam im Verbund betrieben werden können. Die auf dem offenen Standard OSCI (Online Service Computer Interface) basierende Komponente eignet sich insbesondere für die sichere Übertragung von Daten, die über eine Web-Schnittstelle – z.B. ein HTML-Formular – eingegeben werden. Etwas salopp wird diese Komponente daher auch als „Web-VPS“ bezeichnet.

Der andere Bestandteil der VPS nutzt das E-Mail-Transferprotokoll SMTP und eignet sich daher vor allem für die Übertragung heterogen strukturierter Informationen (E-Mail mit Anhängen). Beiden Komponenten gemeinsam ist jedoch, dass sie – gleichgültig, ob sie unabhängig voneinander oder im Verbund betrieben werden – die oben angesprochenen Sicherheitsanforderungen erfüllen.

Ob „Rotes“ (wie hier in Berlin) oder „Schwarzes Rathaus“ – Bürger müssen sich darauf verlassen können, dass ihre Daten beim elektronischen Austausch mit Behörden sicher sind.

Rechts: Von Anfang an wurde bei der Deutschen Emissionshandelsstelle (DEHSt) auf elektronische Kommunikation gesetzt. Per Mail regeln sich Verkauf und Zukauf von Zertifikaten für den CO2-Ausstoß.



VPS im elektronischen Rechtsverkehr

Wie bereits erwähnt, eignet sich die Web-VPS besonders auch für eine direkte Integration in bereits bestehende Fachverfahren. Ebenso steht es jedem Anwender der VPS auch frei, neue Client-Anwendungen zu entwickeln, die über die offen gelegten Schnittstellen der VPS Daten zu Verschlüsselungs- und Authentifizierungszwecken an diese übergeben oder aus ihr abrufen. Eine solche direkt um die Web-VPS „herum entwickelte“ Client-Anwendung ist das „elektronische Gerichts- und Verwaltungspostfach“ (EGVP). Dieses ermöglicht es Rechtsanwälten und sonstigen Verfahrensbeteiligten in rechtlich verbindlicher Form Schriftsätze (die gewissen Formvorschriften genügen müssen) bei den Gerichten einzureichen, das heißt z.B. Klage zu erheben. Seit einer Rechtsverordnung vom 3. Dezember 2004 ist so über das EGVP der elektronische Rechtsverkehr mit dem Bundesverwaltungsgericht und dem Bundesfinanzhof gleichberechtigt zur Papierform möglich. Weitere Gerichte folgten im Laufe des Jahres 2005 bzw. planen den Einsatz des elektronischen Rechtsverkehrs für die nähere Zukunft. Ergänzende Informationen zum EGVP sowie auch den Link zum Download des Clients finden sich unter www.egvp.de.

Die Software „Elektronisches Gerichts- und Verwaltungspostfach (EGVP)“ macht es Juristen leichter, ihre Schriftsätze auszutauschen – aber gerade hier ist die sichere Verschlüsselung oberstes Prinzip.

Das Berliner Heizkraftwerk Mitte bei Nacht. Auch in diesem Fall vergibt die Deutsche Emissionshandelsstelle Zertifikate per Mail für den Kohlendioxid-Ausstoß – für sichere Kommunikation hat das BSI gesorgt.

VPS im Emissionshandel

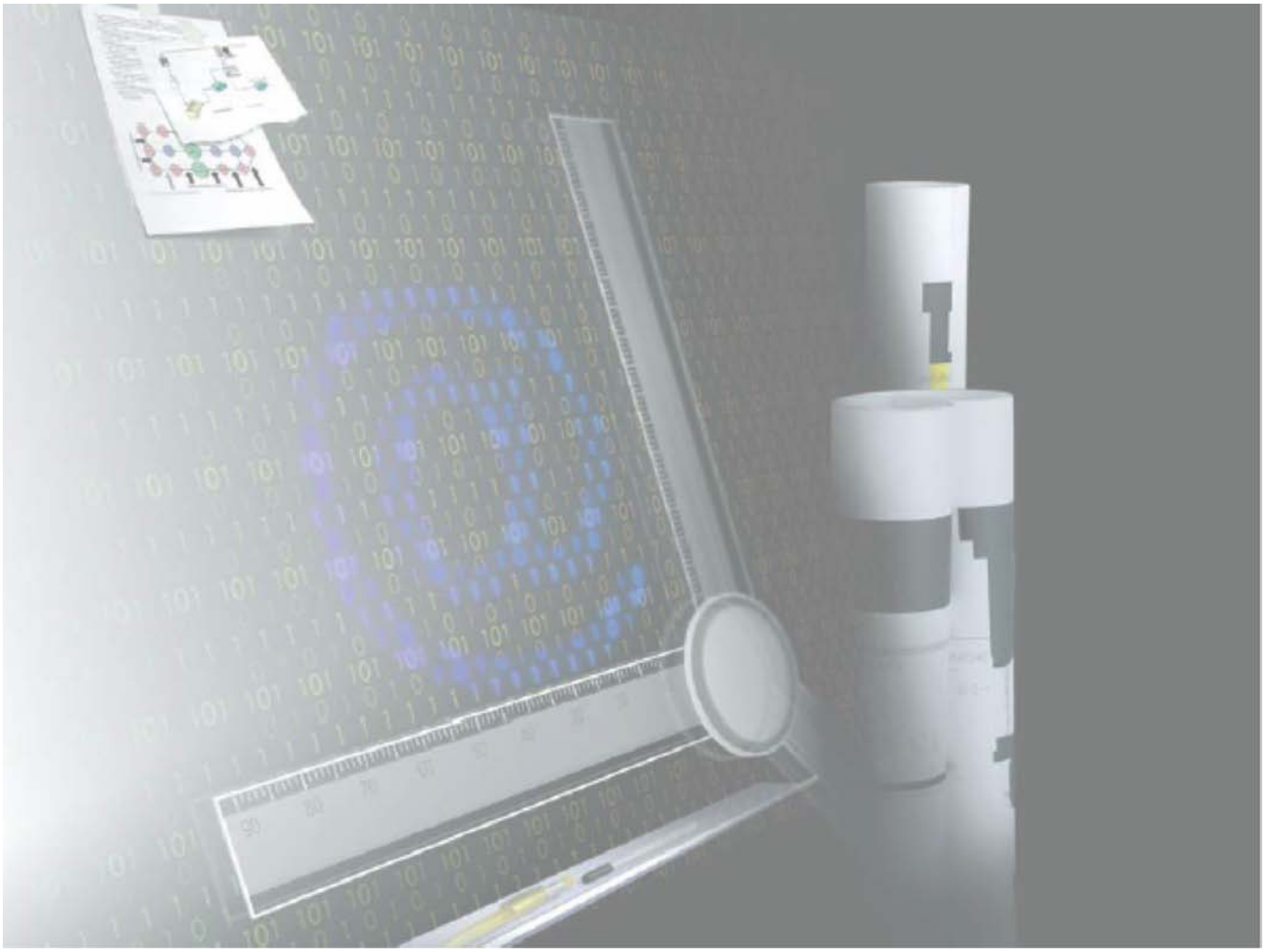
Ein weiteres Verfahren, das im Jahr 2005 in den Wirkbetrieb ging und welches die VPS nutzt, ist der Handel mit Emissionszertifikaten gemäß dem Kyoto-Protokoll. Dazu mussten sich die teilnehmenden Unternehmen – vorwiegend Energieversorger und Betreiber energieintensiver Industrieanlagen – zunächst bei der Deutschen Emissionshandelsstelle (DEHSt) registrieren. Da die hierzu einzureichenden Unterlagen in elektronischer Form teilweise einen Umfang von 30-50 MB umfassten, stellte bereits dieser Registrierungsprozess eine wirkliche Herausforderung an die Performance und Kapazität der VPS – genauer: der Web-VPS – dar.

Alleine während des einmonatigen Registrierungszeitraumes wurden so rund 2500 eingehende verschlüsselte und qualifiziert signierte E-Mails durch die VPS verarbeitet. Besonders bemerkenswert dabei ist die Tatsache, dass die Anzahl der per unverschlüsselter E-Mail, CD oder in Papierform eingereichten Registrierungsunterlagen nur noch weniger als zwei Prozent des Gesamtaufkommens ausmachten.

Neben den genannten Verfahren „elektronischer Rechtsverkehr“ und „Handel mit Emissionszertifikaten“ wird die Web-Komponente der VPS derzeit u.a. auch für die Übermittlung von Meldungen zur Strahlendosis des fliegenden Personals durch die Fluggesellschaften an das Luftfahrtbundesamt genutzt sowie für die Antragstellung zur Genehmigung der Ein- und Ausfuhr geschützter Pflanzen- und Tierarten beim Bundesamt für Naturschutz.

Die SMTP-Komponente „Julia“

Bedarf es bei der Integration der Web-VPS in ein bereits bestehendes Fachverfahren in der Regel gewisser Anpassungen, so lässt sich die SMTP-Komponente „Julia“ meist problemlos in den E-Mail-Strom einer Behörde oder sonstigen Organisation „einfädeln“. Entsprechend den durch den Betreiber frei definierbaren Regeln bearbeitet „Julia“ die ein- und ausgehenden E-Mails in einer für den Endnutzer völlig transparenten Weise, das heißt: letzterer bemerkt oft überhaupt nicht, dass er verschlüsselt kommuniziert, da „Julia“ alle kryptografischen Prozesse automatisch im Hintergrund abwickelt. Im Einsatz befindet sich die SMTP-Komponente der VPS bereits in zahlreichen Behörden, wie etwa dem Auswärtigen Amt, der Finanzverwaltung, der Deutschen Rentenversicherung Bund, dem Statistischen Bundesamt usw. Zahlreiche weitere Behörden planen darüber hinaus, noch im Jahr 2006 die VPS einzuführen. Weitere Informationen zum Thema „VPS“ unter www.bsi.bund.de/fachthem/egov/vps.htm



3 Technische Lösungen für sichere Datenübertragung

3.1 Neues aus der SINA-Welt

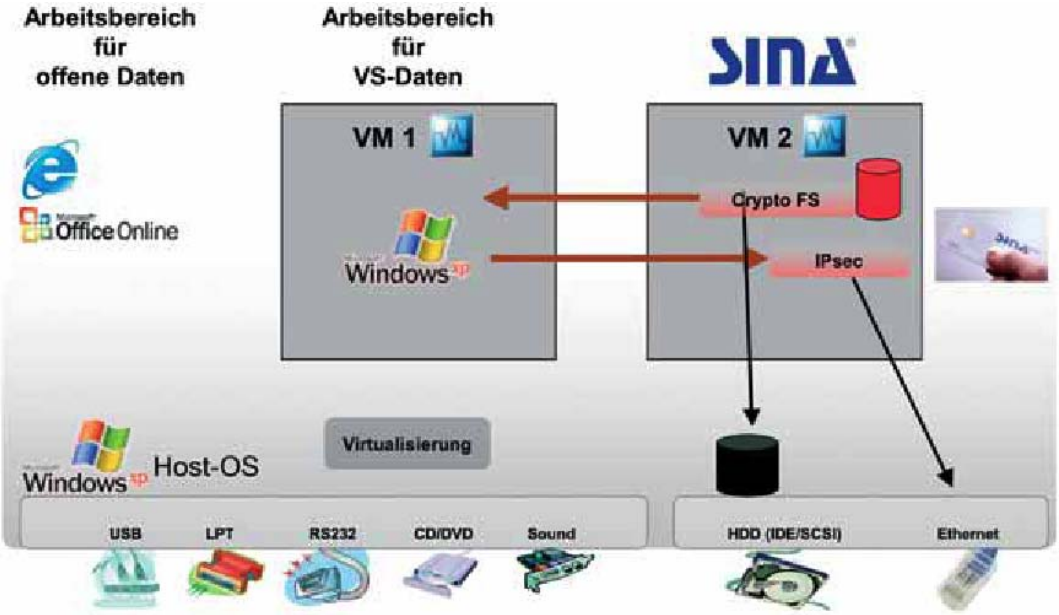
Mit der „Sicheren Inter-Netzwerk Architektur“ – abgekürzt SINA – stellt das BSI eine Technologie zur Verfügung, mit der sich hochsichere Verbindungen aufbauen lassen, und das über das ganz normale Internet. Auch 2005 hat das BSI in Zusammenarbeit mit der Firma secunet Security Networks AG weitere Komponenten rund um die SINA-Architektur entwickelt.

Neben den bereits seit längerem verfügbaren Bestandteilen SINA Box und SINA Thin Client gewinnt die SINA Virtual Workstation (VW) vor allem in mobilen Szenarien zunehmend an Bedeutung. Bei der SINA Virtual Workstation handelt es sich um eine Komponente der SINA-Architektur, bei der eine lokale Verarbeitung und Speicherung staatlicher Verschlusssachen (VS) möglich ist. Zusätzlich ist eine IPSec-verschlüsselte Datenkommunikation über beliebige Netze (z.B. GPRS, UMTS, WLAN oder DSL) möglich. Auch VoIP in SINA-Netzen wird künftig unterstützt. In der SINA VW werden potentiell unsichere oder nicht evaluierbare kommerzielle Betriebssysteme in einer virtuellen Umgebung gekapselt. Diese Umgebung wird durch eine virtuelle Maschine bereitgestellt, die ihrerseits auf dem evaluierten Host-Betriebssystem SINA-Linux ausgeführt wird. Die virtuelle Maschine simuliert eine Standardhardwareumgebung, auf der das Gastbetriebssystem mit den darauf laufenden Applikationen ausgeführt wird. Der Zugriff auf die physikalische Hardware kann nur unter Kontrolle von SINA-Linux erfolgen.

Eine erste Version, die sich bereits bei einigen Kunden, insbesondere beim Auswärtigen Amt, bewährt hat, hat das BSI 2005 grundlegend aktualisiert. Neben einem neuen Betriebssystemkern, der den Einsatz aktueller Hardware erlaubt, wurde die bisherige virtuelle Maschine gegen eine neue Version, die von einem deutschen Hersteller stammt, ausgetauscht. Weil dieser dem BSI den Quellcode offen legte, konnte das BSI eine intensive Evaluation vornehmen. Zusätzlich wurden in Zusammenarbeit mit dem Hersteller für den Einsatzfall erforderliche Anpassungen durchgeführt. Diese Neuerungen ermöglichen nun in Verbindung mit einer Erweiterung der Mechanismen zur Festplattenverschlüsselung auch den Einsatz im Bereich der Hochsicherheit.

Gespannte Aufmerksamkeit: Blick ins Lagezentrum des Auswärtigen Amtes

SINA Virtual Desktop



Im gastgebenden Betriebssystem (hier z.B. Windows) laufen zwei virtuelle Maschinen (VM). Die eine (VM 1) dient als Arbeitsbereich für Verschlusssachen, also VS-Daten. Dieser Bereich wird aus einem verschlüsselten Filesystem (Crypto FS) der zweiten VM gestartet, das heißt: der Kryptocontainer muss mit dem passenden Schlüssel geöffnet werden und erst dann kann dieses System gebootet werden. Das Crypto FS liegt auf der physikalischen Festplatte (HDD). Eine Kommunikation der VM 1 erfolgt über VM 2 über die Ethernet-Schnittstelle des Systems. Dabei werden die Daten IPSec-verschlüsselt übertragen. Offene Daten werden im Host-OS bearbeitet; dieses nutzt die benötigten Hardware-Ressourcen (USB, Sound, usw.) direkt. Das Gast OS in VM 1 nutzt diese Ressourcen über eine Virtualisierungsschicht.

Begriffserklärungen

VM	Virtuelle Maschine (hiervon gibt es zwei)
Crypto FS	Kryptofilesystem
IPSec	Bezeichnung für die Verschlüsselung bei der Datenübertragung. Wenn aus dem Virtual Desktop über das Netz („Ethernet“) gesendet wird, geschieht das über eine IPSec-gesicherte Verbindung. IPSec selbst ist ein Standard, den das BSI in SINA nutzt.
Host OS	Host Operating System – Betriebssystem, welches der „Gastgeber“ für die Gastbetriebssysteme (VMs) ist.

Im Vordergrund: Der Gebäudekomplex des Auswärtigen Amtes in Berlin – einer der „Kunden“ des BSI.

Virtual Desktop

Bedingt durch die Architektur der SINAVW kann dem Gastbetriebssystem nur eine begrenzte Auswahl virtueller Hardware zur Verfügung gestellt werden. Spezielle Hardware (zum Beispiel Prozessoren für Grafikbeschleunigung) kann nicht immer optimal genutzt werden.

Für Einsatzfälle bis VS-NfD (Verschlusssache – Nur für den Dienstgebrauch) wurde deshalb ergänzend das Entwicklungsprojekt SINA Virtual Desktop gestartet. Dabei arbeitet ein kommerzielles Betriebssystem (z.B. Windows) als Host-Betriebssystem, auf dem neben den üblichen Standardapplikationen virtuelle Maschinen dafür sorgen, dass zusätzliche Arbeitsumgebungen für die sicherheitskritische Datenverarbeitung bereitgestellt werden.

So kann in einer virtuellen Umgebung eine SINA-kompatible IPSec-Komponente (SINA-Box) arbeiten, die zusätzlich das kryptografische Filesystem zur verschlüsselten Datenspeicherung zur Verfügung stellt, während in der anderen eine vertrauenswürdige Umgebung zur Verarbeitung eingestufter Daten geschaffen wird.

Bei der Verarbeitung offener Daten kann das Host-Betriebssystem nativ, ohne die oben beschriebenen Einschränkungen, genutzt werden. Diese Variante adressiert Einsatzfälle für niedrigeren Schutzbedarf.

Durch das Prinzip der Virtualisierung, das auch in dieser Variante genutzt wird und den damit verbundenen unterschiedlichen logischen Adressräumen für Host- und Gastbetriebssystem, kann in Verbindung mit den üblichen Absicherungsmaßnahmen für kommerzielle Betriebssysteme ein für die adressierten Einsatzfälle angemessener Schutz erreicht werden.

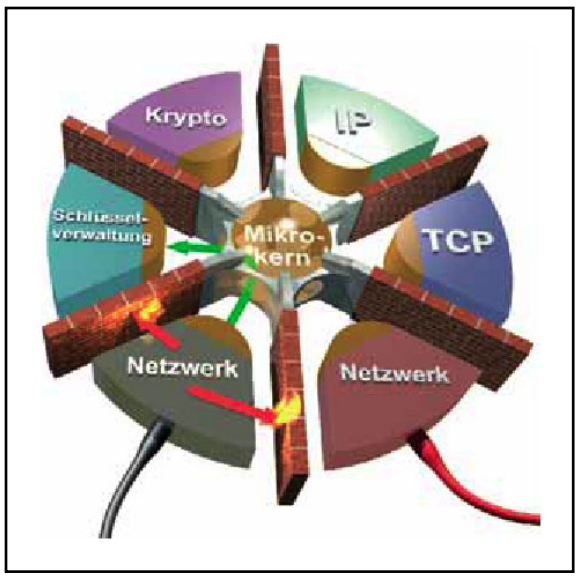
Das Produkt SINA Virtual Desktop soll im Laufe des Jahres 2006 für den Einsatzfall VS-NfD zugelassen werden.

Mikrokern

Die Architekten der Informationstechnik, die für sichere Datenverarbeitung zuständig sind, werden künftig mehr und mehr auf eine mikrokernbasierte Plattform zurückgreifen. Sie erfüllt die steigenden komplexen Anforderungen für Anwendungen und Sicherheitsvorgaben. Ein Mikrokern ist ein extrem kleiner Betriebssystemkern, der als Sicherheitsschicht zwischen einem oder mehreren eigentlichen Betriebssystemen und der Hardware angesiedelt ist.

Diese Plattform ist in der Lage, mit der verfügbaren Hardware Sicherungsmechanismen für Speicherschutz und Zugriffskontrolle umzusetzen. Sie muss neben einer effizienten Kommunikationsinfrastruktur auch eine Virtualisierungsschicht bereitstellen, damit sogenannte Legacy-Betriebssysteme dem Nutzer zur Verfügung stehen. Eine Virtualisierungsschicht stellt den Betriebssystemen virtuelle Geräte zur Verfügung und leitet deren Zugriffe darauf an die vorhandene physikalische Hardware weiter.

Das BSI hat mit dem Projekt „L4VM“ eine prototypische mikrokernbasierte Plattform entwickelt, die in den kommenden Jahren die monolithische Sicherheitsplattform der SINA-Komponenten ersetzen soll. Für die Beurteilung des zusätzlichen Sicherheitsgewinns ist eine kurze technische Beschreibung der grundlegenden Eigenschaften der Mikrokern-Technologie und Hardware-Virtualisierung notwendig.



Die Architektur des Mikrokern basiert auf Firewalls, welche die Programmsegmente untereinander abschotten. Ankommende Informationen verarbeitet allein der Kern.

Mikrokern ersetzt herkömmliche Sicherheitsplattform

Der Mikrokern ist die einzige privilegierte Systemkomponente, die mit Priorität 0, d.h. der höchsten verfügbaren Priorität auf der weit verbreiteten Intel Architektur IA32 betrieben wird. Jede weitere Systemkomponente oder Applikation läuft im Nutzerraum unter der vollständigen Kontrolle des Mikrokerns. In einem monolithischen Betriebssystemkern können Systemaufrufe uneingeschränkt auf den Kernspeicher zugreifen, was unter gewissen Umständen dazu führen kann, dass unbemerkte Programmierfehler oder bösartige Kernelmodule zu einer Kompromittierung des gesamten Systems führen.

Unter einem Mikrokern sind diese Szenarien zwar nicht ausgeschlossen, können aber nicht mehr ohne Weiteres Schaden anrichten. Ladbare Kernmodule können bevorzugt in separate Adressräume geladen und ausgeführt werden, was man als Kapselung der Komponente versteht. Der Mikrokern kann durch das Einblenden von Speicherseiten einen Zugriff auf ausgewählte Kernspeicherbereiche ermöglichen. Durch die Inter-Prozess-Kommunikation (IPC) ist zudem die Möglichkeit gegeben, Systemaufrufe zu protokollieren und ein umfassendes Systemaudit auf unterster Systemebene zu realisieren.

Das Virtual Machine Subsystem (VMS) ist für die Virtualisierung der Hardware verantwortlich. Das VMS erlaubt das Ausführen sogenannter Legacy-Betriebssysteme, z.B. Windows XP, für die eine Portierung auf die Mikrokernschnittstelle nicht ohne weiteres möglich oder nicht erwünscht ist. Das Prinzip der Hardware-Virtualisierung zur Kapselung eines im allgemeinen nicht vertrauenswürdigen beziehungsweise nicht evaluierbaren Gastbetriebssystems sorgt für einen zusätzlichen Schutz des Hostbetriebssystems. Im Falle eines mikrokernbasierten Systems ist dieser Schutzmechanismus wegen der fundamentalen Kapselung des VMS durch den Mikrokern deutlich verstärkt. Zugriffe des Gastbetriebssystems werden von dem VMS ausschließlich über die vom Mikrokern bereitgestellte Kommunikationsinfrastruktur durchgeführt.

Durch eine performante Hardware und/oder Hardwareunterstützung können zusätzliche Sicherheitsmechanismen, wie Mikrokern-Technologien und Virtualisierung für die Ausführung von Legacy-Betriebssystemen, transparent in die Sicherheitsarchitektur integriert werden. Die vorliegende prototypische, vom BSI entwickelte, generische Lösung eignet sich nicht nur für den Einsatz in Hochsicherheitsszenarien des Bundes, sondern ist auch von öffentlichem Interesse für Anforderungen bezüglich einer vertrauenswürdigen Umgebung eines IT-Systems.

3.2 ElcroDat 6-2, GALILEO, SAR-Lupe

Das ISDN-Kryptosystem ElcroDat 6-2 ist für die Übertragung von Daten höchster Geheimhaltungsgrade zugelassen. Es verhindert, dass Unbefugte die übertragenen Daten ausspionieren oder sie unbemerkt manipulieren.

Immer öfter tauschen die Bundesverwaltung, die mit dem Geheimschutz beauftragten Industrieunternehmen oder die Sicherheitsbehörden sensible Informationen aus. Daher sind Verschlüsselungssysteme erforderlich, die höchsten Sicherheitsansprüchen genügen und ausreichende Bandbreiten für moderne Anwendungen bieten.

Projekt ElcroDat 6-2

Mit der vom BSI und der Firma Rohde & Schwarz SIT GmbH entwickelten Hochsicherheitslösung ElcroDat 6-2 lassen sich eine Vielzahl von Einsatzszenarien abdecken. Telefon-und Datenverbindungen sowie Fax und Videokonferenzen – selbst über Satellit – sind möglich. Idee, Konzept und viele technische Details des Systems stammen aus dem BSI. Das System hat die Zulassung sowohl der EU als auch der NATO und ist für alle nationalen Geheimhaltungsgrade einschließlich STRENG GEHEIM geeignet. Es besteht aus folgenden Komponenten:

- den Verschlüsselungsgeräten ElcroDat 6-2 S und ElcroDat 6-2 M
- einer Management-Station für das kryptographische Management
- einer Service-Station zur Fernadministrierung der Verschlüsselungsgeräte
- einer Logging-Station zur Fernüberwachung der Verschlüsselungsgeräte

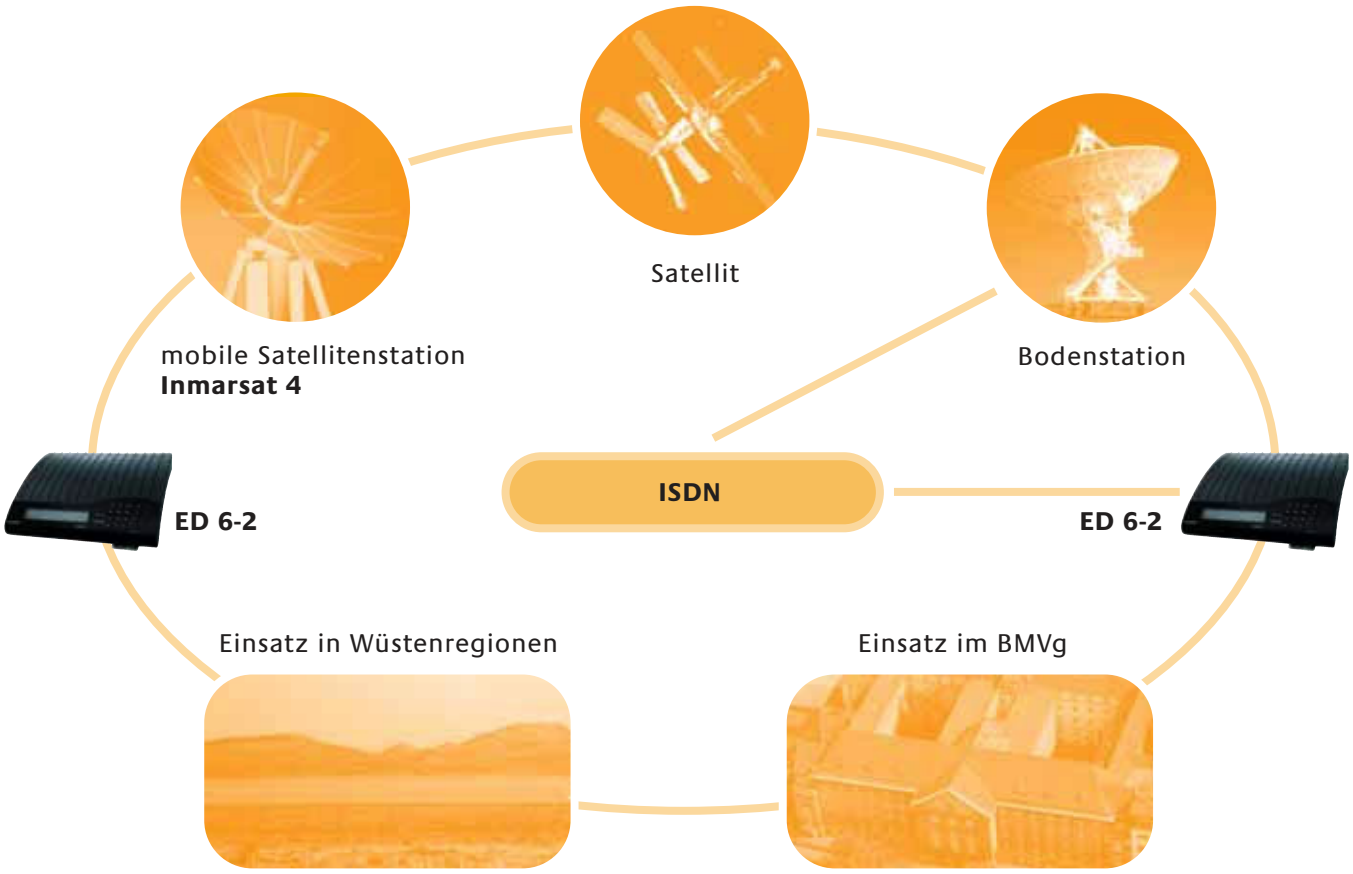
Es existieren zwei Gerätetypen: das ElcroDat 6-2 S für den Basisanschluss im ISDN mit zwei Informationskanälen und das ElcroDat 6-2 M für den Primärmultiplexanschluss mit 30 Informationskanälen. Die Public-Key-Infrastruktur entlastet den Anwender vollständig bei der Versorgung des Systems mit Schlüsselmitteln. Die kryptografische Verwaltung der Geräte übernimmt die Management-Station.

Ein „Gateway“ – fertiggestellt 2005 – erlaubt als Bindeglied die Kommunikation zwischen dem digitalen ISDN und bereits vorhandenen, auf analogen Netzen beruhenden Kryptosystemen.

Das ElcroDat 6-2 wird inzwischen weltweit bei Sicherheitsbehörden eingesetzt. Zu den Anwendern zählen die EU und eine Reihe von europäischen Staaten. Die NATO hat das Elcro-Dat 6-2 zu ihrem Standard-ISDN-Kryptosystem gewählt. Erste Geräte sind bereits seit 2005 bei der NATO installiert. Die Nachfrage nach Elcro-Dat 6-2 Geräten und Systemkomponenten steigt stetig.

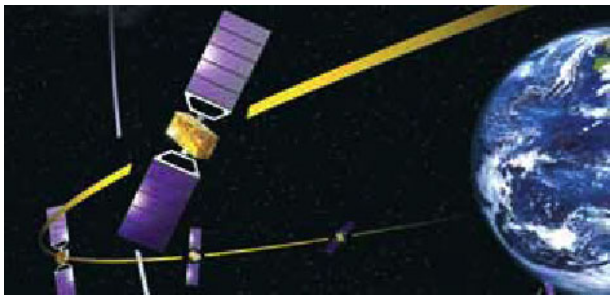
Das System wird ständig an den aktuellen Stand der Technik angepasst, erprobt und in den Einsatz gebracht. In der Konzeption befindet sich aktuell eine Zusatzbaugruppe, die zusammen mit dem Secure Communication Interoperability Protocol (SCIP) auch verschlüsselte Verbindungen über Netzwerkgrenzen hinweg ermöglicht. So soll zukünftig auch die Kommunikation vom ElcroDat 6-2 zu analogen Anschlüssen, Handys oder anderen nicht ISDNfähigen Endgeräten möglich sein. Hieraus ergeben sich enorme Einsatzperspektiven. Als weitere Produkt- und Systeminnovation ist geplant, dass die Software der Geräte durch eine gesicherte Prozedur nachladbar ist.

Aus der Wüste ins Verteidigungsministerium:
Sichere ISDN-Verbindung dank ElcroDat



Die Kryptierung von ISDN-Verbindungen über Satellitenstrecken ist ein weiteres Leistungsmerkmal des Verschlüsselungssystems ElcroDat 6-2. Ein Beispiel: Der tägliche Lagebericht des Bundeswehrkommandos im Ausland, z.B. Afghanistan, wird per Videokonferenzschaltung ins Lagezentrum der Bundeswehr übermittelt. Dort, wo kein ISDN-Anschluss aus einem Festnetz zur Verfügung steht, kommen dann Satellitenterminals zum Einsatz. †ber das Inmarsat-Netz wird die Verbindung zur Bodenstation des Empfangslandes hergestellt. Um die erforderliche Bandbereite zur Verfügung zu stellen, werden mehrere †bertragungskanäle gebündelt. Kryptiert wird die Verbindung mit dem ISDN-Verschlüsselungsgerät ElcroDat 6-2.

Einer von 30 Satelliten, die zusammen das europäischen Navigationssystem GALILEO bilden werden (schematische Darstellung)..



Satelliten-Projekte

Das BSI lieferte 2005 wesentliche Beiträge zum Design und zur Entwicklung aktueller Satellitensysteme. Zu nennen sind hier das Global Navigation Satellite System (GNSS) GALILEO und das nationale Beobachtungssystem SAR-Lupe.

GALILEO

GALILEO ist ein Navigationssystem der neuen Generation. Es verfügt über weltweit verteilte Bodenstationen und wird von zwei Kontrollzentren aus überwacht und gesteuert. Vier unterschiedliche Dienste werden angeboten: ein offener Dienst (OS), ein kommerzieller Dienst (CS), ein Luftverkehrsdienst (SoL) und ein behördlicher Dienst (PRS). GALILEO unterstützt das Seenotrettungssystem (S&R).

Alle Dienste stellen unterschiedliche Anforderungen an Sicherheit, Qualität und Verfügbarkeit:

- Der OS soll allen Nutzern kostenlos zur Verfügung stehen. Garantien zur Sicherheit und Verfügbarkeit dieses Dienstes stehen daher nicht im Vordergrund.
- Kommerzielle Provider haben die Möglichkeit, über den CS ihre Dienste, z.B. Flottenmanagement oder Routenverfolgung, unter anderem Logistikunternehmen kostenpflichtig anzubieten. Das Design des CS erlaubt ein erhöhtes Maß an Sicherheit, Qualität und Genauigkeit.
- Der SoL dient zur Navigation von Flugzeugen.
- Für behördliche Anwender bietet der PRS ein Höchstmaß an Sicherheit, Verfügbarkeit und Qualität.

Ein derartig komplexes System ist einer Vielzahl von Bedrohungen ausgesetzt. Ziel der Mitarbeit des BSI ist deshalb, diese Bedrohungen durch geeignete Sicherheitsmaßnahmen im System abzuwehren.

Der Schwerpunkt der Unterstützung liegt bei der Spezifikation der Satelliten, der Bodenkomponenten und der zugehörigen Sicherheitsbeziehungen einschließlich des Managements und der unterschiedlichen Dienste, insbesondere des PRS. GALILEO erfordert als internationales Projekt besonders die Absprache mit anderen nationalen Sicherheitsbehörden, der beteiligten Industrie und dem Projektmanagement (ESA). Die Unterstützung umfasst alle Bereiche der Sicherheit, u.a. die kryptografische und IT-Sicherheit.

Die Mitwirkung des BSI ist beim Schutz des Regierungsdienstes Public Regulated Service (PRS) von besonderer Bedeutung. Weil der PRS ausschließlich für Behörden oder vergleichbare nationale und internationale Institutionen entwickelt wurde, ist der Dienst potentiellen Bedrohungen von außen ausgesetzt, z.B. Denial-of-Service oder nicht autorisierte Nutzung. Damit stellt er äußerst hohe Anforderungen nicht nur an die Vertraulichkeit, sondern auch an die Robustheit des ausgestrahlten Signals, die Beweisbarkeit der Quelle und die Unveränderbarkeit der Information, auch in den Situationen, in denen andere Dienste nicht verfügbar sind.

Nach Abschluss der Spezifikationen – voraussichtlich 2006 – wird das BSI im Rahmen des Teams nationaler Experten (NETeam), das sich aus Mitarbeitern der verschiedenen Nationen zusammensetzt, an der entwicklungsbegleitenden Evaluierung beteiligt sein. National wird das BSI zusammen mit anderen Bundesbehörden ein Management für die nationale Nutzung des PRS und die Schnittstellen zum System entsprechend den Vorgaben von GALILEO erarbeiten. Die Evaluierung der Kryptografie hat das BSI bereits 2005 weitestgehend abschließen können.

Bei dem Satellitenüberwachungssystem GALILEO sind die verschiedenen Kontrollsegmente, das Schlüsselmanagement und die Generierung der Missionsdaten in zwei Kontrollzentren (GALILEO Control Center – GCC) zusammengefasst. Diese sind auch für die Anbindung von externen Partnern oder Zentren verantwortlich. Das System GALILEO verfügt über 30 Sensor-Stationen zum überwachen der Satelliten und weltweit verteilte Uplink-Stationen für die Steuerung der Satelliten und die Versorgung der Nutzer mit den erforderlichen Daten und Informationen. Insgesamt müssen die GCC 30 Satelliten auf drei verschiedenen Orbits überwachen, steuern und administrieren. Alle Kommunikationsbeziehungen sind mit entsprechenden IT- oder kryptografischen Mitteln einfach oder zum Teil sogar mehrfach gegen äußere und innere Angriffe geschützt. Rechts: Blick in das deutsche Weltraum-Kontrollzentrum Oberpfaffenhofen, einem der beiden künftigen GALILEO-Kontrollzentren.

SAR-Lupe

Das Erdbeobachtungssystem SAR-Lupe verfügt über mehrere Satelliten, mit denen Aufnahmen der Erdoberfläche gemacht werden können. Es gliedert sich in einen rein nationalen und einen internationalen Anteil.
Die kryptografische Sicherheit liegt allein in der Verantwortung des BSI, das eng mit dem Bundesamt für Wehrtechnik und Beschaffung (BWB) in Koblenz, mit Industrieunternehmen und mit weiteren Bundesbehörden zusammenarbeitet. Den Schwerpunkt der Tätigkeiten des BSI hinsichtlich des nationalen Anteils bildete in 2005 die Evaluierung der Kryptokomponenten. Zusätzlich unterstützte das BSI SAR-Lupe bei der Erstellung und Fortschreibung der ITSicherheitsdokumentation. Im internationalen Bereich war 2005 das Kryptokonzept ein Schwerpunkt. Auch hier arbeitete das BSI mit dem BWB bei der Erstellung der IT-Sicherheitsdokumente zusammen.

Das Bundesverteidigungsministerium (BMVg) nutzt SAR-Lupe, das erste satellitengestützte Aufklärungssystem Deutschlands, zur Früherkennung von Krisen und zum Krisenmanagement.

3.3 BOS – das digitale Funknetz

Die ersten Teile des neuen digitalen Funknetzes BOS sollen im Laufe des Jahres 2006 errichtet sein. Dieses Netz ist gedacht für die Kommunikation zwischen Behörden und Organisationen mit Sicherheitsaufgaben (BOS-Digital).

Es gibt verschiedene Realisierungsvarianten für ein solches BOS-Digital Funknetz. International haben sich der ETSI-Standard TETRA (Terrestrial Trunked Radio) und der vom EADS Konzern entwickelte Firmenstandard TETRAPOL etabliert. Auch auf der Basis des GSM-Standards soll es in Zukunft eine für BOS-Digital geeignete Systemvariante geben. Europaweit ist bereits eine Vielzahl unterschiedlicher Systeme im Gebrauch. Das BSI hat den Auftrag, das entstehende Funknetz – unabhängig von der Auswahl des konkreten Funksystems – mit einer sogenannten Ende-zu-Ende-Verschlüsselung auszustatten. Sie gewährleistet einen besonders hohen Grad an Sicherheit.

Um dieses Ziel erreichen zu können, hat das BSI in den vergangenen Jahren intensiv an der Entwicklung einer innovativen Verschlüsselungstechnologie gearbeitet, die auf Chipkarten basiert. Nahezu jedes mobile Kommunikations-Endgerät verfügt heute über eine Chipkartenschnittstelle, um die sogenannte SIM-Karte aufzunehmen.

Chipkarten mit höchstem Sicherheitsstandard

Durch die Integration der Verschlüsselung in eine Chipkarte müssen kommerziell verfügbare Funkendgeräte kaum technisch modifiziert werden. Zugleich sind Chipkarten Mainstream-Produkte, die höchsten Sicherheitsansprüchen genügen und sich millionenfach in diversen Sicherheitssystemen bewährt haben. Nach den bisherigen Planungen werden alle rund 450.000 Endgeräte des Netzes mit der neuen „BOS-Chipkarte“ ausgestattet. Sie enthält alle sicherheitsrelevanten Funktionen. Eine BOS-Chipkarte kann zu sehr geringen Kosten hergestellt werden und ist dennoch ein vollwertiges Verschlüsselungsgerät mit allen erforderlichen Eigenschaften.

Das BOS-Kryptosystem des BSI verfügt über eine eigenständige Public Key Infrastruktur (PKI), die in Zukunft vom BSI betrieben werden soll. Hierdurch kann das Rollout und die Parametrisierung der Systeme sehr effizient erfolgen. Im Rahmen der Entwicklung und Anpassung des Systems haben die Experten alle erdenklichen BOS-spezifischen Einsatzszenarien berücksichtigt. Auf diese Weise konnten Sicherheitsbedürfnisse vom Technischen Hilfswerk über Feuerwehr und Polizei bis hin zu SEK (Sondereinsatzkommandos) berücksichtigt werden. Dabei wurde insbesondere die Integration des Systems in Leitstellensysteme berücksichtigt.

Die Modularität dieses Ansatzes vereinfacht die Entwicklung von Endgeräten für das neue digitale BOS-Netz erheblich und trägt so zur Kostenreduzierung und zur Schaffung eines breiten Angebotes bei. Grundsätzlich wird sich das BOS-Funkgerät der Zukunft nur noch wenig von den üblichen mobilen Telefonen unterscheiden. An die Stelle der vollständigen Neukonstruktion von Geräten wird der Umbau industrieller Serienprodukte treten, die als Sicherheitsanker die BOS-Chipkarte nutzen.

Das Prinzip ist Handy-Nutzern bekannt: Bei BOS-Nutzern funktioniert das Einloggen in das Funknetz nach dem Prinzip der SIM-Karte. Allerdings stellt die BOS-Karte weitaus mehr kryptografische Funktionen zur Verfügung.

Datenbankanbindung

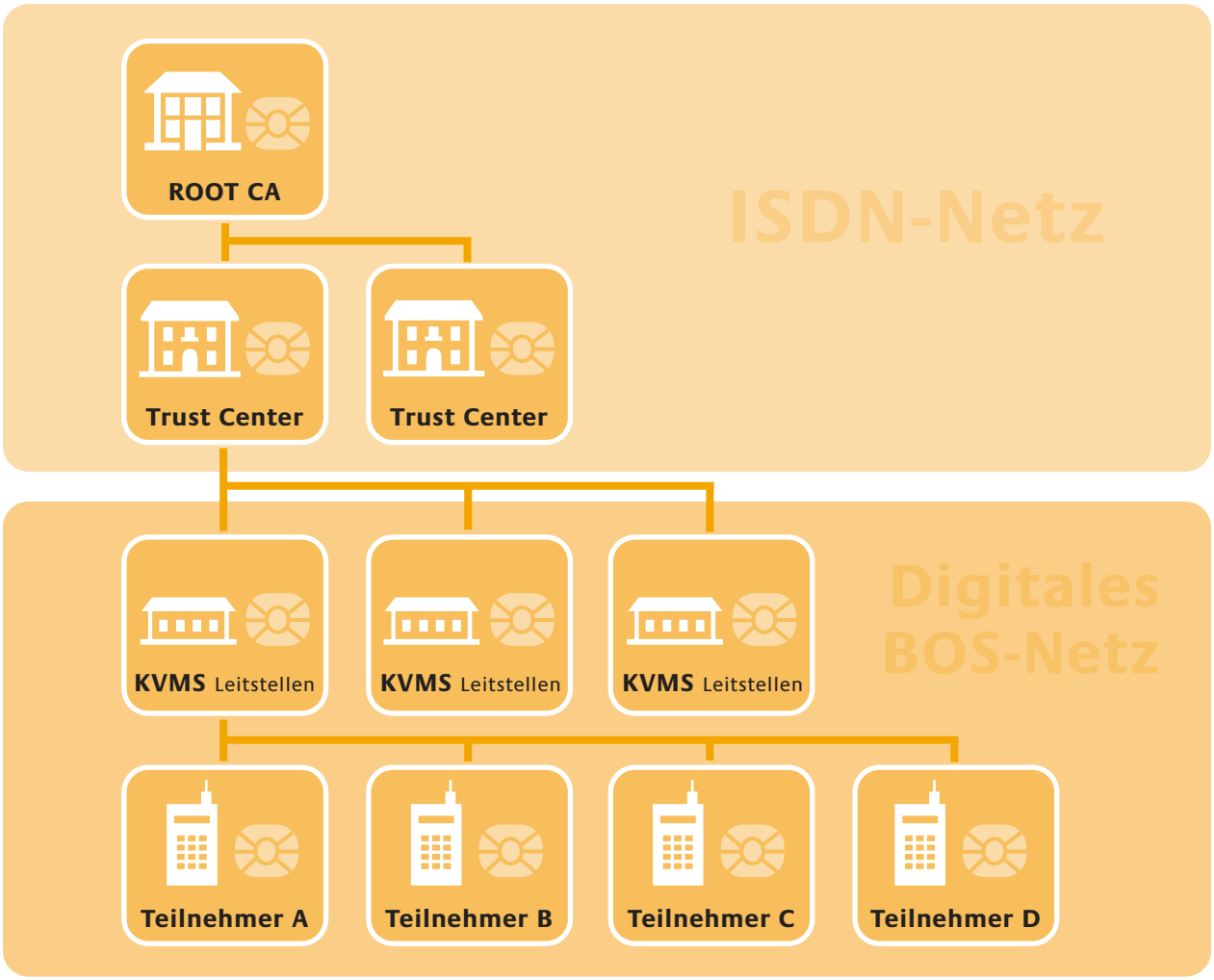
Das hohe Sicherheitsniveau der Ende-zu-Ende-Verschlüsselung soll auch dann erhalten bleiben, wenn einzelne Endgeräte mit zentralen Stellen des BOS-Netzes kommunizieren. So erfordert beispielsweise die Anbindung einer Datenbank an das BOS-Netz die gleichzeitige Verwaltung zahlreicher verschlüsselter Verbindungen, die zu diversen BOS-Teilnehmern aus dem gesamten Bundesgebiet führen können.
In Zukunft wäre auf diese Weise zum Beispiel die Abfrage biometrischer Merkmale möglich (Fingerabdrücke, Gesichtsbild, etc.). Ein Polizist kann also jederzeit vor Ort eine erweiterte Personenidentifikation vornehmen. Für diese Anwendungsfälle soll im Auftrag des BSI ein mehrkanaliges Gegenstück zur BOS-Chipkarte entwickelt werden.

Chipkarten-Technologie und Kryptografie sind hochdynamische Forschungsbereiche, die einer ständigen Innovation unterworfen sind und nicht isoliert von den möglichen Anwendungsszenarien betrachtet werden können. Die Funknetze werden immer leistungsfähiger und in Zukunft voraussichtlich deutlich höhere Übertragungsraten ermöglichen. Auch die Funkendgeräte werden immer höheren Leistungsanforderungen genügen müssen.
Der Takt wird weitgehend von der rasanten Entwicklung im öffentlichen Mobilkommunikationssektor vorgegeben. Das BSI verfolgt daher langfristige Strategien zur Pflege und Weiterentwicklung des BOS-Kryptosystems. Dazu gehören die Portierung der BOS-Chipkarte auf neuere, leistungsfähigere Chipkarten-Typen und die Einbindung der Karte in alternative Formfaktoren wie z.B. die SD-Speicherkarte.

Feuerwerk im Berliner Olympiastadion: Die Sicherheitskräfte sind gerade bei Großveranstaltungen besonders herausgefordert.

Technisches Hilfswerk (THW), Feuerwehr und Polizei brauchen ein sicheres Funknetz, das Missbrauch ausschließt und multifunktional nutzbar ist.

Systemarchitektur digitales Netz
Behörden und Organisationen mit Sicherheitsaufgaben (BOS)



Innerhalb der BOS-Mobilfunkgeräte dient eine Chipkarte (Sicherheitskarte) als Modul, das die kryptografischen Algorithmen sowie die notwendigen kryptografischen Schlüssel kapselt. Zusätzlich werden von der Sicherheitskarte die Netzzugangsfunktion (SIM-Funktion) und die Übermittlung der operativ-taktischen Adresse der BOS zur Verfügung gestellt. Das Schlüsselmanagementsystem wurde für die speziellen Belange der BOS hinsichtlich Verfügbarkeit und Flexibilität optimiert. Es stützt sich dabei auf eine Infrastruktur, die aus den Ebenen KVMS (Krypto-Variablen Management-System), TC (Trust Center) und Root CA (Root Crypto Authority) besteht. Auch für KVMS und TC sind Sicherheitskarten als Kryptomodule und Authentisierungsmodule vorgesehen. Nach einem Beschluss von Bund und Ländern wird das BSI für den späteren Wirkbetrieb des digitalen Funknetzes die Teile Root CA und Trust Center betreiben.

3.4 Technologiefeld Biometrie

Das BSI hat seine Biometrie-Projekte im Jahr 2005 konsequent fortgesetzt. Feldversuche folgten den Laborversuchen, die praktische Anwendung trat in den Vordergrund. Die BSI-Experten griffen neue biometrische Technologien wie die 3D-Gesichtserkennung auf und zeigten mit Untersuchungen zur Multimodalität Methoden auf, welche die Erkennungsleistung biometrischer Verfahren um ein Vielfaches steigern können.

BioFace

Die im Jahr 2002 begonnene Projektreihe BioFace wurde in 2005 mit weiteren Untersuchungen zur Leistungsfähigkeit von Gesichtserkennungssystemen fortgesetzt. Die bereits 2004 abgeschlossene Untersuchung zum Grenzwertverhalten solcher Systeme (BioFace III) wurde 2005 ausgewertet und zur Veröffentlichung vorbereitet. Gleichzeitig trug das BSI mit BioFace V dem aktuellen technologischen Trend hin zur dreidimensionalen Gesichtserkennung Rechnung. Auf Grundlage der Daten eines Feldversuchs wurden zwei marktverfügbare Systeme und ein eigens für das Projekt entwickeltes System auf Funktionsweise und Erkennungsleistung hin untersucht. Die Resultate der Untersuchung flossen in einen Beitrag des BSI für die Standardisierungsansätze der ISO ein.

BioP

Die Untersuchung biometrischer Verifikationsverfahren im Rahmen des Projekts BioP II hatte zum Ziel, die Leistungsfähigkeit von Systemen zur Gesichts-, Fingerabdruck- und Iriserkennung, die zum entsprechenden Zeitpunkt auf dem Markt verfügbar waren, zu ermitteln. Daraus ließen sich Schlüsse für die erfolgreiche Verwendung von biometrischen Verfahren im Zusammenhang mit Personaldokumenten ziehen. Die Ergebnisse der Untersuchung können auf der BSI-Homepage unter www.bsi.de/literat/studien/biop/biop_2.htm eingesehen werden.

BioP II umfasste eine aufgrund wissenschaftlicher Kriterien angelegte Praxiserprobung der drei genannten biometrischen Verfahren in einem vergleichenden Systemtest. Der Schwerpunkt lag auf der Untersuchung der technischen Machbarkeit. Die entscheidenden Fragen:

- Welche Erkennungsleistung bieten die Verfahren Gesichts-, Finger- und Iriserkennung?
- Können die Verfahren mit Bilddateien gemäß ICAO als Referenz zufrieden stellende Ergebnisse erzielen?
- Welche Praxistauglichkeit bieten die drei Verfahren für eine große Testgruppe? Wie ist es um Benutzbarkeit und Akzeptanz bestellt?
- Welches der Verfahren eignet sich unter welchen Bedingungen am besten für die Verwendung in Personaldokumenten?

Das BSI leitete das Gesamtprojekt in enger Kooperation mit dem BKA und den beiden Unternehmen Fraport AG und Deutsche Lufthansa AG. Mit im Boot: Die Firma secunet Security Networks AG als Auftragnehmer.

Das BSI hat im Jahre 2005 auch diese Terminals zur Gesichtserkennung testen lassen.

BioFinger II

Im Mittelpunkt der Versuchsreihe Bio-Finger II standen verschiedene Verfahren zur Steigerung der Erkennungsleistung bei der Fingererkennung. Die Idee: Statt eines Fingerabdrucks werden mehrere verwendet. Beantwortet wurden die Fragen, welche Leistungssteigerung erreicht wird, wenn

- beim Enrollment zwei Aufnahmen vom selben Finger gemacht und gespeichert,
- bei der Verifikation zwei Aufnahmen vom selben Finger gemacht und verglichen,
- bei Enrollment und Verifikation zwei verschiedene Finger verwendet oder
- zwei unterschiedliche Algorithmen zur Fingererkennung verwendet werden.

Im günstigsten Szenario – zwei Finger statt nur einem – konnten die Fehlerraten auf rund ein Zehntel der ursprünglichen Werte reduziert werden.

BioMulti

BioMulti koppelt verschiedene biometrische Verfahren und basiert auf den Daten von BioP II. Das BSI hat im Jahr 2005 die Verfahren aus BioFinger II verfeinert, und zur Kopplung von

- Iris- und Gesichtserkennung,
- Gesichts- und Fingererkennung,
- Iris- und Fingererkennung sowie zur
- doppelten Fingererkennung

verwendet. Die Untersuchungen lassen bei diesen Kopplungen Fehlerraten erwarten, die etwa eine Zehnerpotenz kleiner sind als bei den einfachen Verfahren.

Reisepass mit biometrischen Merkmalen – ePass

Die Einführung des neuen elektronischen Reisepass (ePass) zum Stichtag 1. November 2005 setzte in Deutschland die Akzente in der Debatte um biometrische Merkmale in hoheitlichen Reisedokumenten.

Deutschland ist eines der ersten EU-Länder, das den ePass einführt. Im Chip enthalten sind biometrische Daten: zunächst das digitale Passfoto, ab März 2007 sollen zusätzlich die Fingerabdrücke digital erfasst werden.

Demonstration auf der Messe „Moderner Staat 2005“: Ohne entsprechende Berechtigung lässt sich der Chip im elektronischen Pass nicht auslesen – das BSI liefert die notwendige Software-Applikation, das „Golden Reader Tool“.

Die Staats- und Regierungschefs der EU hatten sich Mitte 2003 im Grundsatz darauf verständigt, biometrische Merkmale in die ePässe aufzunehmen. Eine entsprechende Verordnung erging im Dezember 2004. Danach müssen innerhalb von 18 Monaten alle EU-Mitgliedsländer Gesichtsbilder in digitaler Form in den Reisepass integrieren.

Das BSI hat bei der technischen Gestaltung der Sicherheitsspezifikationen maßgeblich in Gremien der International Civil Aviation Organization (ICAO) und der EU mitgewirkt. Dabei lag der Aufgabenschwerpunkt der „Projektgruppe Hoheitliche Dokumente“ im BSI bei der Realisierung der IT-Sicherheitskonzeption im neuen ePass.

Um die Diskussion über die Sicherheit des neuen Passes in der ...ffentlichkeit zu versachlichen, hat das Bundesamt auf einer eigenen Homepage alle technische Informationen zum ePass für interessierte Bürgerinnen und Bürger zur Verfügung gestellt.

Auskunft zum elektronischen Pass

Projektreferat Hoheitliche Dokumente und elektronische Ausweise

Postfach 20 03 63, 53133 Bonn

Internet: www.bsi.bund.de/fachthem/epass

E-Mail: ePass@bsi.bund.de

Hotline: 01805-274 300 *(12 ct/min, erreichbar von 8 bis 17 Uhr)*

Country Signing Certification Authority (CSCA)

Rechtzeitig zum Start der Produktion der ePässe hat das BSI in seiner Funktion als Country Signing Certification Authority (oberste Zertifizierungsstelle) in Deutschland die Bundesdruckerei GmbH mit Document Signer-Signaturschlüssel-Zertifikaten (DS) ausgestattet. Dadurch ist die Passproduzentin in der Lage, die Integrität und die Authentizität der im RF-Chip des ePasses gespeicherten Daten mit einer digitalen Signatur gegen nachträgliche Verfälschungen oder Manipulationen zu sichern.

So kann etwa bei einer Grenzkontrolle geprüft werden, ob die signierten Daten auf einem ePass von einer berechtigten Stelle erzeugt und seit der Erzeugung nicht mehr verändert worden sind. Durch die Integration dieser digitalen Signatur wird die Fälschungssicherheit des Reisespasses auf ein qualitativ neues Niveau gehoben.

Kein „magisches Auge" – dieser Mann nähert sich einem Irisscan-Gerät.

Digitale Sicherheitsmerkmale im ePass

• Extended Access Control – Die Sicherheitskonzeption des BSI

Ab 2007 sollen im EU-Reisepass neben dem Gesichtsbild zusätzlich die Fingerabdrücke auf einem RF-Chip gespeichert sein. Derart sensitive Daten müssen besonders stark vor unberechtigtem Auslesen geschützt sein. Das BSI hat dazu das Extended Access Control-(EAC)-Protokoll zum erweiterten Zugriffschutz entwickelt und der zuständigen EU-Arbeitsgruppe präsentiert. Das EAC-Protokoll sieht einen Authentisierungsmechanismus sowohl zur Echtheitsprüfung eines RF-Chips im ePass als auch für das Lesegerät vor. Das Lesegerät wird mit einem eigenen Schlüsselpaar und einem vom RF-Chip verifizierbaren Zertifikat ausgestattet, das definiert, auf welche Daten zugegriffen werden darf. Damit ist sichergestellt, dass Lesegeräte nur auf die Daten zugreifen können, für die sie auch legitimiert wurden.

• Das „Golden Reader Tool" – Basis für interoperable elektronische Reisepässe

Bei dem im Auftrag des BSI entwickelten „Golden Reader Tool" (GRT) handelt es sich um eine Software-Applikation zum Lesen von ICAO-konformen Reisepässen mit RF-Chip (eMRTD: electronic Machine Readable Travel Documents). Das BSI verfolgt mit dem GRT das Ziel, die Voraussetzungen für weltweite Interoperabilität im Bereich eMRTDs basierend auf den Vorgaben der ICAO zu schaffen. Tests in Singapore, Japan und in den USA haben bewiesen, dass das GRT weltweit einsetzbar ist. Das BSI hat damit die Grundlage geschaffen, ePässe praxisgerecht unter Beachtung der hohen Sicherheitsanforderungen weltweit nach einheitlichem Standard lesen zu können.

- **Protection Profiles für eMRTD**

Das BSI hat in den so genannten Protection Profiles (PP) die von den RF-Chips zu erfüllenden Sicherheitskriterien beschrieben. Die für die deutschen Reisepässe vorgesehenen RF-Chips wurden bereits nach Sicherheitskriterien der BSI-PP überprüft und zertifiziert. Inzwischen werden die Sicherheitskriterien der BSI-PP europaweit zur Prüfung ICAO-konformer Chips herangezogen.

Die Fotomustertafel der Bundesdruckerei zeigt, was bei Passfotos zu beachten ist. Sie müssen den Anforderungen der International Civil Aviation Organization (ICAO), einer Unterorganisation der Vereinten Nationen, genügen. Der alte Passbildautomat am Hauptbahnhof hat wohl bald ausgedient.

4 Prüfung, Bewertung, Zertifizierung

4.1 Technische Sicherheitsrichtlinien

Das BSI verfolgt mit der Veröffentlichung von technischen Richtlinien (TR) das Ziel, Vorgaben und Handlungsrahmen für die Entwicklung und den Einsatz sicherer und interoperabler IT-Sicherheitslösungen festzulegen.

Mit Hilfe der definierten Kriterien können geeignete Produkte ausgewählt und auf Konformität zur entsprechenden Richtlinie geprüft werden. Die technischen Richtlinien haben Empfehlungscharakter. Verbindlichkeit kann entstehen, wenn die Vorgaben der TR in Ausschreibungsverfahren Verwendung finden.

Technische Richtlinie Smart-Cards

Bei SmartCard-Lösungen steht einer breiten und kostengünstigen Verwendung häufig die fehlende Interoperabilität verschiedener Kartentypen und Hardwarekomponenten entgegen. Die Richtlinie des BSI zielt auf eine Erhöhung der IT-Sicherheit sowie eine standardkonforme, multifunktionale, interoperable und zukunftssichere Nutzung bestehender Karteninfrastrukturen. Die Technische Richtlinie für SmartCard-Lösungen besteht aus drei Teilen:

- **Teil 1: Chipkarten**

Dieser Teil beschreibt die Eigenschaften einer interoperablen und multifunktionalen Chipkarte unter Einbeziehung internationaler Standards und Einschränkung von Freiheitsgraden aus Gründen der Interoperabilität und Kompatibilität.
Funktionelle und sicherheitstechnische Anforderungen ergeben sich aus den operativen Zielen. Sie bilden zusammen mit anwendungsbedingten Anforderungen die Grundlage für Prüfungen im Rahmen einer Qualitätssicherung.

- **Teil 2: Chipkartenleser**

Teil zwei beschreibt die Anforderungen an interoperable und multifunktionale Chipkartenleser. Sie müssen sich für folgende Anwendungen eignen:

- Zutrittskontrolle,
- Zeiterfassung,
- Rechner-/Netzzugang,
- Bürokommunikation und firmeneigene Bezahlsysteme.

Als Basis dient die in Teil 1 spezifizierte multifunktionale Dual-Interface Chipkarte. Der Teil enthält sowohl Empfehlungen für preisgünstige Standardleser als auch für professionelle multifunktionelle Chipkartenleser, die für eine Vielzahl von derzeitigen und zukünftigen Chipkartenanwendungen geeignet sind.

- **Teil 3: Chipkartenspezifische Anforderungen an Anwendungen**

Der dritte Teil beschreibt die chipkartenspezifischen Anforderungen an Hintergrundsysteme, welche die Fähigkeiten der in Teil 1 der Technischen Richtlinien beschriebenen multifunktionalen Chipkarte nutzen. Die Richtlinie definiert konkrete Implementierungen, die ein funktionelles und sicheres Zusammenwirken zwischen Chipkarte und Hintergrundsystem gewährleisten. Gleichzeitig wird mit der Harmonisierung der Verfahren die Basis für ein einheitliches Berechtigungs-Managementsystem gelegt, das für weitere Systemanwendungen offen ist.

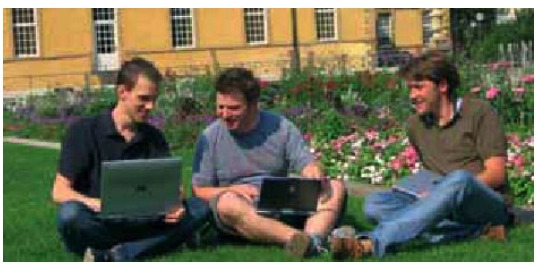
Die sichere Verifizierung elektronischer Signaturen ermöglichen spezielle SmartCards. Sie werden über ein Lesegerät mit dem Rechner verbunden.

Technische Richtlinie Sicheres Wireless LAN (TR-S-WLAN)

Die TR-S-WLAN soll die Entwicklung und den Betrieb sicherer, interoperabler und standardkonformer Wireless LAN Systeme und Infrastrukturen nach dem Standard IEEE 802.11 fördern. Die Technische Richtlinie (TR) liefert dazu konkrete Handlungsempfehlungen für die Planung, Beschaffung, Installation, Konfiguration, Abnahme, Administration und Außerbetriebnahme von sicheren Wireless LANs in der Wirtschaft sowie im Behördenbereich.

Die TR richtet sich an alle, die mit der Absicherung von WLAN-Installationen als Planer, Beschaffer, Betreiber oder Nutzer befasst sind. Sie erhalten Hilfestellung bei der Auswahl und Beschaffung sicherer, interoperabler und zukunftstauglicher WLAN-Systeme. Hersteller und Prüfinstanzen finden in der TR erforderliche Sicherheitsfunktionalitäten von WLAN-Produkten und Verfahren zur Prüfung.

Drahtlos ins Internet – dieser Router verfügt über mehrere Anschlüsse für DSL-Anbindung, Netzwerk und Funk.



Die drahtlose Anbindung macht's möglich: Studenten im Schlossgarten der Universität Osnabrück tauschen sich über ihre Laptops mit den Kommilitonen aus.

Die Technische Richtlinie Sicheres WLAN besteht aus mehreren Teilen:

- **Teil 1: Darstellung und Bewertung der Sicherheitsmechanismen**

In diesem Teil werden die wesentlichen marktgängigen und sich in der Standardisierung abzeichnenden Methoden und Mechanismen zur WLAN-Absicherung vorgestellt und bewertet. Außerdem werden Architekturen, Realisierungsalternativen und Anwendungsbereiche diskutiert.

- **Teil 2: Vorgaben eines WLAN Sicherheitskonzeptes**

Hier wird die Bedrohungslage analysiert und es werden allgemeine sowie szenarienspezifische Sicherheitsmaßnahmen abgeleitet. Der Aufbau orientiert sich an der Struktur und der Methodik des IT-Grundschutzhandbuchs. Ein Musterkonzept illustriert die Anwendung der Vorgaben.

- **Teil 3: Auswahl und Prüfung von WLAN-Systemen**

Der dritte Teil dieser Richtlinie ist in zwei Teildokumente aufgeteilt. Teil 3a definiert Kriterien für die Auswahl von WLAN-Systemen, das heißt nachprüfbare Produkteigenschaften der verschiedenen Komponenten eines WLAN-Systems. Dieses Dokument richtet sich vor allem an Beschaffer und Hersteller. Die Prüfkriterien im Teil 3b definieren Verfahren, mit deren Hilfe überprüft werden kann, ob die Anforderungen aus den Auswahlkriterien erfüllt werden. Je nach benötigter Vertrauenswürdigkeit des Prüfergebnisses werden drei Prüfklassen definiert, die von Herstellerangaben, über funktionale Labortests bis zur Evaluierung und Zertifizierung nach Common Criteria reichen.

Auf Basis der TR-S-WLAN können zukünftig spezielle Schutzprofile nach Common Criteria erstellt werden.

Diese Technische Richtlinie (TR) wendet sich an alle, die mit der Absicherung von WLAN-Installationen als Planer, Beschaffer, Betreiber oder Nutzer befasst sind. Ihnen wird Hilfestellung bei der Auswahl und Beschaffung sicherer und interoperabler WLAN-Systeme gegeben. Zu beziehen über den SecuMedia Verlag (www.secumedia.de) in gedruckter Form inklusive CD zum Preis von 75 Euro.

Surfen in der Straßenbahn: auch das ist per Funk möglich, wenn ein sogenannter Hotspot – ein Router mit Netzanbindung – vorhanden ist.

4.2 Wachsende Bedeutung von Zertifikaten

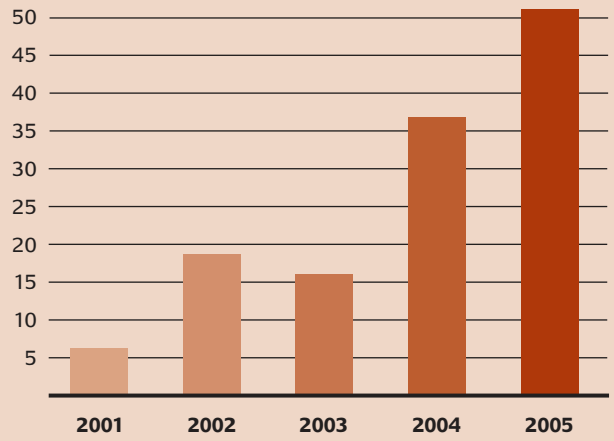
Die Zertifizierung von IT-Produkten auf Basis von international anerkannten IT-Sicherheitskriterien gewinnt für das BSI zunehmend an Bedeutung. Das Ziel der Zertifizierung, IT-Produkte und -Systeme hinsichtlich ihrer Sicherheitseigenschaften transparent und vergleichbar zu machen, ließ insbesondere die Nachfrage nach international anerkannten Zertifikaten auf Basis der Common Criteria (ISO/IEC 15408:1999) im vergangenen Jahr stark steigen.

Aufgrund dessen konnte das BSI im Jahre 2005 über 50 Zertifikate für ein weites Spektrum an unterschiedlichen Produkttypen, sowohl aus dem Hardware- als auch aus dem Software-Bereich ausstellen.

Beispielhaft für den Software-Bereich steht z/OS – ein Großrechner-Betriebssystem der Firma IBM. Dieses System erhielt ein Zertifikat für den Einsatz auf Rechnern der IBM zSeries.

Im Hardware-Bereich hat das BSI zahlreiche Zertifikate, vor allem auf dem Gebiet der SmartCard-Entwicklung ausgestellt. Unter anderem ging es dabei um die Verwendung in elektronischen Reisepässen.

Immer mehr Zertifikate



Ein neuer Höchststand bei der Vergabe von Zertifikaten wurde im Jahre 2005 erreicht: BSI-Zertifikate gingen an Hersteller aus dem Software-Bereich, wie z.B. IBM. Aber auch auf dem Gebiet der SmartCard-Entwicklung im Zusammenhang mit dem elektronischen Reisepass konnten die international anerkannten Bescheinigungen erteilt werden.

Wie im vorangegangenen konnten auch im Jahr 2005 einige Zertifikate und Reports für „Assurance Continuity“ überreicht werden. Bei diesem Verfahren wird bestätigt, dass trotz Veränderungen am Produkt das Zertifikat seine Gültigkeit behält. Insbesondere für Hardware-Hersteller bietet „Assurance Continuity“ eine signifikante Effizienzsteigerung bei der Zertifizierung ihrer Produkte.

Internationale Überprüfung bestanden: Blick auf das Gebäude des Bundesamtes für Sicherheit in der Infor mationstechnik an der Godesberger Allee in Bonn.

Zertifizierungsstelle des BSI: Überprüfung erfolgreich

Im Mai 2005 hat die Zertifizierungsstelle des BSI eine Überprüfung des CCRA erfolgreich absolviert. Das CCRA (Common Criteria Recognition Arrangement), ein internationales Abkommen zur Anerkennung von Zertifikaten, verlangt diese gegenseitige Überprüfung. Im CCRA sind aktuell 21 Nationen zusammengeschlossen. Vertreter aus den USA, Kanada und Schweden haben die Zertifizierungsstelle des BSI mit positivem Ergebnis überprüft. Die regelmäßige Überprüfung stellt sicher, dass alle Nationen gleichwertig hohe Qualitäts-Standards bei der Zertifizierung einhalten. Die Anforderungen im CCRA entsprechen im Wesentlichen den internationalen Standards DIN/EN 45011 beziehungsweise ISO-Guide 65. Als Grundlage für die Überprüfung diente das Qualitätsmanagementhandbuch der Zertifizierungs- und Akkreditierungsstelle.

Internationale Zusammenarbeit

Wie bei der Schutzprofilentwicklung *(siehe Kapitel „Profilierter Schutz“)* ist das BSI auch bei der Zertifizierung an vielen unterschiedlichen internationalen Projekten beteiligt. Dazu gehört zum Beispiel die Weiterentwicklung der Common Criteria auf Basis der Version 2.1.

Die neue Version 3.0 wird grundlegende Veränderungen bringen, die den aktuellen Entwicklungen in der Informationstechnik angepasst sind. Ziel ist es, Evaluierungen und Zertifizierungen effizienter und wirtschaftlicher zu gestalten. Die Version 3.0 wurde den entsprechenden ISO-Gremien bereits vorgelegt.

Aufgabe des BSI ist die Kommentierung neuer oder geänderter Teilbereiche. Auch die Revision einzelner Teile liegt in der Verantwortung des BSI. Dabei geht es um die Anpassung der Sicherheitsanforderungen an den Lebenszyklus der Produkte, die zertifiziert werden sollen und die entsprechende Bearbeitung der Handbücher.

Das BSI ist außerdem beteiligt an internationalen Projekten wie etwa der Zertifizierung verschiedener Systembestandteile des A400M-Flugzeugs. Dabei geht es hauptsächlich um Cockpit-Systeme.

Seit dem 1.1.2005 obliegt der Vorsitz des „Joint Certification“-Panel dem BSI. Diesem Panel gehören Deutschland, Spanien, Frankreich, Belgien, England und die Türkei an.

Der Airbus A400M (Simulation) – ein taktischer Militärtransporter mit großer Reichweite, einsatzfähig ab 2007.

Neue Prüfstellen lizenziert

Zu den bisher zwölf akkreditierten und lizenzierten Prüfstellen sind 2005 zwei weitere hinzugekommen, die das Verfahren zu einer Lizenzerteilung erfolgreich absolviert haben. Seit Mitte 2005 sind die Firmen „media transfer AG“ und „Secunet SwissIT AG“ berechtigt, IT-Produkte hinsichtlich ihrer Sicherheitseigenschaften gemäß den internationalen Sicherheitskriterien (Common Criteria) im Rahmen von BSI-Zertifizierungsverfahren zu prüfen.

IT-Sicherheit hängt nicht nur von der Technik und den verwendeten Produkten ab. Organisatorische und personelle Rahmenbedingungen spielen eine ebenso wichtige Rolle. Neben der Produktzertifizierung nach den Common Criteria besteht für Firmen die Möglichkeit, ihre Geschäftseinheiten oder -abläufe zertifizieren zu lassen.

IT-Grundschutz: Die Fortentwicklung

Das IT-Grundschutzhandbuch, das seit Jahren kontinuierlich weiterentwickelt wird, bietet dazu die entsprechenden Grundlagen. Durch die darin festgelegten Standard-Sicherheitsmaßnahmen lässt sich ein angemessenes Sicherheitsniveau für typische IT-Systeme erreichen. Das Vorgehen nach IT-Grundschutzhandbuch ist Voraussetzung für die Erteilung eines Zertifikats. 2005 wurde die Entwicklung der neuen ISO 27001-Zertifikate auf Basis des IT-Grundschutzes abgeschlossen. Sie werden ab Anfang 2006 zur Verfügung stehen.

BSI-Präsident Dr. Udo Helmbrecht zusammen mit Abteilungsleiter Bernd Kowalski und Referatsleiter Jürgen Schwemmer von der Bundesnetzagentur bei der Übergabe eines IT-Sicherheitszertifikats an Dr. Rüdiger Mock-Hecker, Leiter der Geschäftssparte Kartensysteme des Deutschen Sparkassenverlages, für die elektronische Signatursoftware des Deutschen Sparkassenverlages „S-TRUST Sign-it“ im Rahmen der Fachmesse Systems.

4.3 Profilierter Schutz

Sogenannte Schutzprofile (Protection Profiles) formulieren Anforderungen für Produktklassen (zum Beispiel Firewalls, Geldkarten oder Betriebssysteme), ohne dabei auf ein konkretes Produkt Bezug nehmen zu müssen.

Mit Schutzprofilen können Anforderungen an die IT-Sicherheit einer ganzen Kategorie von IT-Produkten oder IT-Systemen definiert werden, ohne dabei auf eine konkrete Implementierung eines IT-Produkts oder Systems Bezug zu nehmen. Mit Hilfe der Anforderungen aus den Common Criteria wird eine Musterlösung auf angemessen abstrakter Ebene beschrieben. Auf diese Weise haben Autoren von Schutzprofilen die Möglichkeit, Standards zu setzen, die dann national wie international Anerkennung finden.

Das Konzept der Schutzprofile erhöht die Vergleichbarkeit von Produktevaluationen nach den CC erheblich. Bedingt durch das allgemeine Sicherheitskonzept eines Schutzprofils ist für den IT-Anwender eine gute Vergleichbarkeit verschiedener Produkte gewährleistet, die auf Basis ein und desselben Schutzprofils entwickelt und evaluiert worden sind. Beschaffer von IT können sich diese Möglichkeiten zu Nutze machen. Sie können bei Ausschreibungen die Konformität zu einem bestimmten Schutzprofil im Lastenheft verlangen. Dies ist in manchen Bereichen bereits gängige Praxis, wie z.B. bei der Abfallentsorgung sowie bei der digitalen Signatur.

Zertifizierte Schutzprofile werden auf der offiziellen „Common Criteria“-Website und den entsprechenden nationalen Websites der Zertifizierungsstellen veröffentlicht. Sie stehen als Grundlage für die Evaluierung und Zertifizierung von IT-Produkten zur Verfügung.

Schutzprofile für verschiedene Produktklassen

Im Jahr 2005 wurden im Auftrag des BSI mehrere Schutzprofile für unterschiedliche Produktklassen entwickelt und durch das BSI zertifiziert. Dazu im Folgenden einige Beispiele:

- **Biometrische Verifikationssysteme**

Ein zu diesem Schutzprofil konformes biometrisches Verifikationssystem dient dazu, die vorgegebene Identität eines Benutzers durch eindeutige Merkmale seines Körpers zu verifizieren, um den Zutritt zu einem Portal zu kontrollieren.

- **Elektronische Gesundheitskarten**

Dieses Profil legt die Anforderungen zur Verwendung einer elektronischen Gesundheitskarte basierend auf den Vorschriften des deutschen Gesundheitssystems fest.

• **IT-gestützte Verarbeitung von personenbezogenen Daten**
In diesen Schutzprofilen sind die logischen funktionalen Komponenten (Aufzeichnungs- und Bediengeräte für Benutzung, Administration und Revision) für Videoüberwachungsanlagen beschrieben.

• **Reisepass/Kartenlesegerät**
Angelehnt an den ICAO-Standard (International Civil Aviation Organisation) wird es zur Datenübertragung zwischen einem elektronischen Reisepass und dem Kartenlesegerät eingesetzt. Das ICAO-Schutzprofil dient in der Variante „Basic Access Control“ zur Authentifizierung zwischen Karte und Leser. Dieses Schutzprofil wurde nach internationalen Absprachen zu elektronischen Reisedokumenten im Auftrag des Bundesministerium des Innern entwickelt und zertifiziert. Es beschreibt dabei die Ziele und Anforderungen an den kontaktlosen Chip.

Auch die neue elektronische Gesundheitskarte ist mit einem Schutzprofil ausgestattet. In die Gestaltung der Technik ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) bei allen Schritten einbezogen.

Gerade beim Check-In auf dem Flughafen werden Daten übertragen, eingelesen und ausgedruckt. Schutzprofile sorgen dafür, dass die Datenübertragungswege nicht abgehört oder ausspioniert werden können.

Systeme mit geringerem Schutzbedarf

Im Rahmen von Projekten zur Evaluierung von Schutzprofilen mit Anforderungen aus der Version 2.4 der „Common Criteria“ wurden mehrere Low Assurance Schutzprofile entwickelt, in denen die Anforderungen an Systeme mit geringem Schutzbedarf beschrieben werden. Ziel dieser Low Assurance Profile ist, den Einstieg in eine Common Criteria Zertifzierung zu erleichtern. Zertifizierte Low Assurance Schutzprofile werden im Folgenden kurz dargestellt:

• **Low Assurance Protection Profile for an Office Based Photocopier Device**
Dieses Schutzprofil definiert funktionale Anforderungen und Kriterien an die Vertrauenswürdigkeit eines Fotokopierers in einer gängigen Büroumgebung. Ein zu diesem Schutzprofil konformer Fotokopierer ist ein eigenständiges Gerät, das ohne weitere Hardware, Firmware oder Software auskommt.

• **Low Assurance Protection Profile for a Software Based Personal Firewall for home Internet use**
Dieses Schutzprofil definiert funktionale Anforderungen und Anforderungen an die Vertrauenswürdigkeit einer Personal Firewall. Eine zu diesem Schutzprofil konforme Firewall ist ausschließlich als Software zu implementieren und für die Anbindung eines privaten PCs an das Internet gedacht.

• **Low Assurance Protection Profile for a VPN Gateway**
Dieses Schutzprofil spezifiziert sowohl funktionale als auch Vertrauenswürdigkeitsanforderungen für Virtual Private Network (VPN) Gateways. Es definiert die Sicherheitsanforderungen von VPN-Gateways für die Identifikation und Authentisierung von Benutzern, das Management der Gateways, vertrauenswürdige Kanäle und den Selbstschutz der Gateways.

• **Low Assurance Protection Profile for a Voice over IP Infrastructure**
Dieses Schutzprofil spezifiziert sowohl funktionale als auch Vertrauenswürdigkeitsanforderungen für „Voice over IP"-Infrastrukturen (VoIP). Das Schutzprofil definiert die Sicherheitsanforderungen von VoIP-Infrastrukturen für die Identifikation und Authentisierung von Benutzern, das Management der Infrastruktur, die Protokollierung und den Selbstschutz des Systems.

Ein weiteres Projekt im Zusammenhang mit der Erstellung von Schutzprofilen ist für das BSI die Konvertierung bereits bestehender Schutzprofile auf die Anforderungen der neuen Version 3.0 der „Common Criteria". Dabei steht das Schutzprofil „Smartcard IC Platform Protection Profile", in dem bedeutende Hardwarehersteller Sicherheitsanforderungen an den Integrated Circuit (IC) beschreiben, im Vordergrund. Dieses Schutzprofil, das die neuesten Ansätze zur Modularität und Wiederverwendung von Evaluierungsaufwänden beschreibt, wird mit Unterstützung des BSI dem neuen Standard angepasst. Das BSI begleitet dabei sowohl die redaktionelle Arbeit als auch die Evaluierung des Schutzprofils. Eine Zertifizierung auf Basis der „Common Criteria" in der Version 3.1 ist für Mitte des Jahre 2006 geplant.

In Zusammenarbeit mit der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen sind weitere Projekte geplant, bei denen mehrere Schutzprofile entwickelt werden. Die fachliche Betreuung der Entwicklung der Schutzprofile für sichere Signaturerstellungseinheiten (SSEE), Signaturanwendungskomponenten (SAK) und technische Komponenten für Zeitstempeldienste (TSS) wird durch das BSI durchgeführt.

Ziel der Schutzprofile ist es, einheitliche IT-Sicherheitsstandards als Sollvorgaben für SSEE, SAK und TSS zu schaffen, die den Herstellern als Entwicklungsspezifikation der benötigten Sicherheitsfunktionalität dienen.

Gesundheitskarte mit Lesegerät. Der Zugriff erfolgt grundsätzlich nach dem Zwei-Schlüssel-Prinzip: Nur wenn Arzt und Patient gleichzeitig ihre Schlüssel nutzen, sind die Daten lesbar.

5 Exakt messen – sicher arbeiten: IT und Geheimschutz

5.1 Abstrahlgeschützte Hardware

Jedes elektronische Gerät strahlt mehr oder weniger starke elektromagnetische Wellen ab. Diese Abstrahlung wird Störstrahlung genannt. Bei Geräten, die Informationen verarbeiten – wie einem PC – kann sie auch die gerade verarbeiteten Informationen mit sich führen. Damit wird sie zur „bloßstellenden Abstrahlung“.

Wird diese Strahlung in einiger Entfernung empfangen, z.B. in einem Nachbarhaus oder auch in einem in der Nähe abgestellten Fahrzeug, kann daraus die Information rekonstruiert werden. Die Vertraulichkeit der Daten ist in Frage gestellt. Abstrahlschutz bedeutet die Verminderung der sogenannten bloßstellenden Abstrahlung auf Werte, die ein tragbares Risiko darstellen.
Die NATO hat ein Regelwerk zur Beherrschung der bloßstellenden Abstrahlung geschaffen. Es beschreibt die Verfahren zur Feststellung des Informationsanteils der Abstrahlung und legt entsprechende Grenzwerte fest. Diese Messvorschriften sind für den nationalen Gebrauch übernommen worden. Das BSI wendet sie auch bei seinen Zulassungsuntersuchungen an. Das NATO-Regelwerk sieht drei Grenzwert-Kategorien vor, aus denen sich unterschiedlich stark entstörte Geräteklassen ergeben. Sie beschreiben den Abstrahlschutz an dem elektronischen Gerät selbst.

Das Zonenmodell

Das BSI ist noch einen Schritt weiter gegangen und hat ein sogenanntes Zonenmodell entwickelt. Es geht davon aus, dass elektromagnetische Felder durch die Entfernung schwächer und durch die Struktur eines Gebäudes (Bunker, Holzhaus) messbar gedämpft werden. Das BSI hat daraus drei Kategorien entwickelt, die einen Betriebsstandort in „Zone 1“ (wenig gedämpft), „Zone 2“ (mittel gedämpft) oder „Zone 3“ (stark gedämpft) einteilen. Ist keine ausreichende Dämpfung in dieser Klassifizierung feststellbar, kann das Zonenmodell auf den Betriebsstandort nicht angewendet werden. Der Standort ist nicht abstrahlsicher, fällt also unter die Kategorie „Zone 0“.

Ähnlich wie bei der gesetzlich vorgeschriebenen Prüfung zur Elektro-Magnetischen Verträglichkeit (EMV), wird der Abstrahlpegel auch im Zonenmodell unter möglichst realitätsnahen Bedingungen gemessen, allerdings mit eigenen Grenzwerten und Bandbreiten. Der Signalinhalt wird nicht analysiert. Dadurch sind die Prüfungen schnell durchführbar; mit dem vom BSI entwickelten automatisierten Messverfahren können heute bis zu zwei Geräte am Tag untersucht werden. Pro Woche erhalten so durchschnittlich sechs bis acht IT-Geräte (PC, Drucker, Server oder andere Systembestandteile), die Verschlusssachen in elektronischer Form verarbeiten, eine Zulassung für den Einsatz im Rahmen des Zonenmodells (veröffentlicht auf der BSI-Website unter „Liste der für staatliche Verschlusssachen zugelassene abstrahlsichere/-arme Hardware“ – TL 03305).

Blick in eine Messzelle. Sie kann die Stärke der bloßstellenden Abstrahlung eines IT-Gerätes bestimmen.

Bei der Informationsverarbeitung wird an jedem PC eine gewisse Menge Strahlung freigesetzt, die mit entsprechenden Geräten aufgefangen und entschlüsselt werden kann.

Gesetzliche Anforderungen gestiegen

Aufgrund der in den vergangenen Jahren gestiegenen gesetzlichen Anforderungen an den EMV-Schutz bestehen viele IT-Geräte heute die „Zone 2"-Prüfung ohne oder mit nur geringfügigen zusätzlichen Entstörmaßnahmen. Die Geräte sind so sicher, dass sie in Gebäuden, die eine mittlere Dämpfung der Abstrahlung gewährleisten, eingesetzt werden können. Für „Zone 1" (wenig Dämpfung) sind aber zusätzliche Entstörmaßnahmen erforderlich. „Zone 3" setzt eine starke Dämpfung voraus und verlangt vom Gerät selbst den geringsten Abstrahlschutz. Die obere Grenze einer zulässigen Abstrahlung legt das Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) fest. Wer allerdings in einer „Zone 0"-Umgebung sicher arbeiten möchte, muss so strenge Anforderungen an die Geräte stellen, dass die klassischen Entstörmaßnahmen der EMV nicht zum Erfolg führen. Es ist nicht möglich, die Abstrahlung so zu vermindern, dass die Grenzwerte der „Zone 0" nicht mehr überschritten werden. Deswegen werden eigene signalanalytische Verfahren eingesetzt, die sicherstellen, dass der informationstragende Anteil der Störstrahlung die Grenzwerte nicht überschreitet. Dazu müssen diese Signale identifiziert und gezielt vermindert werden – eine Aufgabe, die Wochen oder sogar Monate in Anspruch nehmen kann und entsprechende Kosten für die Entwicklung der Entstörung verursacht. „Zone 0"-Geräte werden daher nur dort eingesetzt, wo es unvermeidbar ist.

Im Gegensatz zu den oben behandelten IT-Geräten sind bei Kryptogeräten für den Geheimschutz analytische Untersuchungen obligatorisch. Im Jahre 2005 wurden unter anderem das Schlüsselgerät ElcroDat 4-2, ein System für die Verbindung analoger und digital verschlüsselter Telefonsysteme (Red Gateway) und das Schlüsseleingabegerät DTD zugelassen. Ein Kryptofunkgerät für das Jagdflugzeug 2000 und ein Schlüsselverteilgerät für Hubschrauber sind neben anderen Geräten in der Bearbeitung.

Das „Jagdflugzeug 2000" ist als Kampflugzeug der vierten Generation mit modernster Technik ausgestattet. Piloten der Bundeswehr flogen Ende 2005 die ersten Probeeinsätze.

Zusammenarbeit mit der Bundeswehr

Für IT-Geräte, die nach dem Zonenmodell zugelassen sind, hat das BSI ein verkürztes Prüfverfahren entwickelt, mit dem die Qualität am Einzelgerät nachgewiesen und das von „anerkannten Labors“ durchgeführt wird.
Bei Geräten, die so abstrahlsicher sind, dass sie für den Einsatz in „Zone 0“ zugelassen sind, ist dieses Verfahren zu pauschal. Es kann die besonderen Entstörmaßnahmen nicht erfassen. Hier kommen sogenannte Kurzmessverfahren, die das BSI explizit für das zu prüfende Gerät ausarbeitet, zum Einsatz.
Auch die Erstvermessung mobiler Systeme der Bundeswehr fällt in die Zuständigkeit des BSI – vom Geländewagen mit IT- und Kommunikationsausstattung bis zur Fregatte oder zum Großraumflugzeug. Diese Erstvermessungen werden in enger Zusammenarbeit mit dem Abstrahlprüfdienst der Bundeswehr durchgeführt, der dann auch die Einzelprüfungen weiterer gleichartiger Systeme durchführt. Für das Jahr 2005 ist hier insbesondere ein Aufklärungssystem (KWS_RMB) der Streitkräfte zu nennen.

Weitere Systeme haben Experten des BSI an den jeweiligen Standorten gemeinsam mit dem Abstrahlprüfdienst der Bundeswehr untersucht. Sie haben die Streitkräfte in vielen Fällen beraten, die durch Systemänderungen bei der Modernisierung der Bundeswehrnetze verursacht wurden.
Auch bei der internationalen Zusammenarbeit bringt das BSI seine Kompetenz mit ein. So war für das Jahr 2005 die Erstvermessung einer norwegischen Fregatte als gemeinsames Projekt der norwegischen Behörde, des Abstrahlprüfdienstes der Bundeswehr und des BSI geplant, musste aber auf das Jahr 2006 verschoben werden. Als Fachbehörde ist das BSI in den Facharbeitsgruppen internationaler Projekte wie „Jagdflugzeug 2000“, „Nato-Hubschrauber NH 90“ und „Transportflugzeug A400M“ tätig. Mit den Untersuchungen zur Abstrahlsicherheit an der Informationstechnik, die für Verschlusssachen genutzt wird, leistet das BSI einen wichtigen Beitrag zur IT-Sicherheit im Geheimschutz.

Abstrahlprüfungen hat das BSI in Zusammenarbeit mit der Bundeswehr beispielsweise für Geländewagen mit IT- und Kommunikationsausstattung (oben) sowie für den NATO-Hubschrauber NH 90 (links) vorgenommen.

5.2 Prüfverfahren bei der Lauschabwehr

Das BSI entwickelte im Jahre 2005 seine Messsysteme und Prüfmethoden weiter, um die Vertraulichkeit von persönlichen und telefonischen Gesprächen zu gewährleisten. Denn zu seinen Aufgaben gehört auch der Schutz des gesprochenen Wortes im Bereich der staatlichen Geheimhaltung: die Lauschabwehr. Im Folgenden werden einige ausgewählte Prüfverfahren vorgestellt.

„Wanzen“ kennt jeder Laie aus Agentenfilmen. Die Miniatur-Lauschgeräte, die das illegale Abhören von Gesprächen möglich machen, übertragen die abgehörten Inhalte per Funk. Dabei übersieht man leicht, dass schon eine schlecht schallgedämmte Tür oder ein einfach verglastes Fenster reichen, um Gespräche auf dem Flur oder auf der Straße mitzubekommen – sei es mit bloßem Ohr oder mit einem technischen Hilfsmittel wie dem Richtmikrofon.

Wer sich also nicht so leicht belauschen lassen möchte, muss dafür sorgen, dass Fenster und Türen, Wände, Decken und Fußböden ausreichend schallgedämmt sind. Das BSI setzt zur messtechnischen Beurteilung der Schalldämmung ein so genanntes Bauakustik-Messsystem ein. Mit den gewonnenen, normgerechten Messergebnissen können Mängel gezielt beseitigt werden.

„Wanzen“, oder fachlich ausgedrückt Funk-Lauschgeräte, senden auf bestimmten Frequenzen, die sich mit speziellen Messempfängern, zum Beispiel Spektrum-Analysatoren, identifizieren lassen. Doch ein solches Signal zweifelsfrei zu orten ist sehr aufwändig, da unter den Frequenzen einer Vielfalt von legalen Sendern, wie Radio- und Fernsehsendern, Mobiltelefonen, Datenfunkverbindungen, gesucht werden muss. Die „Wanze“ wird zur Stecknadel im Heuhaufen.

Endoskopische Untersuchung eines Kabelschachtes im Rahmen der Lauschabwehr: Auf dem Monitor sind die Bilder zu sehen, die das biegsame Rohr mit der Kamera aus dem Innern der Kabelkanäle auffängt.

Abhörsicherheit muss auch für die modernsten Geräte gewährleistet sein. Ein mobiles Videotelefon ist heute nicht größer als ein Laptop.

Mit Taschenlampe und Spiegel

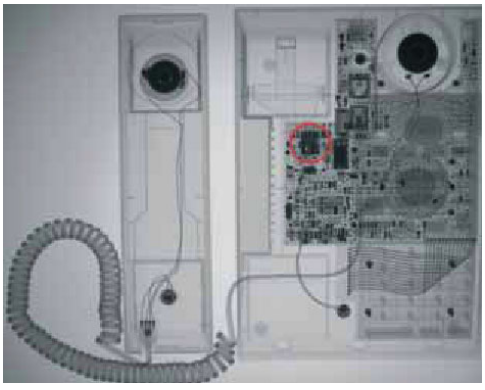
Und was passiert, wenn das Funk-Lauschgerät einfach ausgeschaltet wurde? Moderne Fabrikate sind fernsteuerbar, und wenn sie vor der Überprüfung deaktiviert wurden, findet das Messgerät nichts. Außerdem sind Lauschgeräte auf dem Markt, die als Übertragungsmedium statt Funk elektrische Leitungen oder Infrarotlicht nutzen. Die wichtigste Lauschabwehr-Prüfmaßnahme ist daher nach wie vor die so genannte visuelle Überprüfung. Mit diversen Hilfsmitteln – von einfachen wie Taschenlampen und Spiegeln bis zum hochwertigen Endoskop – werden Möbel und Einrichtungsgegenstände, Hohlräume in Wänden und Decken, aber auch Elektrogeräte auf unerwünschte Einbauten untersucht.

Doch was ist mit Gegenständen, die nicht zerlegt werden können? Oder mit hochwertigen technischen Geräten, bei denen man Gefahr läuft, sie zu beschädigen, wenn sie zerlegt werden? In diesen Fällen wird ein modernes Röntgensystem eingesetzt. Durch die Verwendung eines hoch empfindlichen Sensors kann die erforderliche Röntgenstrahlung so gering gehalten werden, dass eine Gefährdung des Prüfpersonals durch die Strahlung ausgeschlossen ist.

Bei elektrischen Leitungen – dazu zählen auch solche für Telekommunikation und Informationstechnik – besteht nicht nur die Gefahr, dass sie als Übertragungsmedium für abgehörte Gespräche missbraucht werden. Sie können außerdem auch zur Stromversorgung der „Wanzen“ dienen. Also ist die Überprüfung der Leitungen mit speziellen Messgeräten ebenfalls unverzichtbar für die Lauschabwehr.

Besonders schwierig ist der Nachweis von Lauschgeräten, die in die Bausubstanz, also Wänden, Decken und Fußböden eingebaut wurden. Als Standard-Messgerät für die zerstörungsfreie Untersuchung von Bausubstanz hat sich der so genannte Nichtlinearitäten-Detektor bewährt. Dieses Gerät reagiert auf elektronische Schaltungen aller Art, also auch auf Lauschgeräte. Wegen der hohen Empfindlichkeit dieses Messverfahrens sind allerdings Fehlalarme an der Tagesordnung. Da hilft die Kombination mehrerer Untersuchungsmethoden. Zum Beispiel mit einer Wärmebildkamera: Lauschgeräte verbrauchen Strom, also erwärmen sie sich leicht gegenüber der Umgebung. Die Wärmebildkamera zeigt die Temperaturunterschiede.

Links: Untersuchung einer Wand mit dem Nichtlinearitäten-Detektor. Das Gerät reagiert auf Unregelmäßigkeiten bei elektrischen Schwingungen.



Das Röntgenbild (rechts) zeigt einen Telefonapparat mit eingebautem Lauschgerät, das zur Verdeutlichung nachträglich mit einem Kreis markiert wurde.

Schutz für digitale Telefonanlagen

Ein besonders hohes Abhörrisiko kann beim Einsatz von modernen digitalen Telefonanlagen bestehen. Diese Anlagen sind durchgehend mit Leistungsmerkmalen ausgestattet wie der „Babyfon“-Funktionen zur akustischen Überwachung eines Raums, dem direkten Ansprechen eines Telefonapparates, dem Aufschalten auf Telefongespräche und Konferenzschaltungen, die für bestimmte Anwendungsfälle sinnvoll sind und den Komfort erhöhen. Wer illegal abhören will, kann diese Funktionen aber auch leicht missbrauchen.

Viele Anlagen lassen sogar die Möglichkeit zu, kritische Warntöne und Anzeigen im Telefondisplay zu unterdrücken. Wer die Telefonanlage entsprechend manipulieren kann, bleibt unentdeckt. Die Einstellungen müssen noch nicht mal im direkten Zugriff vorgenommen werden. Das geht oft auch über einen Fernwartungszugang, wenn er nicht genügend abgesichert ist.

Das BSI überprüft bei Lauschabwehrprüfungen, ob in der Telefonanlage Leistungsmerkmale mit möglicher Abhörfunktion geschaltet sind. Für die in der Bundesverwaltung am häufigsten eingesetzten Anlagentypen wurden beim BSI Software-Tools entwickelt, die diese Aufgabe weitgehend automatisch erledigen. Bei dieser Gelegenheit wird auch die ausreichende Absicherung des Fernwartungszugangs, sofern vorhanden, überprüft.

Die Schilderung der möglichen Lauschabwehr-Prüfverfahren kann aus verständlichen Gründen nicht vollständig sein. Dennoch sollte deutlich geworden sein, dass auf die immer ausgefeilteren Methoden des illegalen Abhörens mit entsprechend differenzierten Prüfmaßnahmen reagiert werden muss. Lauschabwehrprüfungen, die nicht einen gewissen Mindeststandard aufweisen, sind unseriös.

Lauschabwehrprüfungen sind außerdem immer nur eine Momentaufnahme. Sie ersetzen nicht die notwendigen personellen und materiellen Sicherungsmaßnahmen. Nur so lässt sich der Einbau von Lauschmitteln in gefährdete Räume wirklich verhindern.

Mit einem Telefon, das auf akustische Raumüberwachung gestellt ist, ließe sich zum Beispiel diese Konferenz mühelos überwachen und mitschneiden.

5.3 Dämpfungsmessungen in Liegenschaften und Gebäuden

Eine Möglichkeit, sich unbefugt vertrauliche Informationen zu beschaffen, ist der Empfang der bloßstellenden elektromagnetische Abstrahlung von IT-Geräten (siehe Kapitel „Abstrahlgeschützte Hardware“). Soll dies verhindert werden, sind besondere Schutzmaßnahmen notwendig.

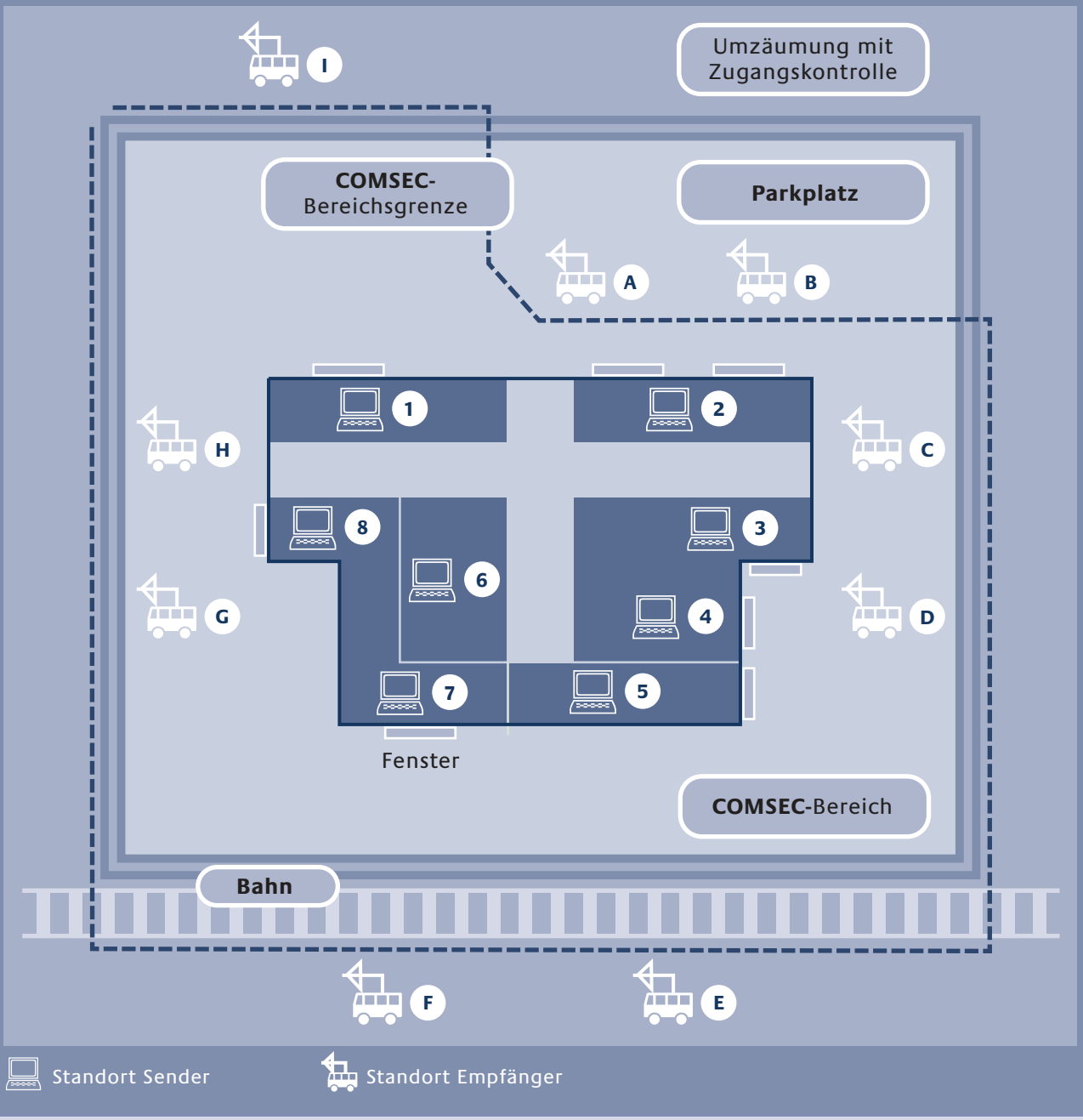
Der Schutz kann beispielsweise darin bestehen, die IT-Geräte selbst so abzuschirmen, dass sie keine bloßstellende Abstrahlung mehr aussenden. Solche Geräte, die sogenannten „TEMPEST“-Geräte, sind allerdings extrem teuer. Sie werden deshalb nur dort eingesetzt, wo besonders hohe Anforderungen an den Abstrahlschutz gestellt werden. Eine andere Methode ist die Bildung einer Sicherheitszone um die IT-Geräte herum. Bei dieser Methode muss jedoch der Nachweis erbracht werden, dass die bloßstellende Abstrahlung an der Grenze der Sicherheitszone tatsächlich auf ein nicht mehr verwertbares Maß abgeklungen ist. Die Nachweisgrenze für die bloßstellende Abstrahlung wird, sofern staatliche Verschlusssachen zu schützen sind, durch einschlägige Vorschriften der NATO definiert. Wie stark die bloßstellende Abstrahlung, vom IT-Gerät bis zum Empfänger, dem potentiellen Angreifer, bis zur Bereichsgrenze gedämpft wird, hängt von vielen Faktoren ab. Neben der räumlichen Distanz spielt die Infrastruktur und die Bausubstanz des Gebäudes eine entscheidende Rolle. Da diese Einflüsse allein auf Grundlage von Planungsunterlagen kaum zu erfassen sind, bleibt nur die Möglichkeit, die Dämpfung an Ort und Stelle messtechnisch zu ermitteln.

Die Vermessung der Liegenschaft

In einem ersten Schritt müssen die Grenzen des Sicherheitsbereiches festgelegt werden. Dieser muss durch Sicherungsmaßnahmen so kontrollierbar sein, dass sich Angriffsversuche von dort ausschließen lassen. Dieser Bereich muss nicht zwangsläufig mit der Grundstücksgrenze übereinstimmen. Einerseits können schwer kontrollierbare Flächen der Liegenschaft, wie z.B. ein frei zugänglicher Parkplatz, herausgenommen werden. Andererseits kann der Sicherheitsbereich aber auch um externe Flächen, auf denen sich niemand längere Zeit unbemerkt aufhalten kann, erweitert werden. Dies kann zum Beispiel für ein angrenzendes Bahngelände oder eine stark befahrene Straße gelten.

Nachdem die Bereichsgrenze festgelegt wurde, gilt es messtechnisch zu ermitteln, wie stark die bloßstellende Strahlung auf ihrem Weg von der Quelle bis zur Bereichsgrenze abgeschwächt wird. Dazu wird in dem zu vermessenden Raum ein Sender aufgestellt, der ein Signal abstrahlt, das an der Bereichsgrenze empfangen wird. Bezogen auf den Grad der Dämpfung, welche die abgestrahlte Leistung des Senders auf dem Weg zum Empfänger erfährt, wird der Raum einer bestimmten Zone zugeordnet. Je nach Lage bzw. Art des zu vermessenden Raumes können mehrere Messungen zu verschiedenen Empfangsstandorten notwendig sein. Nach festgelegten Bewertungsmerkmalen ergibt sich aus den Messwerten die „Zone“ für den entsprechenden Raum. Dabei bestimmt das Ergebnis mit den niedrigsten Werten die Einstufung.

Versuchsmessanlage zur Bestimmung der Abstrahlsicherheit



Die Zahlen 1 bis 8 entsprechen den Raumnummern und gleichzeitig den Senderstandorten, während die Buchstaben A bis I die Empfängerstandorte außerhalb und innerhalb der Umzäunung an der Bereichsgrenze darstellen. Gemessen wird, welche Dämpfungsleistung vorliegt, wenn IT-Geräte in den verschiedenen Räumen eingesetzt werden und wie stark sie außerhalb der Bereichsgrenze abfällt. Aus der Kombination von gemessener Abstrahlsicherheit am Gerät selbst und Dämpfungsleistung ergibt sich, welches Gerät sicher an welcher Stelle eingesetzt werden kann.

Die Empfängereinheit – als Teil eines Messsystems, das Zonen klassifizieren kann.

Die Zonenbewertung

Bezogen auf eine Referenzmessung in 20 m Freiraumabstand zwischen Sender und Empfänger gibt es folgende Zoneneinteilungen:

- Zone 1 entspricht einer Dämpfung äquivalent zu 20 Meter Freiraum
- Zone 2 entspricht einer Dämpfung äquivalent zu 100 Meter Freiraum und
- Zone 3 ergibt sich aus Zone 2 plus 20 dB.

Zone 1 ist der Bereich mit der geringsten, Zone 3 der mit der größten Dämpfung. Zone 0 wird für Räume vergeben, die die Mindestanforderungen an die Dämpfung nicht erreichen. Hier müssen sonderentstörte Geräte (TEMPEST-Geräte) eingesetzt werden.

Einschränkungen

Das Zonenmodell kann nur auf Gebäude und Liegenschaften sowie ortsfest eingesetzte mobile Einrichtungen angewendet werden, für die eine klar definierbare Bereichsgrenze außerhalb des Gebäudes festgelegt werden kann. Einzelne Etagen oder Räume innerhalb von Gebäuden können nicht gegenüber anderen Etagen bzw. Räumen „verzont“, also klassifiziert werden.

Dies ist darin begründet, dass die Störstrahlung der IT-Geräte auf verschiedene metallische Leiter einkoppeln kann, die diese über weite Strecken innerhalb des Gebäudes unkontrollierbar verteilen. Da sich diese Ausbreitung nicht mit vertretbarem Aufwand unterbinden lässt, muss die Bereichsgrenze außerhalb des Gebäudes liegen.

Aktivitäten

Die Vermessung von Liegenschaften nach dem Zonenmodell ist eine der Aufgaben des BSI. Das Bundesamt ist sowohl für Bundesbehörden als auch über das Bundesministerium für Wirtschaft (BMWi) für die geheimschutzbetreute Wirtschaft tätig. In allen Fällen handelt es sich immer um Objekte, in denen vertrauenswürdige Daten verarbeitet werden, die einem besonderen Schutz unterliegen. Das BSI bietet seinen Kunden an, sie in Fragen der Abstrahlsicherheit umfassend und bereits im Vorfeld der Planungen zu beraten.

Durch die unabhängige Feststellung der Gebäudedämpfung und Störstrahlung der Geräte stellt das Zonenmodell für den Anwender eine Erleichterung bei der Auswahl und dem Einsatz von elektronischem Gerät für die Verarbeitung von vertraulichen Daten dar. Das Zonenmodell ist anwendbar für Gebäude und Liegenschaften, die die Kriterien für die Festlegung eines Sicherheitsbereiches erfüllen. Ist dies nicht der Fall, ist der Einsatz von zugelassenem abstrahlfreiem IT-Gerät für die Verarbeitung von vertraulichen Daten notwendig.

Rechts im Bild: die zu einem klassifizierten Messsystem gehörende Sendereinheit.

Dr. Udo Helmbrecht,

Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Michael Hange,

Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik

Dr. Hartmut Isselhorst,

Leiter der Abteilung 1 – Sicherheit in Anwendungen, Kritischen Infrastrukturen und im Internet

Dr. Gerhard Schabhüser,

Leiter der Abteilung 2 – Kryptologie und Abhörsicherheit

Bernd Kowalski,

Leiter der Abteilung 3 – Zertifizierung, Zulassung und Konformitätsprüfungen

Horst Samsel,

Leiter der Abteilung Z – Zentrale Aufgaben

Anja Hartmann,

Referatsleiterin Information und Kommunikation, Öffentlichkeitsarbeit
E-Mail: anja.hartmann@bsi.bund.de

Matthias Gärtner,

Pressesprecher
E-Mail: matthias.gaertner@bsi.bund.de

Meilensteine in der Geschichte des BSI

1990 wird das BSI-Errichtungsgesetz verabschiedet, in dem die Bedeutung der Informationstechnik hervorgehoben wird.

1991 Das Bundesamt für Sicherheit in der Informationstechnik nimmt am 1. Januar 1991 seine Arbeit auf. Gründungspräsident des BSI ist Dr. Otto Leiberich. Die Europäischen IT-Sicherheitskriterien (ITSEC) werden unter der Leitung des BSI entwickelt.

1992 Start des Zertifizierungs- und Akkreditierungsverfahrens gemäß ITSEC/ITSEM. Aufbau des IT-Grundschutzes. Das Schulungssystem für die Bundesverwaltung mit mehr als 1.000 Teilnehmern pro Jahr nimmt die Arbeit auf.

1993 Nach dem Ausscheiden von Dr. Otto Leiberich Ende 1992 wird Dr. Dirk Henze am 1.1.1993 zum neuen BSI-Präsidenten bestellt. Beginn der Mitarbeit an dem Common Criteria Zertifizierungsstandard.

1994 Beginn der Umsetzung einer breit angelegten Kryptoinnovationsstrategie im BSI, in deren Folge bis heute wesentliche kryptografische Systeme wie ElcroDat 6-2, Kryptosystem für den BOS-Digitalfunk, PLUTO Hochleistungskryptomodul, ElcroDat 4-2 Funksystem, SINA und zahlreiche Innovationen auf dem Gebiet der Public-Key-Kryptografie entstanden.

1996 Veröffentlichung der ersten Common Criteria (Version 1.0).

1998 Das neue Referat „Internetsicherheit“ trägt der wachsenden Bedeutung des World Wide Web Rechnung.

1999 Beim „Jahr 2000-Problem“ stellte das BSI umfangreiche Services und Informationen zur Verfügung, z.B. eine spezielle Bürgerbroschüre. Es erfolgt der Aufbau und die Unterstützung der Public-Key-Infrastruktur. Mit dem Start des Regierungsnetzes IVBB (Informationsverbund Berlin-Bonn) übernimmt das BSI die technische Koordination des Netzes.

2001 Bundesinnenminister Otto Schily setzt neue organisatorische, personelle und fachliche Rahmenbedingungen für die Weiterentwicklung des BSI zum zentralen IT-Sicherheitsdienstleister des Bundes in Kraft. Im Rahmen des Antiterrorpakets werden das Referat „IT-Penetrationszentrum“ und die Biometrie-Projektgruppe gegründet. Das Referat „Kritische Infrastrukturen“ startet umfangreiche Sektorenanalysen als Reaktion auf die Terroranschläge.

2002 Start der Bürger-CD, die mittlerweile zum Online-Portal ausgebaut und als CD über 1,6 Millionen Mal verteilt wurde.

2003 Nach dem Ausscheiden von Dr. Dirk Henze im November 2002 wird Dr. Udo Helmbrecht im März 2003 neuer Präsident des BSI.

2004 Das neue strategische Gesamtkonzept des BSI rückt durch den Einsatz moderner Steuerungsinstrumente die Bedürfnisse der Kunden stärker in den Mittelpunkt. Ein Veranstaltungshighlight 2004 ist der ICCC/ISSE-Kongress, den das BSI in Berlin ausrichtet.

2005 Die Bundesregierung stellt den Nationalen Plan zum Schutz der Informationsinfrastrukturen vor. Damit verbunden ist der Beginn des Ausbaus des BSI zu einer operativ tätigen Sicherheitsbehörde. Mit der Entwicklung eines Schutzprofils für die elektronische Gesundheitskarte leistet das BSI einen Beitrag zu einem der größten und innovativsten IT-Projekte weltweit.

B

BKA – Bundeskriminalamt

BMF – Bundesministerium der Finanzen

BMI – Bundesministerium des Innern

BMWA – Bundesministerium für Wirtschaft und Arbeit

BOS – Behörden und Organisationen mit Sicherheitsaufgaben

BWB – Bundesamt für Wehrtechnik und Beschaffung

C

CBAS – CERT-Bund Alarmierungssystem

CC – Common Criteria

CCRA – Internationales Abkommen zur Anerkennung von Zertifikaten *(Common Criteria Recognition Arrangement)*

CERT – Computer-Notfallteam *(Computer Emergency Response Team)*

COMSEC – NATO-Standard für Fernmeldesicherheit *(Communication Security)*

CS – Kommerzieller Dienst *(Commercial Service)*

CSCA – Landes-Zertifizierungsstelle *(Country Signing Certification Authority)*

D

DDoS-Angriffe – Verteilte Denial of Service(DoS)Angriffe *(Distributed Denial of Service)*

DEHSt – Deutsche Emissionshandelsstelle

DS-Zertifikat – Dokument, das die Erstellung von Signaturschlüsseln zulässt *(Document Signer-Signaturschlüssel-Zertifikat)*

DTD – Bestimmung der Struktur von Webseiten *(Document Type Definition)*

E

EAC – Protokoll zum erweiterten Zugriffschutz *(Extended Access Control)*

EADS – Europäische Luft- und Raumfahrtbehörde *(European Aeronautic Defence and Space Company)*

EEMA – European Electronic Messaging Association

EGVP – Elektronisches Gerichts- und Verwaltungspostfach

ElcroDat 6-2 – Kryptosystem für sichere Sprach-und Datenkommunikation über Euro-ISDN

eMRTD – Maschinenlesbares Reisedokument *(electronic Machine Readable Travel Document)*

EMVG – Gesetz über die Elektro-Magnetische Verträglichkeit

EMVP – Elektro-Magnetische Verträglichkeitsprüfung

ePass – Elektronischer Reisepass

ESA – Europäische Raumfahrtorganisation *(European Space Agency)*

ETSI – Europäisches Institut für Normen *(Institut Européen des Normes de Télécommunication)*

G

GNSS – Globales Satellitennavigationssystem *(Global Navigation Satellite System)*

GPRS – Allgemeiner paketorientierter Funkdienst *(General Packet Radio Service)*

GRT – Software zum Auslesen von elektronischen Dokumenten *(Golden Reader Tool)*

H

HTML – Internetsprache *(Hypertext Markup Language)*

I

ICAO – Internationale Luftfahrt-Organisation *(International Civil Aviation Organization)*

ICCC – Internationale Zertifizierungskonferenz *(International Common Criteria Conference)*

IEC – Internationale Kommission für Elektrotechnik *(International Electrotechnical Commission)*

IEEE – Institut für drahtlose Netzwerkkommunikation *(Institute of Electrical and Electronics Engineers)*

IP – Internet Protokoll

IPC – Inter Prozess Kommunikation

IRC – Internet Relay Chat Protokoll

ISDN – Internationaler Standard für ein digitales Telekommunikationsnetz *(Integrated Services Digital Network)*

ISO – International Organization for Standardization

ISO Guide 65 – Audit für Zertifizierungsorganisationen

ISSE – Information Security Solutions Europe

IT – Informationstechnik

iTAN – Indizierte Transaktionsnummer (TAN) beim Electronic Banking

IVBB – Informationsverbund Berlin-Bonn

K

KRITIS – Kritische Infrastrukturen

L

L4VM – Prototypische mikrokernbasierte Plattform

LAN – Local Area Network

M

MCert – MittelstandsCert (siehe CERT)

mTAN – Mobile TAN (per SMS)

N

NAGIOS – Network und Hagios (gr.: heilig) – Software, die es ermöglicht, komplexe IT-Strukturen abzubilden und zu überwachen

NETeam – Team nationaler Experten

NPSI – Nationaler Plan zum Schutz der Informationsinfrastrukturen

O

OS – Offener Dienst *(Open Service)*

OSCI – Online Service Computer Interface

OSS – Open-Source-Software

P

PIN – Persönliche Identifikationsnummer

PKI – Public Key Infrastruktur

PRS – Behördlicher Dienst *(Public Regulated Service)*

R

RFChip – Radiofrequency(RF)-Chip, Speichermedium für digitale Daten auf einem per Funk auslesbaren Chip

S

SAK – Signaturanwendungskomponenten

SAR-Lupe – Aufklärungssatellit, der mit Radar mit synthetischer Bündelbreite ausgestattet ist *(Synthetic Aperture Radar)*

SCIP – Sicheres Übertragungsverfahren *(Secure Communication Interoperability Protocol)*

SEK – Sondereinsatzkommando

SIM-Karte – Chipkarte für Mobiltelefone *(Subscriber Identity Module)*

SINA – Sichere Inter-Netzwerkarchitektur

SIRIOS – Vorfallsbearbeitungssystem für Computer-Notfallteams

SmartCard – Chipkarte mit integriertem Schaltkreis (Mikrochip)

SMTP – E-Mail-Übertragungsverfahren *(Simple Mail Transfer Protocol)*

SoL – Luftverkehrsdienst *(Safety-of-Life)*

SSEE – Schutzprofile für sichere Signaturerstellungseinheiten

T

TAN – Transaktionsnummer beim Electronic Banking

TCP/IP – Standard Protokoll-Stack für die Anbindung an das Internet *(Transmission Control Protocol / Internet Protocol)*

TETRA – Digitaler Bündelfunkstandard für Behörden- und Betriebsfunk *(Terrestrial Trunked Radio)*

TETRAPOL – Digitales Bündelfunksystem für die französische Police Nationale

TK – Telekommunikation

TR – Technische Richtlinie

TR S-WLAN – Technische Richtlinie Sicheres Wireless LAN

TSS – Technische Komponenten für Zeitstempeldienste *(Timestamping Server)*

U

UMTS – Mobilfunkstandard *(Universal Mobile Telecommunications System)*

URL – Einheitlicher Ortsangeber für Ressourcen im Internet *(Uniform Resource Locator)*

V

VMS – Virtual Machine Subsystem

VoIP – Voice over Internet Protokoll

VPN – Virtual Private Network

VPS – Virtuelle Poststelle

VS-NfD – Verschlusssache – Nur für den Dienstgebrauch

VW – Virtual Workstation

W

WDR – Westdeutscher Rundfunk

WID – Warn und Informationsdienst

WLAN – Drahtloses lokales Netzwerk *(Wireless Local Area Network)*

Z

z/OS – Name eines Betriebssystems für IBM-Großrechner

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
53175 Bonn

Bezugsstelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Referat 321 – Information und Kommunikation, Öffentlichkeitsarbeit
Godesberger Allee 185-189, 53175 Bonn
Telefon: 01888-95 82-0, E-Mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de

Texte und Redaktion
Felix Fortelka, BSI; Volker Thomas, Thomas Presse & PR

Layout & Gestaltung
Thomas Presse & PR, Berlin/Bonn
Grafik: Annette Conradt, Pierre Boom
Screen-Version: Ludwig Lang
Internet: www.thomas-ppr.de

Bildnachweis
1&1 Internet AG, Alcatel Deutschland, AOK-Bundesverband/Presseservice, AVM Computersysteme Vertriebs GmbH, Berliner Flughäfen/Pressestelle, Berlin Partner/FTB-Werbefotografie, Bildstelle im Bundesministerium der Verteidigung (BMVg), Pierre Boom, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundesanstalt Technisches Hilfswerk (THW), Bundesbildstelle, Bundesdruckerei, Bundesministerium des Innern (BMI), Deutsche Postbank, Deutsche Telekom, Deutsches Zentrum für Luft- und Raumfahrt (DLR), Dresdner Bank/Presse-Center, Andreas Ernst, Fraunhofer-Gesellschaft/Volker Steger, Intel Pressroom, OHB-System, Rohde & Schwarz, Siemens, Volker Thomas, Vattenfall Europe, virtUOS/Universität Osnabrück
Fotocomposings: r.e.m./Hans-Georg Gaul

Stand
August 2006