Bundesamt
für Sicherheit in der
Informationstechnik

Jahresbericht 2004

Bundesamt für die Sicherheit in der Informationstechnik

www.bsi.bund.de

Sichere Informationstechnik für unsere Gesellschaft

Unser Leitbild

2004 wurde ein Leitbild für das BSI entwickelt. Alle Mitarbeiterinnen und Mitarbeiter des Amtes waren dazu aufgerufen, sich an der Gestaltung und Ausarbeitung des Leitbildes aktiv zu beteiligen. Durch das rege Engagement wurde ein Leitbild erstellt, in dem sich alle Beschäftigten des Amtes wiederfinden.

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.

Information
Aufklärung und Sensibilisierung von Bürgern
Zukunfts- und Trendanalysen

Beratung und Unterstützung
IT-Grundschutz, IT-Sicherheitsberatung für Behörden
E-Government und Initiative BundOnline 2005
Lauschabwehr und Abstrahlsicherheit, Penetrationstests
Unterstützung der Datenschutzbeauftragten
Unterstützung der Strafverfolgungsbehörden

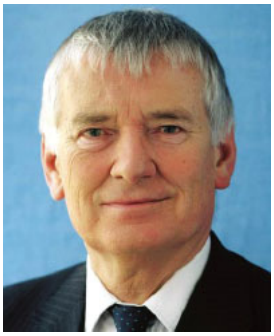
Risikountersuchung, Prüfung und Bewertung
Schadprogramme, Internetsicherheitsanalysen
IT-Plattformen, Kritische Infrastrukturen
Biometrische Verfahren, Mobile Anwendungen
Zertifizierung von IT-Produkten und -Systemen
Zulassung von Produkten für den
staatlichen Geheimschutz

Entwicklung
Evaluierung und Entwicklung von Kryptogeräten
Sicherheitstools, Formale Sicherheitsmodelle

Betrieb
CERT-Bund (Computer Emergency Response Team)
Technische Koordination des IVBB
(Informationsverbund Berlin-Bonn)
Verwaltungs-PKI
Schlüsselmittelherstellung für Kryptogeräte

Gremien
Mitarbeit in nationalen und internationalen Gremien
und Standardisierungsorganen für Deutschland

IT-Sicherheit – fester Bestand der Inneren Sicherheit



Liebe Leserinnen und Leser,

Sicherheit ist ein Garant für die gesellschaftliche und wirtschaftliche Entfaltung, für die persönliche Freiheit. Überall dort, wo Leib und Leben direkt in Gefahr sind, wird uns dies unmittelbar bewusst. Je mehr sich eine Gesellschaft aber entwickelt, desto weiter muss das klassische Sicherheitsverständnis erweitert übertragen werden.

Um den erarbeiteten Wohlstand erhalten und ausbauen zu können, braucht ein moderner Wirtschaftsstandort gesicherte Infrastrukturen. Von besonderer Bedeutung sind z.B. Energieversorgung, Verwaltung, Finanzen, Verkehr, Polizei und Rettungswesen. Sie müssen zuverlässig funktionieren und ständig verfügbar sein, wobei hier die Informations- und Kommunikationstechnik eine Schlüsselrolle einnimmt. Microcontroller finden sich in PCs und Handys, sie ermöglichen die maschinelle Erkennung von Menschen an Grenzkontrollen, speichern Geld in Chipkarten oder steuern ganze Produktionsprozesse. Über die weltweite Vernetzung ist ein immer schnellerer Informationsaustausch selbst über mobile Geräte längst selbstverständlich geworden. IT-Sicherheit ist daher fester Bestandteil der Inneren Sicherheit Deutschlands.

Wo die kritischen Punkte in der Informationstechnik liegen, untersucht das BSI: Dabei analysiert und bewertet das BSI IT-Systeme hinsichtlich ihrer Sicherheitseigenschaften und stellt Zertifikate nach internationalen Kriterien aus. Außerdem entwickelt das BSI eigene Schutzvorkehrungen. Durch die ausgewiesene Fachkompetenz haben die Aussagen des BSI zu aktuellen Fragestellungen der Informationsgesellschaft ein großes Gewicht.

Berlin, im Juli 2005

Otto Schily
Bundesminister des Innern

Ein moderner Wirtschaftsstandort braucht gesicherte Infrastrukturen

Liebe Leserinnen und Leser,

die Schlagworte Viren, Würmer oder SPAM standen auch 2004 im Fokus der Öffentlichkeit. Dabei gerät schnell in Vergessenheit, wie weit das Spektrum der IT-Sicherheitsfragen reicht. Beispielsweise bei RFID-Chips, der Biometrie oder beim Betrug über Phishing. IT-Sicherheit spielt überall dort eine Rolle, wo IT eingesetzt wird. Betroffen ist jeder.

Aus diesem Grund ist es wichtig, dass nicht nur wenige Spezialisten über dieses Thema aufgeklärt werden, sondern alle Bürger verantwortungsvoll mit der schnelllebigen, technischen Vielfalt umgehen können. Es drohen hohe Schäden durch Ausfall oder erfolgreiche Angriffe. Richtige Vorsorge setzt aber das entsprechende Wissen voraus. Risiken und Schutzmaßnahmen müssen daher so bekannt sein wie die Anschnallpflicht im Auto.

Dazu sind zuverlässige, aktuelle Informationen notwendig. Aufklärung und Sensibilisierung über IT-Sicherheit sind Aufgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI). Es wendet sich mit seinen Produkten und Informationsangeboten sowohl an IT-Experten als auch an breite Bevölkerungskreise.

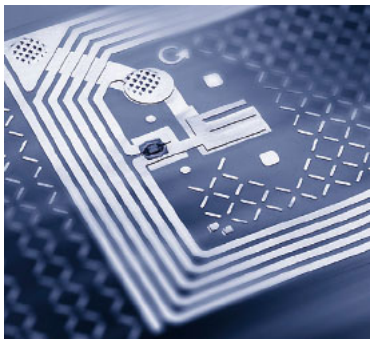
Dabei ist die Bandbreite der aufkommenden IT-Sicherheitsfragen weit gespannt. Nicht nur technische Probleme sind zu klären, sondern auch juristische, wirtschaftliche und gesellschaftliche Antworten zu finden. Ausgangspunkt ist die verfügbare Technik: Sie gibt den Rahmen vor, in dem wir Potenziale erschließen können oder Grenzen setzen müssen.

Technische Fragen stehen für das BSI im Zentrum seiner Aktivitäten – national wie international. Um hier erfolgreich zu agieren, braucht es langjährige Erfahrung und umfassendes Fachwissen. Nur so lassen sich Trends früh erkennen, Chancen und Risiken richtig bewerten und entsprechende IT-Sicherheitsstrategien durchsetzen.

Im Rückblick reiht sich das Jahr 2004 mit seinen Erfolgen in die erfreuliche Historie des Amtes ein. Ohne die Einsatzbereitschaft und das Expertenwissen der Mitarbeiterinnen und Mitarbeiter des BSI wäre das nicht zu leisten gewesen. Dafür möchte ich ihnen meinen herzlichen Dank aussprechen.

Bonn, im Juli 2005

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



SEIT DER GRÜNDUNG HAT SICH DAS BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK EINE HERVORRAGENDE REPUTATION ERARBEITET. DAS HABEN IT-SICHERHEITSEXPERTEN IN UMFRAGEN EINDRUCKSVOLL BESTÄTIGT.

1 Die Basis des Erfolgs: Vertrauen

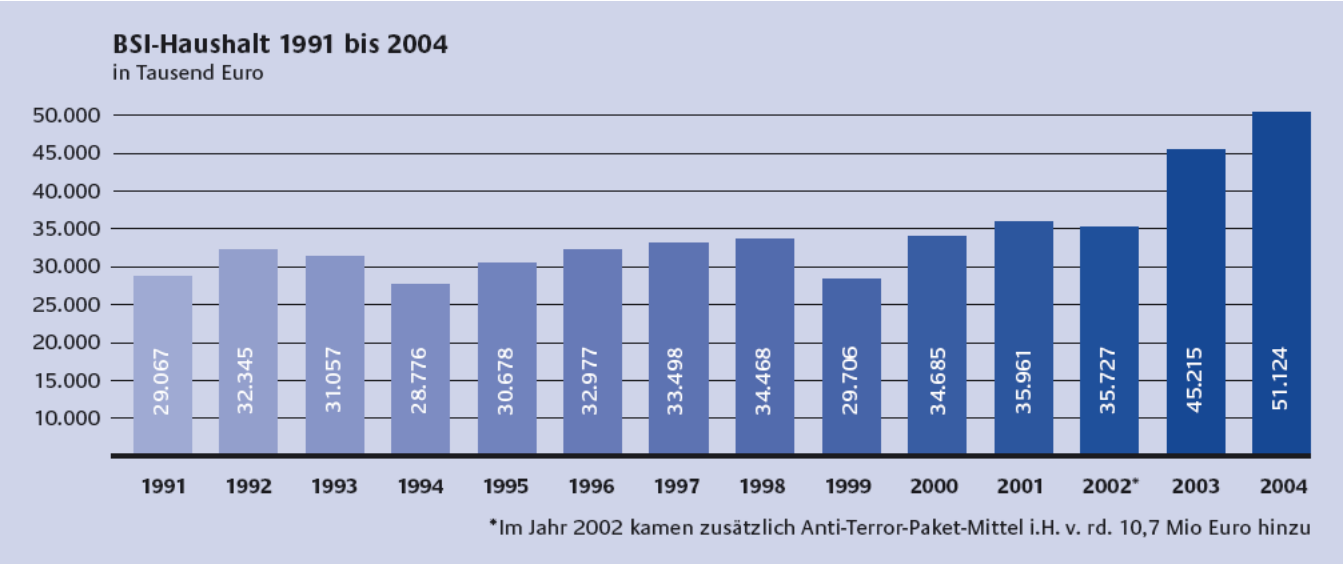
Die Informationstechnik ist allgegenwärtig. Es gibt heute fast keinen Lebensbereich, der nicht von ihr durchdrungen wäre. Dabei führt diese Technik ihren Siegeszug häufig unbemerkt fort, etwa in Form von winzigen Funketiketten, die an Joghurtbechern, Jacketts oder CDs angebracht werden, den RFID-Chips (Radio Frequency Identification Chips).

Handys, PCs oder Chipkarten sind kaum noch weg zu denken. Die moderne Fahrzeugtechnik kommt ohne Informationstechnik (IT) nicht aus. Effiziente Produktionsprozesse und Verwaltungsabläufe setzen eine reibungslos funktionierende Informationstechnik voraus. Wirtschaftlicher Erfolg, individuelle Freiheit und Innere Sicherheit sind längst untrennbar mit einer zuverlässigen IT verknüpft.

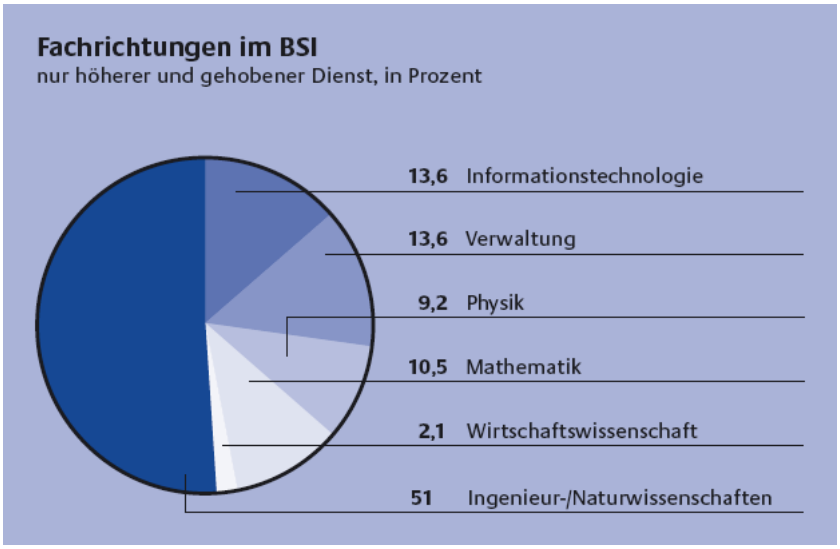
IT-Sicherheit geht jeden an. Die Ansprüche an Vertraulichkeit, Verfügbarkeit und Integrität der IT-Anwendungen steigen mit ihrer Verbreitung unaufhörlich weiter. Ohne sichere Informationstechnik ist die Zukunft für einen modernen Wirtschaftsstandort wie Deutschland undenkbar.

Für IT-Sicherheit zu sorgen ist anspruchsvoll. In Deutschland nimmt diese Aufgabe das Bundesamt für Sicherheit in der Informationstechnik (BSI) wahr. Für dieses Ziel hat das BSI nicht nur das enorme Entwicklungstempo zu meistern, sondern muss sich auch in die ungeheure Komplexität der Einzelthemen einarbeiten. Nur so kann das Bundesamt die Innovationen, die sich in rascher Folge verbreiten, richtig einschätzen und ihre sicherheitsrelevanten Eigenschaften bewerten.

Kompetentes Handeln im hochtechnisierten Umfeld setzt erstklassiges Expertenwissen voraus. Sorgfältige Facharbeit ist Ausgangspunkt und Kern aller Aktivitäten des BSI. So werden Grundlagen erarbeitet, die für Produktentwicklung und Beratung unerlässlich sind. Neben den rein technischen Fragestellungen müssen aber auch wirtschaftliche, gesellschaftliche und rechtliche Hintergründe einbezogen werden, wenn das BSI dem Bedarf seiner Kunden gerecht werden will.



Die stetig wachsende Bedeutung des BSI spiegelt sich auch in den Haushaltszahlen. Der Etat weist 2004 einen Zuwachs von elf Prozent auf.



Im höheren und gehobenen Dienst liegt das Durchschnittsalter der Mitarbeiterinnen und Mitarbeiter bei 44,3 beziehungsweise. bei 42,1 Jahren. Von den 407 Mitarbeiterinnen und Mitarbeitern des BSI sind die meisten Naturwissenschaftler, zum Beispiel Elektro- oder Nachrichtentechniker.

So vielfältig die Faktoren im IT-Sicherheitsbereich sind, so komplex ist das Aufgabenspektrum des BSI:

Prüfung und Bewertung der Sicherheit von IT-Systemen

Evaluierung und Zertifizierung nach internationalen Kriterien macht die Sicherheitseigenschaften von Produkten transparent. Dies ist für ihre Konkurrenzfähigkeit im hart umkämpften Markt ein bedeutender Mehrwert, für ihre Zulassung in Sicherheitsbereichen von Staat und Industrie ist es schlicht Voraussetzung.

Entwicklung von IT-Schutzvorkehrungen

Das BSI entwickelt und vertreibt – teilweise in enger Kooperation mit Partnern aus der Industrie – Sicherheitssysteme, angefangen von Produkten für den Umgang mit klassifizierten Informationen bis hin zu Tools für die Umsetzung des IT-Grundschutzes.

Beratung von Herstellern, Vertreibern und Anwendern von IT-Systemen

Aufklärung und Beratung stehen für IT-Verantwortliche in Behörden und Unternehmen, für private Anwender sowie für Hersteller von IT-Produkten zur Verfügung. Mit diesem breiten Spektrum wird sichergestellt, dass alle Beteiligten von Anfang an IT-Sicherheitsaspekte bei Entwicklung, Einkauf und Einsatz der Systeme beachten können.

Mitarbeit in internationalen Gremien

Das BSI vertritt und unterstützt durch seine Arbeit in internationalen Gremien, zum Beispiel der Nato und der EU, die Interessen Deutschlands im Hinblick auf IT-Sicherheitsaspekte. Dadurch sollen Fehlentwicklungen verhindert, der Informationsaustausch gefördert und internationale Kontakte gepflegt werden.

Marktbeobachtung und Trendforschung

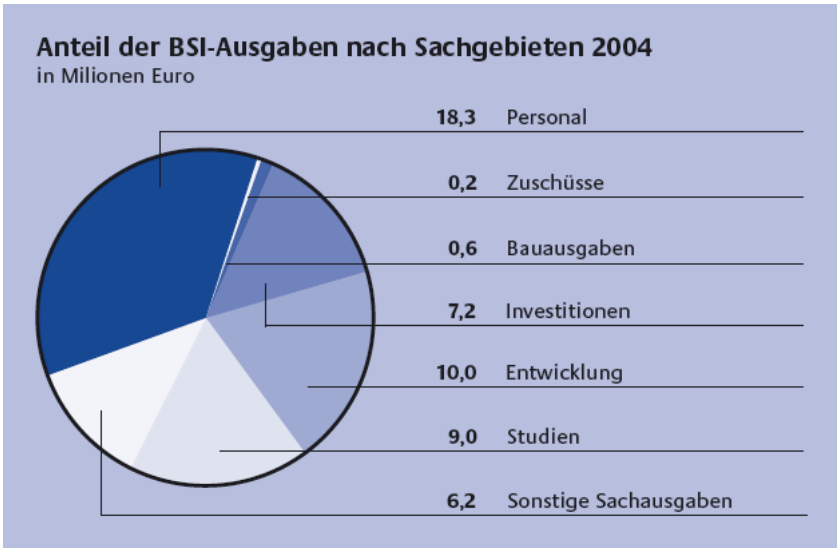
Die frühzeitige und möglichst präzise Erfassung von aktuellen und sich abzeichnenden Entwicklungen erlaubt rechtzeitiges, umsichtiges und bedarfsgerechtes Handeln. Aus diesem Grund beschäftigt sich das BSI in Arbeitsgruppen und Projekten mit allen wichtigen Themen mit Bezug auf IT-Sicherheit. Die laufende Marktbeobachtung spielt hier eine wichtige Rolle: Die Angebote des BSI müssen kundengerecht und aktuell sein, um erfolgreich IT-Sicherheit zu fördern.

Unterstützung von Strafverfolgungsbehörden und Geheimschutzberatung

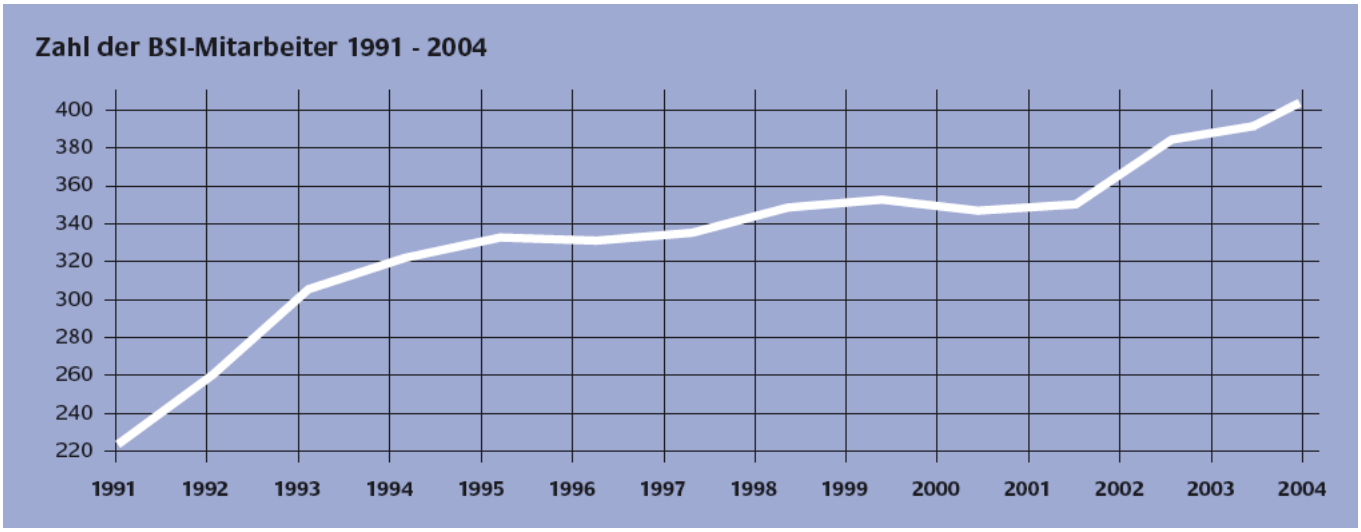
Als IT-Sicherheitsbehörde unterstützt das BSI die Strafverfolgungsbehörden bei ihren Ermittlungen und bietet Geheimschutzberatung für Behörden sowie für einzelne Kunden aus der Industrie. Lauschabwehr- und Abstrahlprüfungen sind weitere Aufgaben des Amtes.

Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), bei seiner Abschlussrede auf dem ICCC/ISSE-Kongress vom 28. bis 30. September 2004 in Berlin.

Girls' Day im BSI: Dr. Hans-Josef Ganser zeigt am Innenleben eines Computers interessierten jungen Frauen, wie eine Festplatte Informationen speichert und sicher verarbeitet.



Investitionen in die Köpfe: Mit 19 Millionen Euro lagen die Ausgaben für Entwicklungen und externe Studien bei 38 Prozent des Gesamtetats.



Auf 407 stieg die Zahl der Mitarbeiter im BSI im Jahre 2004. Sie haben größtenteils ein abgeschlossenes Hoch- beziehungsweise Fachhochschulstudium der Ingenieurwissenschaften, Mathematik, Informatik sowie Physik. Team- und Projektarbeit werden besonders gefördert.

Das BSI ist in erster Linie der IT-Sicherheitsdienstleister des Bundes. Als Behörde aus dem Geschäftsbereich des Bundesministeriums des Innern (BMI) bietet es Bundes-, aber auch Landes- und Kommunalbehörden umfangreichen Service an. Zu den Zielgruppen des BSI gehören aber auch Organisationen aus dem Privatbereich. Gerade kleine und mittelgroße Unternehmen können von Produkten, die auf ihre Bedürfnisse zugeschnitten sind, profitieren. Denn hier ist der Nachholbedarf an informationstechnischer Risikovorsorge besonders groß. Wirtschaftliche Aspekte der IT-Sicherheit spielen dabei eine besonders große Rolle. Nur wer die Anforderungen der Kunden versteht, kann bedarfsgerecht anbieten und wirkungsvolle Strategien zur Steigerung der IT-Sicherheit entwickeln. Für das BSI ist es daher wichtig, die Rahmenbedingungen in den einzelnen Marktsegmenten genau zu verstehen und kommende Trends frühzeitig zu erkennen.

Im Jahre 2004 hat das BSI ein neues strategisches Gesamtkonzept verabschiedet, um für die Herausforderungen der Zukunft gerüstet zu sein. Es verbindet die Vision der kommenden IT-Entwicklung mit dem Selbstverständnis des BSI und seinen Kernaufgaben. Moderne Controllingwerkzeuge wie die 2004 eingeführte Balanced Scorecard unterstützen neben der hergebrachten Kosten- und Leistungsrechnung die Steuerung.

Die wichtigste Neuerung ist die Verlagerung des Schwerpunkts von einer primär inputbezogenen zu einer output- beziehungsweise ergebnisorientierten Führung des Amtes. Dadurch rücken die Bedürfnisse der Kunden in den Mittelpunkt. Die neu eingerichteten Key-Account Manager haben dabei eine wichtige Funktion: Sie sind das zentrale Bindeglied zwischen dem BSI und den jeweiligen Ansprechpartnern und erfassen Einflussfaktoren aus Markt, Technik und operativer Arbeit. Wünsche, Anregungen oder Kritik der Kunden können sie schnell berücksichtigen und umgehend reagieren. Der ständige Kontakt ermöglicht die passgenaue Auswahl und Weiterentwicklung von Projekten, Produkten und Grundlagenforschungen.

Ob sich nun die Arbeit des Amtes an einzelne Behörden und Unternehmen richtet oder an die breite Bevölkerung adressiert ist: Ein kritischer Aspekt ist häufig das nicht ausreichend vorhandene Risikobewusstsein. IT-Gefahren und die richtige Vorsorge müssten jedem Nutzer bekannt sein. Und das heißt jedem Anwender, nicht nur den IT-Experten. Erstes Ziel muss es sein, direkte Schäden durch Schutzmaßnahmen und umsichtiges Verhalten zu verhindern. Zweitens geht es aber auch darum, das Vertrauen in die Informationstechnik insgesamt zu stärken. Nur so lassen sich ihre Potenziale wirklich ausschöpfen.

Das BSI kann beide Ziele nur dann erreichen, wenn auch Vertrauen in das Bundesamt selbst vorhanden ist. Alle Aktivitäten, Produkte und Informationen, die vom BSI ausgehen, müssen deswegen höchsten Ansprüchen gerecht werden. Sonst bleiben Empfehlungen wirkungslos, Maßnahmen werden nicht um- und Produkte nicht eingesetzt.

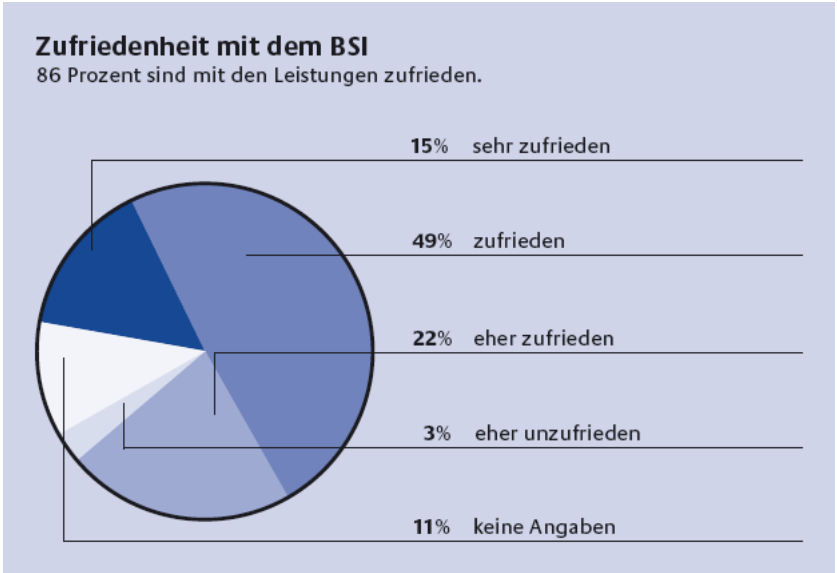
Die wichtigste Basis für den Erfolg ist geschaffen: Dem BSI wird großes Vertrauen entgegengebracht. Seit seiner Gründung 1991 hat es sich eine hervorragende Reputation erarbeitet. Die im Auftrag des BSI von TNS-Emnid durchgeführte Erhebung unter 500 IT-Sicherheitsexperten bestätigt dies für 2004 eindrucksvoll: Danach halten 93 Prozent der Befragten das BSI für kompetent, 91 Prozent für neutral und 95 Prozent für glaubwürdig. Diese Spitzenwerte sind eine klare Bestätigung für die geleistete Arbeit. Allerdings gibt es noch viel zu tun. Insgesamt zeigt sich bei der IT-Sicherheitslage ein besorgniserregender Trend. Eine IT-Sicherheitsstudie, die in Zusammenarbeit mit der Zeitschrift <kes>, dem BSI und Microsoft durchgeführt wurde, kam zu dem Ergebnis, dass der Stellenwert der IT-Sicherheit im Top-Management zwar gewachsen ist, aber die Verantwortlichen klagen zunehmend über mangelnde Gelder. 40 Prozent haben nicht einmal eine schriftlich fixierte IT-Sicherheitsstrategie, nur 58 Prozent verfügen über einen zentralen IT-Sicherheitsbeauftragten.

Virenscanner und Firewalls als technische Schutzmaßnahmen werden auch zukünftig eine wachsende Rolle spielen. Technische Mängel verursachten bei Software (43 Prozent) und Hardware (38 Prozent) im vergangenen Jahr wiederum häufiger Schäden als unbeabsichtigte Beeinträchtigungen durch Externe (15 Prozent) oder gezielte Angriffe (neun Prozent).

Sicherheitskonzepte werden laut der Studie nur lückenhaft umgesetzt. Die Gefährdungslage bei Notebooks, PDAs, Heim- und Telearbeitsplätzen sowie WLAN ist besorgniserregend. Fast die Hälfte der Befragten halten auf diesem Gebiet die Sicherheit für „gerade noch ausreichend“ oder sogar „nicht ausreichend“. Auch hier können technische Einzelmaßnahmen nicht ein systematisches Sicherheitskonzept ersetzen, das bei Administrationsrechten beginnt und bei Zutrittskontrollen endet. Das BSI bietet hierzu mit dem IT-Grundschutzhandbuch das passende Angebot. Es wird erfreulicherweise bereits von 45 Prozent der Befragten genutzt. Weitere 31 Prozent planen den Einsatz des Handbuchs.

Auch andere Zahlen sprechen für den Erfolg der BSI-Produkte: Bei der Zertifizierung von Produkten nach den internationalen Common Criteria hat das BSI große Erfolge zu verzeichnen. Kontinuierlich steigt die Zahl der vom BSI jährlich erteilten Zertifikate, auf 38 alleine in 2004. Zu den namhaften Kunden gehören mittlerweile Weltunternehmen wie IBM Corporation, Siemens AG, Renesas Technology Corporation, Philips Semiconductors GmbH, SuSE Linux AG, Infineon Technologies AG, Giesecke & Devrient GmbH, Red Hat Inc., SAP AG, Microsoft Corporation, T-Systems. Erstmals konnte das BSI auch für Deutschland die Internationale Common Criteria Conference (ICCC) in Berlin als Gastgeber ausrichten. Nicht zuletzt deshalb kann das BSI auf ein sehr erfolgreiches Jahr zurückblicken.

Das BSI bildet junge Leute in den Berufen „IT-Systemelektroniker/in“ und „Verwaltungsfachangestellte/r“ aus. Diese sechs Auszubildenden sind seit September 2004 neu an Bord.



Themen zur IT-Sicherheit standen im Mittelpunkt einer repräsentativen Umfrage von TNS-Emnid unter 500 IT-Experten. Unter anderem ergab die Umfrage: Der Bekanntheitsgrad des BSI ist hoch, die meisten Befragten sind mit seinen Leistungen zufrieden. Bei der IT-Sicherheit herrschen jedoch Mängel: Jeder fünfte deutsche IT-Experte hält die eigene Organisation und sogar 89 Prozent der Befragten die Wirtschaft in Deutschland durch unzureichende IT-Sicherheit für gefährdet.

Bedeutung der verschiedenen Gefahrenbereiche

Gefahrenbereich	Rang	Prognose: Risiko ...
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	... nimmt zu.
Malware (Viren, Würmer, Trojanische Pferde, u.ä.)	2	... nimmt stark zu.
Unbefugte Kenntnisnahme, Informationsdiebstahl	3	... nimmt gering zu.
Software-Mängel/-Defekte	4	... bleibt gleich.
Hacking (Vandalismus, Probing, Missbrauch, u.ä.)	5	... nimmt gering zu.
Hardware-Mängel/-Defekte	6	... bleibt gleich.
Unbeabsichtigte Fehler von Externen	7	... bleibt gleich.
Höhere Gewalt	8	... bleibt gleich.
Manipulation zum Zweck der Bereicherung	9	... bleibt gleich.
Mängel der Dokumentation	10	... bleibt gleich.
Sabotage (inkl. DoS)	11	... bleibt gleich.
Sonstiges	12	... bleibt gleich.

Quelle: <kes>-Sicherheitsstudie 2004, in Zusammenarbeit mit BSI und Microsoft

Nach wie vor schätzen die befragten Manager die eigenen Mitarbeiter als den größten Risikofaktor ein, dicht gefolgt von Schadprogrammen. Von ihnen – so ihre Prognose – werden in den nächsten Jahren die größten Risiken ausgehen. Bereits jetzt war „Malware“ für eine mittlere Ausfallzeit von über 54 Stunden und durchschnittliche Kosten von 25.954 Euro pro Jahr verantwortlich.

Die 2004 neu herausgegebene Mitarbeiterzeitschrift „@BSI“ ist ein Medium von und für Mitarbeiterinnen und Mitarbeiter des Amtes. „@BSI“ fördert den Erfahrungsaustausch und die interne Kommunikation durch die Diskussion aktueller BSI-Themen, Vorstellung von Mitarbeitern, Projekten oder auch Beiträgen abseits des Dienstgeschäfts. Die Hauszeitung erscheint viermal im Jahr und wird durch ein Redaktionsteam erstellt, das quer durch die Hierarchie- und Organisationseinheiten aufgebaut ist. Die interne Kommunikation wird neben „@BSI“ vor allem durch das Intranet und die interne Veranstaltungsreihe „BSI-Forum“ getragen.

Zielgruppengenaue Angebote – IT-Sicherheit geht alle an

Informationstechnik nutzt nahezu jeder in Deutschland. Alle profitieren von den enormen Möglichkeiten, die uns das Informationszeitalter bietet. Tagtäglich greifen wir zum Handy, surfen im Internet, zücken Geld- oder Kreditkarten.

Doch über die Gefahren, die dabei lauern, machen sich viele erst Gedanken, wenn es zu spät und der Schaden bereits eingetreten ist. Und das ist leider nicht nur bei privaten Anwendern zu beobachten, sondern auch in großen Unternehmen. Deshalb klärt das BSI über Risiken und Schutzmaßnahmen in der IT umfassend bei allen Zielgruppen auf: Verwaltung, Wirtschaft und Bürger.

Jede Zielgruppe hat ihre eigenen Risiken, der Stand des Fachwissens ist sehr heterogen und die spezifischen Bedrohungen werden völlig unterschiedlich wahrgenommen. Deswegen setzt das BSI auf bedarfsspezifisch zugeschnittene Informationsangebote.

- Für das Management in Unternehmen und Behörden müssen die Angebote schnell erfassbar, verlässlich und auf das Wesentliche konzentriert sein. So unterstützt zum Beispiel der „Leitfaden IT-Sicherheit“, bereits in zweiter Auflage erschienen, Entscheider dabei, sich zügig einen fundierten Überblick zum Thema IT-Sicherheit zu verschaffen. Daran anknüpfende Produkte zum Beispiel zum IT-Grundschutz stellen die notwendigen Werkzeuge bereit, um das passende IT-Sicherheitskonzept zu realisieren.

- IT-Experten, Wissenschaftler und das versierte Fachpublikum finden beim BSI umfassende und unabhängige Informationen. Zahlreiche Publikationen zu Themen wie drahtlose Kommunikation, Biometrie, Zertifizierung, Schadprogramme, Chipkartentechnik, E-Government und vieles mehr stehen auf der Webseite www.bsi.bund.de oder in gedruckten Publikationen zur Verfügung. Alle Veröffentlichungen befinden sich auch auf einer CD, die gegen einen frankierten Rückumschlag kostenlos beim BSI erhältlich ist. Zum Online-Service gehören regelmäßige Newsletter, die auf Wunsch für jeden zu beziehen sind.

„Argus“ heißt die offizielle Sicherheitsspürnase auf der BSI-Seite für Bürger (links). Die Startseite (rechts) www.bsi.bund.de öffnet den Weg zu vielen aktuellen Informationen, von A wie Ausschreibungen bis V wie Virenwarnung.

- Seitdem das Internet immer stärker in den eigenen vier Wänden Einzug gehalten hat, stehen die privaten Anwender von Informationstechnik zunehmend im Mittelpunkt des BSI, wenn es um IT-Sicherheit geht. Denn jeder verantwortet im Kleinen den Schutz des Internets im Ganzen. Sicherheitslücken lassen sich von Angreifern um so wirkungsvoller ausnutzen, je häufiger sie vorkommen. Speziell an die privaten IT-Nutzer gerichtet ist deshalb das Internetangebot www.bsi-fuer-buerger.de. Dort finden sich seit Anfang 2003 leicht verständliche Informationen rund um das Thema IT-Sicherheit. Das Angebot umfasst zudem die Möglichkeit, einen 14tägig erscheinenden Newsletter mit den wichtigsten Sicherheitsnachrichten zu beziehen und verschiedene Sicherheitsprogramme kostenlos herunterzuladen.

- Über Partnerschaften mit Wirtschaft, Verwaltung, Medien und Wissenschaft spricht das BSI unterschiedliche Personenkreise an. Fachlich begleitet das Bundesamt seit 2004 die Kampagne „Mittelstand-sicher-im-Internet“, die vom Bundesministerium für Wirtschaft und Arbeit (BMWA) sowie dem Bundesministerium des Innern (BMI) initiiert wurde.
Die erfolgreiche Zusammenarbeit mit Fujitsu Siemens Computers (auf den Scaleo-Rechnern sind die Informationen des Bürgerportals vorinstalliert) und mit dem Heise Verlag (www.heisec.de) setzt sich bereits im zweiten Jahr fort. 2004 neu hinzugekommen ist die Kooperation mit Freenet (www.freenet.de), auf deren Portalseite unter „Viren und Sicherheit“ aktuelle Informationen des BSI bereitgestellt werden. Ebenfalls 2004 gestartet ist die Sicherheitskooperation mit der Bull GmbH, die ihrer Serverfamilie jetzt standardmäßig ein BSI-Sicherheitspaket beilegt.

Die Liste der Kooperationspartner des BSI hat sich 2004 stetig erweitert. Bei www.freenet.de ist das BSI in der Rubrik „Viren und Sicherheit“ vertreten.

Bewährt: Schirmherrschaften des BSI

Besondere Bedeutung hat die Zusammenarbeit mit der SecuMedia Verlags-GmbH. Im BSI-Forum der Fachzeitschrift „<kes> – Die Zeitschrift für Informations-Sicherheit“ informiert das BSI regelmäßig über aktuelle Themen der IT-Sicherheit. Auch bei Messen kooperiert das BSI eng mit dem SecuMedia-Verlag. Die IT-Security Area auf der Münchner „Systems“ wird von SecuMedia organisiert und steht unter der Schirmherrschaft des Bundesamtes. Das BSI ist aber nicht nur Aussteller, sondern wirkt durch zahlreiche Vorträge in technischen und managementorientierten Foren mit.

Neben der „Systems“ ist das BSI auf allen wichtigen Messen mit Bezug zu IT-Sicherheitsthemen vertreten, sei es auf der CeBIT in Hannover oder bei der „Security“ in Essen. Bei der Fachmesse „Moderner Staat“ in Berlin ist das BSI Partner für den Bereich der IT-Sicherheit. Neben persönlichen Gesprächen steht bei diesen Treffen die Präsentation wichtiger IT-Sicherheitsthemen und aktueller Arbeitsschwerpunkte im Vordergrund.

Neue Reihe: Das BSI im Gespräch

Eine neue Veranstaltungsreihe „Das BSI im Gespräch“ hatte mit der Vorstellung der RFID-Studie „Risiken und Chancen des Einsatzes von RFID-Systemen (RIKCHA)“ im Berliner Museum für Kommunikation ihre gelungene Premiere. Zahlreiche Gäste, darunter Leiter aus Behörden und Unternehmen, informierten sich hier und diskutierten mit den Experten des BSI. Daneben organisierte das BSI 2004 eine Reihe von weiteren Veranstaltungen, wie etwa in Boppard am Rhein den 11. Diskurs zum Thema „Das Urheberrecht von Morgen – ist eine sichere DRM-freie Medienzukunft möglich?“

Die Aktivitäten im Bereich Open Source Software, wie zum Beispiel den Behördendesktop „ERPOSS“, stellte das BSI auf dem Linux-Tag in Karlsruhe vor. Die SAFECOMP 2004 in Potsdam hat das BSI in Zusammenarbeit mit der Universität Münster und dem Potsdamer Hasso-Plattner-Institut für Softwaresystemtechnik ausgerichtet.

Alle zwei Jahre veranstaltet das BSI zudem den Deutschen IT-Sicherheitskongress. Er hat sich in den vergangenen Jahren zu dem zentralen Treffen der IT-Experten entwickelt. Unter dem Motto „IT-Sicherheit geht alle an!“ findet der 9. Deutsche IT-Sicherheitskongress vom 10. bis 12. Mai 2005 in der Stadthalle Bonn-Bad Godesberg statt.

2 Kontrolle ist besser – Basis für IT-Sicherheit

Das Internet bietet fantastische Kommunikationsmöglichkeiten: E-Mails, Fotos, Videos schießen in Sekundenschnelle um den ganzen Erdball. Die Freiheiten, welche die moderne Kommunikationstechnik bietet, haben allerdings ihren Preis: Sie können missbraucht werden.

Viren, trojanische Pferde, verseuchte Programme sind in der Lage, in Sekundenbruchteilen riesige Schäden zu verursachen. Private Anwender sind dabei genauso betroffen wie Wirtschaftsunternehmen und Behörden. Der Unterschied besteht allerdings darin, dass von einem Virus in einem Privathaushalt vielleicht nur ein PC betroffen ist. In einer Behörde oder in einer Firma aber kann ein ganzes Kommunikationsnetz mit möglicherweise Hunderten oder Tausenden von Nutzern ausfallen.

Wer sich schützen will, muss sicher sein können, dass die verwendeten IT-Produkte auf Herz und Nieren geprüft sind, und hat immer wieder neu dafür zu sorgen, dass sein gesamtes System sicher angelegt ist. IT-Grundschutz und Zertifizierungen durch das BSI sind dafür eine gute Basis. Beispielsweise zeigen Zertifikate, welches Sicherheitsniveau nationale und internationale Produkte erreicht haben.

Das IT-Grundschutzhandbuch hat sich mit seinen verschiedenen Ergänzungslieferungen in den Händen von IT-Verantwortlichen mittlerweile als Klassiker erwiesen. Heute bietet das BSI für unterschiedliche Organisationen zugeschnittene Grundschutzprofile an. Vom BSI geprüfte Sicherheitsexperten, die Auditoren, unterstützen Anwender bei der Umsetzung.

2.1 Tägliche Herausforderung: Viren, Schadprogramme, Dialer

Nicht nur Industrie und Behörden verlassen sich zunehmend auf IT-Systeme, auch aus Privathaushalten sind sie nicht mehr wegzudenken.

Immer mehr Dienste, für die eine Vielzahl von unterschiedlichen IT-Systemen eingesetzt werden, sollen künftig automatisiert werden. Eine große Zahl von E-Commerce- und E-Government-Anwendungen laufen nur über Rechner: Einige Städte haben zum Beispiel Online-Tickets für den öffentlichen Nahverkehr eingeführt, die während der Fahrt per Handy bestellt und bezahlt werden können.

Das BSI gibt auf seinen Internetseiten www.bsi-fuer-buerger.de Hinweise, wie man sich vor Viren, Dialern und Schadprogrammen schützen kann. Aber wenn der Totenkopf auf dem Bildschirm erscheint, ist es meistens schon zu spät: Der Virus ist im System.

TCG – Sichere Kommunikationsplattformen

Mit der Verbreitung von IT-Systemen vervielfältigen sich deren Sicherheitsprobleme. Viren und andere Schadprogramme pflanzen sich über das Internet weltweit und rasend schnell fort. Spionageprogramme gelangen an sensible Daten auch von Privatleuten. Dem Informationsangebot von Firmen werden über DoS-Angriffe hohe Schäden zugefügt. Statt die Kommunikation zu erleichtern, wird das E-Mail-Netz mit der immensen Zunahme der Spam-Mails zu einer Belastung. Kurz gesagt: Das Vertrauen in die IT-Plattformen ist nicht besonders hoch, während gleichzeitig viele Dienste nur noch über diese Kommunikationsmöglichkeit zu erreichen sind. Aus diesem Grund haben sich Ende 1999 mehrere IT-Firmen zu einer Allianz zusammengeschlossen, um gemeinsam Spezifikationen für sichere Plattformen zu entwickeln. Die heute unter dem Namen Trusted Computing Group (TCG) bekannte Vereinigung zählt inzwischen insgesamt 86 Mitglieder (Stand 3. November 2004), wobei einige der bedeutendsten Firmen der Branche (AMD, HP, IBM, Intel, Microsoft, Sony und Sun) maßgeblich die Entwicklungen steuern.

Mit den Mitteln eines „Kammerjägers“ ist den schädlichen Computerviren nicht beizukommen. Nur regelmäßig aktualisierte Antiviren-Programme garantieren Sicherheit.

Die TCG beabsichtigt, bestehende IT-Systeme (Computer, Handys, PDAs) durch eine Hardware-Erweiterung so weit vertrauenswürdig zu machen, dass in Zukunft die Sicherheit der eigenen Daten sowie der sichere Austausch von Daten mit unbekannten IT-Systemen besser als heute gewährleistet werden kann. Kritiker beanstanden allerdings das Missbrauchspotenzial, welches die Technologie birgt. So wird zwar die Hardware spezifiziert, die Sicherheit der Plattform bleibt jedoch davon abhängig, ob die Software die Hardware im gedachten Sinn nutzt, und die notwendige neue Infrastruktur vertrauenswürdig ist. Die bislang im Markt eingeführten Produkte beinhalten nur kleinere Software-Anwendungen. Es hat sich auch noch keine neue Infrastruktur herausgeformt.

Das BSI hat zu diesem Thema eine Arbeitsgruppe gebildet, welche sich nicht nur mit den Aktivitäten der TCG beschäftigt, sondern auch andere Entwicklungen zur Erstellung sicherer Plattformen untersucht.

Die Trusted Computing Group (TCG) hat ihren Hauptsitz in Portland/Oregon (USA) und wird von einem Komitee aus gewählten Vertretern der beteiligten Firmen geleitet. Da die Bandbreite der Unternehmen sehr weit reicht, kann die TCG geeignete Produkte für ganz unterschiedliche IT-Systeme entwickeln lassen.

Aktivitäten des BSI zur Trusted Computing Group (TCG)

Erstens

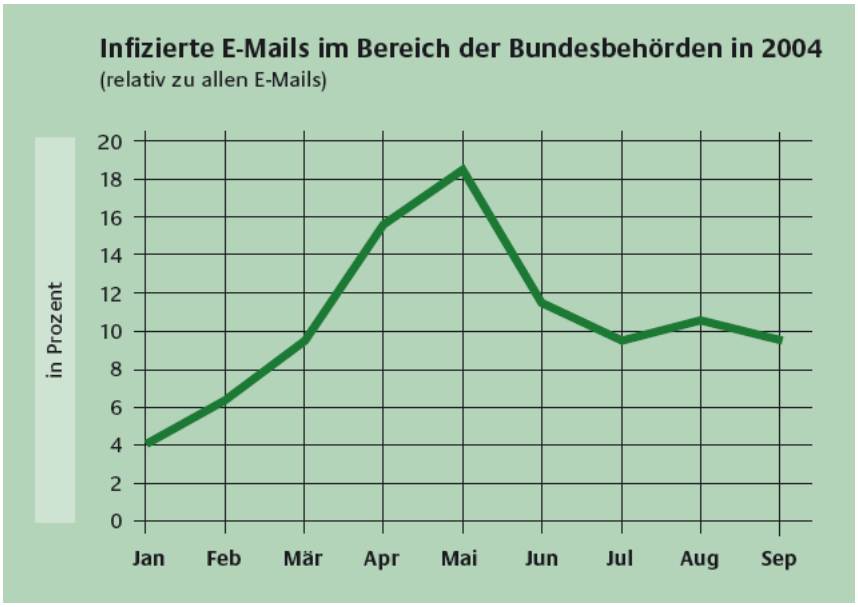
Mitarbeiter aus den unterschiedlichen Arbeitsgebieten des BSI haben bis Ende 2003 die Aktivitäten der TCG, der Vorgängerorganisation TCPA sowie der einzelnen Firmen, die auf dem Gebiet tätig sind, beobachtet. Ziel war es, Know-how bezüglich der neuen Technologie aufzubauen, um für Entscheider Transparenz zu schaffen und als zentraler Dienstleister für IT-Sicherheit Änderungs- und Nachbesserungsbedarf gegenüber beteiligten Organisationen und Firmen äußern zu können.

Zweitens

Im Jahr 2004 wurden diese Beobachtungen intensiviert und Sicherheitsanalysen der neuen Technologie aufgenommen. Dazu haben BSI-Mitarbeiter die Spezifikationen durchgearbeitet und zahlreiche Gespräche mit Vertretern der TCG geführt, bei denen die einzelnen Firmen ihre Entwicklungen erläutert haben und offene Fragen diskutiert wurden.

Drittens

Mit diesem Wissen wurde vom BSI ein Übersichtsreport erstellt, der das Trusted Platform Module (TPM) erläutert. Dieses Modul bildet die Grundlage der sicheren Plattform. Informationen hierzu wurden Ende des Jahres auf den Webseiten des BSI für Einsteiger und Entscheider veröffentlicht. Anhand dieser Beschreibung sollen Interessierte aufgeklärt und es für IT-Verantwortliche einfacher gemacht werden, die komplexe Thematik zu erfassen und notwendige Schlüsse zu ziehen.



Von vier Prozent im Januar auf 18 Prozent im Mai stieg der Anteil der infizierten E-Mails an allen Mails, die an Bundesbehörden gingen.

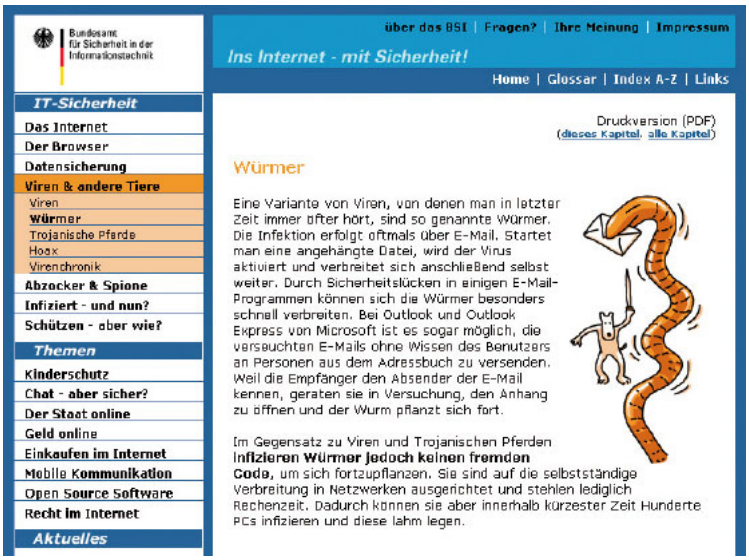
Angriffe über Dialer

Bis von einer sicheren Plattform ausgegangen werden kann, müssen die Gefahren anderweitig bekämpft werden. Damit Sicherheitsprobleme erkannt und entsprechende Schutzmaßnahmen entwickelt werden können, bedarf es einer Analyse der Angriffsszenarien. Eines davon ist der Angriff über sogenannte Dialer.

Die Abrechnung von minimalen Beträgen (sog. Micro-Payment) über die Telefonrechnung in Form von Dialern ist an und für sich eine recht gute und einfache Sache. Der Anbieter muss nicht aufwendig eine Rechnung stellen, den Zahlungseingang überprüfen und ggf. eine Mahnung schreiben. Alles wird über die Telefongebühren abgerechnet. Leider sind Dialer in Verruf geraten, weil Firmen versucht haben, ahnungslose Bürger zu prellen, insbesondere mit den 0190-Dialern. Seit dem 14. Dezember 2003 gilt: Kostenpflichtige Dialer dürfen nur noch über die Rufnummerngasse 0900-9- betrieben werden. Und sie müssen bei der Regulierungsbehörde für Telekommunikation und Post (Reg TP) registriert sein. Telekommunikationsunternehmen bieten seitdem an, kostenlos teure Vorwahlen zu sperren. Damit ist es Dialern nicht mehr möglich, sich unbemerkt auf den Rechnern von ahnungslosen Kunden einzunisten und teure Verbindungen aufzubauen.

Unseriöse Anbieter versuchten zeitweise, über Auslands-Rufnummern bei Telefonkunden auf unlautere Art Gebühren zu kassieren. Viele Kunden haben 2004 zu ihrer Überraschung auf ihrer Monatsabrechnung einen oder mehrere Posten gefunden, bei denen Verbindungen zu Rufnummern ins Ausland oder zu Satelliten aufgeführt sind. Durch schnelles Eingreifen der Netzbetreiber aufgrund der Warnungen des BSI konnten weitere Schäden vermieden werden.

Das BSI sammelt Informationen zu diesen neuen Methoden. Angaben über die gewählten Nummern, Dauer der Verbindungen, in Rechnung gestellte Kosten, Informationen über möglicherweise verdächtige Internet-Seiten (URL) sowie ein eventuell aufgefundenes Dialer-Programm, die dem BSI zugehen, werden nach Prüfung des Sachverhalts zur Sperrung an die zuständigen Netzbetreiber weitergeleitet. Bis Ende September 2004 wurden rund 3500 solcher Auslandsrufnummern als dialer-verdächtig gesperrt. Viele Bürger mussten nach ihren berechtigten Einwänden solche Posten nicht bezahlen beziehungsweise bekamen bereits abgebuchte Beträge gutgeschrieben.



Das Bundesamt erläutert auf speziellen Internetseiten www.bsi-fuer-buerger.de, was Bürgerinnen und Bürger über Würmer, Trojanische Pferde und Viren wissen sollten.

Sober, Sasser, Mydoom

Für Schlagzeilen und große Schäden sorgen neben Dialern vor allem Computerviren, Würmer und Trojanische Pferde. Auch im Jahr 2004 blieben die Computernutzer davon nicht verschont. Bemerkenswert ist: Es gab noch nie so viele gefährliche und stark verbreitete Viren wie im ersten Halbjahr 2004, und da besonders im Monat März.

Durchschnittlich waren monatlich rund sieben Prozent der von den zentralen E-Mail-Gateways der Bundesbehörden empfangenen E-Mails infiziert. Im Mai wurde eine Spitze mit über 18 Prozent erreicht. Das lag an dem Sober.G-Wurm. Wegen des deutschen Textes in der E-Mail verführte er gerade in Deutschland sehr viele Nutzer, die Datei-Anlage anzuklicken und damit den Wurm zu aktivieren.

Nur wenig Veränderungen gab es bei der Verteilung der einzelnen Virenarten. Nach wie vor müssen die meisten Programme mit Schadfunktionen als Würmer (über 60 Prozent) klassifiziert werden, gefolgt von Trojanischen Pferden (über 30 Prozent). Boot-Viren sind mittlerweile nahezu ausgestorben, was ursächlich mit dem Verschwinden der Diskette als Datenträger zusammenhängt. Die Viren und Würmer mit der größten Verbreitung im Jahre 2004 waren Sasser, Sober, Mydoom, Netsky und Bagle (beziehungsweise Beagle) mit ihren Varianten.

Es gelang, den Autor des Sasser-Wurms zu ermitteln. Er entpuppte sich außerdem als Urheber des Netsky-Wurms. Anklage ist erhoben, Prozessbeginn war im Frühjahr 2005.

2.2 Beglaubigte IT-Sicherheit: Zertifizierung

Die Zertifizierung von IT-Produkten auf Basis von international anerkannten IT-Sicherheitskriterien ist eine zentrale Aufgabe des BSI.

In mehreren Staaten ist der Einsatz zertifizierter Produkte, insbesondere in der öffentlichen Verwaltung, vorgeschrieben. Auch IT-Verantwortliche fordern zunehmend den Einsatz dieser Produkte, da es für den Anwender in der Regel schwierig ist, selbst Sicherheitseigenschaften zu bewerten. Eine neutrale unabhängige Prüfung – bestätigt durch das international anerkannte BSI-Zertifikat – gibt dem Anwender die Gewähr, dass das IT-Produkt die angegebenen Sicherheitsleistungen tatsächlich erbringt. Die Evaluierung wird im Rahmen des Zertifizierungsschemas des BSI von akkreditierten und lizenzierten Prüfstellen auf Basis der Common Criteria (CC, ISO/IEC 15408) durchgeführt. Beantragen können die Zertifizierung ein Hersteller, ein Vertreiber oder eine Bundesbehörde als Anwender.

In den Common Criteria sind Anforderungen an die Vertrauenswürdigkeit in sieben hierarchisch angelegten Stufen (Evaluation Assurance Level – EAL) zusammengefasst, von geringen Anforderungen (EAL1) bis hin zu den Anforderungen für den Einsatz im Bereich hochsensibler Daten (EAL7).

Die Common Criteria bieten Anwendergruppen und Herstellern die Möglichkeit, die jeweiligen Anforderungen für Produkt- und Systemklassen, wie Firewalls, Geldkarten oder Betriebssysteme, in Schutzprofilen (Protection Profiles) festzulegen. Diese Schutzprofile können Anforderungen an die IT-Sicherheit einer ganzen Kategorie von Produkten oder Systemen definieren, ohne dabei auf ein konkretes IT-Produkt oder -System Bezug zu nehmen. Mit Hilfe von Anforderungen aus den Common Criteria wird dann eine Musterlösung skizziert. Diese Musterlösungen werden sowohl von der ISO als auch auf entsprechenden nationalen Websites registriert und stehen damit weltweit zur Verfügung.

Auf diese Weise haben Autoren von Schutzprofilen die Möglichkeit, weltweit Standards zu setzen. Auch Behörden und internationale Organisationen können mit Hilfe von Schutzprofilen ihre Sicherheitsinteressen und Vorstellungen für bestimmte IT-Anwendungen und Produkttypen in Form eines standardisierten Sicherheitskonzepts zum Ausdruck bringen.

Ein Beispiel dafür ist das 2004 vom BSI gemeinsam mit dem deutschen Städte- und Gemeindebund sowie der Abfallwirtschaft definierte Schutzprofil WBIS zur Übertragung und Speicherung aufgezeichneter Leerungsdaten von Abfallbehältern. Es soll zukünftig in kommunalen Ausschreibungen verwendet werden.

Um Mehrfach-Zertifizierungen des gleichen Produktes in verschiedenen Staaten zu vermeiden, wurden die im folgenden aufgeführten Vereinbarungen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten getroffen.

ITSEC- und CC-Zertifikate

Das europäische Abkommen SOGIS bezieht sich auf Zertifikate aller Evaluierungsstufen. Sofern eine Nation über keine eigene Zertifizierungsstelle verfügt, handelt es sich um eine einseitige Anerkennung.

CC-Zertifikate

Eine Vereinbarung über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der Vertrauenswürdigkeitsstufe EAL4 wurde von den nationalen Stellen der folgenden Staaten unterzeichnet: Frankreich, Deutschland, Großbritannien, Kanada, den USA, gemeinsame Zertifizierungsstelle Australiens und Neuseelands, Japan, Finnland, Griechenland, Italien, Niederlande, Norwegen, Spanien, Israel, Schweden, Österreich, Türkei, Ungarn und Tschechische Republik. Weitere Nationen haben bereits ihr Interesse bekundet.

Die Länge des Verfahrens der Evaluierung und Zertifizierung kann – in Abhängigkeit von der Komplexität des Produkts und der angestrebten Evaluationsstufe – stark differieren. Damit das Zertifikat gleichzeitig mit dem Erscheinen des Produktes auf dem Markt erteilt werden kann, erfolgt die Evaluierung oft entwicklungsbegleitend.

Um den sehr kurzen Produktzyklen, insbesondere im Smart Card-Bereich, Rechnung zu tragen, wurden zusätzlich möglichst effiziente Verfahrensweisen zur Aufrechterhaltung eines Zertifikats international diskutiert und abgestimmt. Definiert wurde ein Verfahren zur sogenannten Assurance Continuity. Dieses ermöglicht dem Hersteller, mit Zustimmung der Zertifizierungsstelle bei geringfügigen Änderungen die Gültigkeit des Zertifikats aufrechtzuerhalten.

Das Verfahren wurde im Smart Card-Umfeld bereits angewandt. Es ist davon auszugehen, dass es in Zukunft breitere Verwendung finden wird. Dass es auch möglich ist, Open Source Produkte einer CC-Zertifizierung zu unterziehen, zeigt das Beispiel LINUX. Die 2002 begonnenen Aktivitäten führten zur Zertifizierung des SUSE LINUX Enterprise Server 8 und des RedHat Enterprise LINUX 3 AS/WS. Beide Betriebssysteme konnten als konform zum US-Schutzprofil CAPP (Controlled Access Protection Profile) nach der CC-Stufe EAL3 auf IBM Hardware-Plattformen zertifiziert werden. Zertifizierungen auf anderen Hardware-Plattformen (zum Beispiel von Hewlett-Packard) wurden ebenfalls durchgeführt oder sind in der Planung.

Das BSI arbeitet kontinuierlich in Projekten zur Schutzprofilentwicklung beziehungsweise Zertifizierung neuer Technologien mit. Dafür exemplarisch drei Beispiele:

Erstens

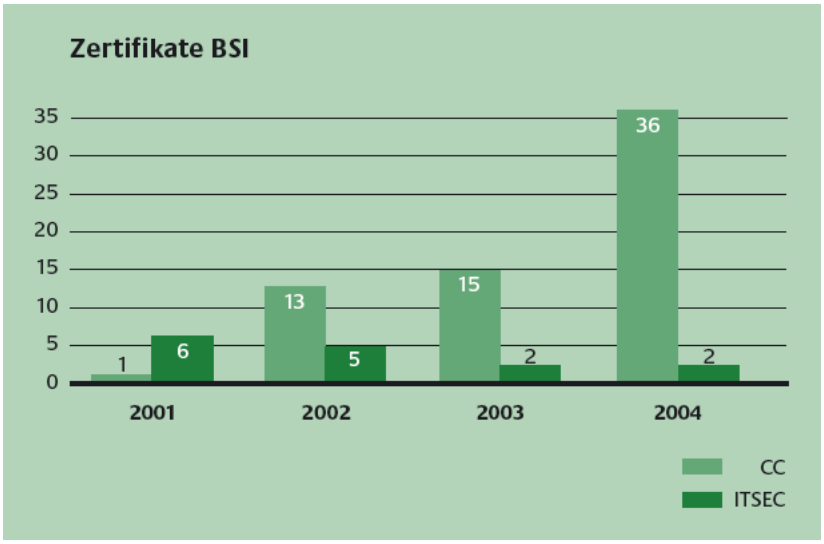
In Abstimmung mit der französischen Partnerbehörde DCSSI sowie dem Kraftfahrbundesamt, dem Bundesverkehrsministerium und der zuständigen Generaldirektion der EU-Kommission wurden Konzepte für die Zertifizierung von Komponenten des Digitalen Tachographen (Fahrtenschreiber) erarbeitet.

Zweitens

Weil davon auszugehen ist, dass zertifizierte Produkte zum Beispiel bei der Gesundheitskarte, im biometrischen Pass und im digitalen Personalausweis Verwendung finden werden, arbeitet das BSI an der Erstellung von Schutzprofilen für diese Bereiche. Erste Ergebnisse sind Anfang 2005 zu erwarten.

Drittens

In Zusammenarbeit mit europäischen Prüfstellen und Eurosmart wurde die Grundlagenarbeit zur Smart Card-Zertifizierung, die im Rahmen von eEurope begonnen wurde, in verschiedenen Arbeitsgruppen fortgesetzt.



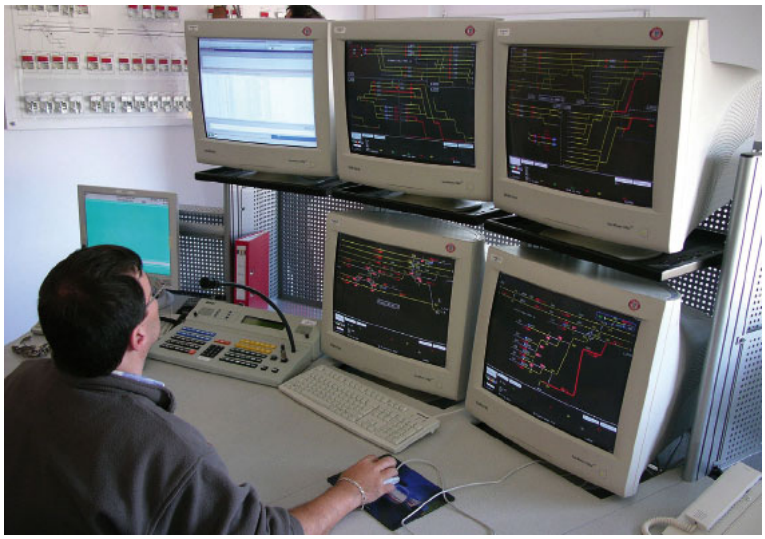
Das BSI zertifiziert IT-Produkte und IT-Systeme nach den internationalen Kriterien der Common Criteria oder der europäischen ITSEC. 2003 wurden 15 CC-Zertifikate erteilt; demgegenüber stehen 2004 36 CC-Zertifikate. Die Nachfrage nach ITSEC-Zertifizierung (2003: zwei Zertifikate; 2004: auch zwei Zertifikate) wird dagegen durch die Nachfrage nach CC-Zertifikaten ersetzt.

Um den Einstieg in die CC-Zertifizierung zu erleichtern, wurden die Anforderungen in Bezug auf die Spezifikation für niedrige Evaluierungsstufen (EAL1) überarbeitet. Dadurch reduziert sich der Aufwand für den Hersteller signifikant. Entsprechende Zertifizierungsverfahren werden bereits international durchgeführt.

Zur Erweiterung und Ergänzung der jetzigen Produktzertifizierung ist ein Verfahren für ganze IT-Produktlösungen in der Entwicklung. Das Zertifikat für eine IT-Produktlösung soll eine Gesamtsicht des Zusammenwirkens von Sicherheitsfunktionen und Produkteigenschaften bieten und gegebenenfalls nach CC zertifizierte Komponenten einbinden. Die Machbarkeitsstudie ist bereits erfolgreich abgeschlossen worden. Die Pilotphase startete im Dezember des Jahres 2004.

Dieses Sicherheitshandy (links) ist für fast alle Applikationen geeignet: USIM, Identification, Banking, PayTV. Das Produkt wurde Mitte dieses Jahres vom BSI nach Common Criteria E-AL 5+ zertifiziert. Der Digitale Tachograph (rechts oben) ist ein Fahrtenschreiber, der Lenk- und Ruhezeiten, Geschwindigkeit und Drehzahl erfasst. Sie werden auf dem Speicherchip der Fahrerkarte und dem Festspeicher des Geräts festgehalten.

BSI-Präsident Dr. Udo Helmbrecht (rechts) überreicht ein CC-Zertifikat an den Product Manager Smart Card IC Security, Hans-Gerd Albertsen, von Philips Semiconductors, Hamburg.



An Leitzentralen wie das Deutsche Bahn-Stellwerk in Frankfurt/Main-Ost werden hohe Sicherheitsanforderungen gestellt.

ICCC erstmals in Deutschland

Vom 28. bis 30. September 2004 fand die International Common Criteria Conference (ICCC) zum ersten Mal in Deutschland statt. Sie wurde zusammen mit der europäischen IT-Sicherheitskonferenz ISSE (Information Security Solutions Europe) in Berlin durchgeführt. Beide Konferenzen fanden zeitgleich statt, und es konnten mit insgesamt 650 Besuchern etwa doppelt so viele wie in den vorangegangenen Jahren begrüßt werden. Auch dieses Jahr wurde die ICCC wieder dazu genutzt, um 10 aktuelle CC-Zertifikate offiziell an die Hersteller zu überreichen. Zusätzlich wurde ein Report für Assurance Continuity übergeben.

BSI-Abteilungsleiter Bernd Kowalski (rechts) übergibt beim ICCC-Kongress ein Zertifikat an Mike Balma, HP Linux Strategy and Planning, Hewlett Packard Company.

2.3 IT-Grundschutz: Praxisorientierte Sicherheit

Informationssicherheit ist nicht nur eine Frage der Technik. Sie hängt in erheblichem Maße auch von den organisatorischen und personellen Rahmenbedingungen ab.

Dieser Erkenntnis trägt das IT-Grundschutzhandbuch des BSI seit langem Rechnung, indem es sowohl technische als auch nicht-technische Standard-Sicherheitsmaßnahmen für typische IT-Anwendungen und -Systeme empfiehlt.

Im Vordergrund stehen dabei praxisnahe und handlungsorientierte Hinweise mit dem Ziel, die Einstiegshürde in den Sicherheitsprozess so niedrig wie möglich zu halten und hochkomplexe Vorgehensweisen zu vermeiden. Mit diesem Ansatz hat sich das IT-Grundschutzhandbuch zu einem Standardwerk für IT-Sicherheit entwickelt. Über 3500 Anwender haben sich inzwischen freiwillig beim BSI registrieren lassen.

Das IT-Grundschutzhandbuch wird ständig weiterentwickelt und bedarfsgerecht um aktuelle Fachthemen ergänzt.

Eine wertvolle Hilfestellung für die Analyse und Bewertung der IT-Sicherheit bei der täglichen Arbeit bietet das IT-Grundschutzhandbuch. Neben konkreten Maßnahmen wird beschrieben, wie Defizite erkannt und dauerhaft beseitigt werden können.

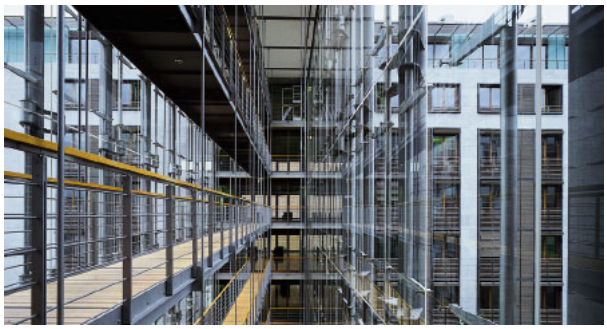
Outsourcing, Webserver, Outlook

Im Oktober 2003 erschien die 5. Ergänzungslieferung mit den Themen „Outsourcing“, „Internet Information Server“, „Apache Webserver“, „Exchange/Outlook 2000“ und „Archivierung“.

Aktualisierter Baustein „Firewall“

Ende 2004 kam die 6. Ergänzungslieferung heraus, die neue Kapitel zu den Themen „Router und Switches“, „S/390- und zSeries-Mainframe“ und „Personal Digital Assistant (PDA)“ enthält. Darüber hinaus wurde der existierende Baustein zum Thema „Firewall“ grundlegend überarbeitet.

Alle Versionen des IT-Grundschutzhandbuchs werden in gedruckter Form als Lose-Blatt-Sammlung beim Bundesanzeiger-Verlag sowie in elektronischer Form über die BSI-Website und auf CD-ROM veröffentlicht. Um die internationale Zusammenarbeit von Behörden und Unternehmen zu unterstützen, wird das vollständige Handbuch auch in englischer Sprache elektronisch zur Verfügung gestellt. Positive Resonanz hat auch die Veröffentlichung der neuen BSI-Methodik zur „Risikoanalyse auf der Basis von IT-Grundschutz“ ausgelöst. Das Dokument steht als PDF-Datei auf dem Webserver des BSI zur Verfügung.



Übergang im Jakob-Kaiser-Haus des Deutschen Bundestages. Sichere IT-Netzwerke verbinden Abgeordnetenbüros, Fraktionsstäbe und Parlamentsdienste.

Das GSTOOL steht Behörden kostenlos zur Verfügung

Parallel zum IT-Grundschutzhandbuch entwickelte das BSI mit dem GSTOOL (aktuell in der Version 3.1) eine komfortable und ergonomisch handhabbare Software, die das Vorgehen nach IT-Grundschutz auf elektronischem Weg durchgängig unterstützt. Es steht deutschen Behörden kostenlos zur Verfügung und wird dort ebenso wie in der freien Wirtschaft (kostenpflichtig) überaus positiv angenommen. Belegt wird die positive Resonanz durch aktuell über 4000 vergebene Lizenzen im Behördenbereich und durch mehr als 500 verkaufte Lizenzen an – zum Teil international agierende – Unternehmen (Großkunden sind beispielsweise Siemens und MAN). Seit Mitte 2004 steht auch eine englische Version des GSTOOL zur Verfügung.

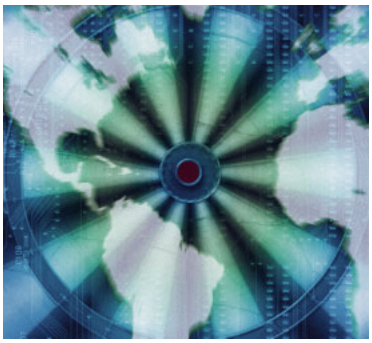
Weil das vom BSI entwickelte IT-Grundschutzhandbuch mit der Zeit immer umfangreicher geworden ist, wurde der Ruf nach beispielhaft nachvollziehbaren Sicherheitskonzepten immer lauter. Mit der Darstellung von drei Profilen für unterschiedliche Organisationsgrößen wurde der Vorgang, ein Sicherheitskonzept zu planen, umzusetzen und zu pflegen, exemplarisch mit vielen Hilfen und Tipps erläutert.

Profile ermöglichen eine schnelle Umsetzung

Zusätzlich enthält das neue IT-Grundschutzhandbuch Richtlinien zur Internet- und E-Mail-Nutzung, ein Viren-Schutzkonzept, ein Datensicherungskonzept, ein Notfallvorsorgekonzept und ein Archivierungskonzept. Diese auf die jeweilige Institution zugeschnittenen Profile sollen ihre schnelle Umsetzung ermöglichen. Die Musterdokumente zeigen, welche IT-Sicherheitsthemen besonders wichtig sind und wie eine hierarchische Anordnung von Richtlinien aussehen kann.

Neben diesen Hilfestellungen bieten vom BSI geschulte und geprüfte Auditoren ihre Unterstützung an. Die Nachfrage nach einer Lizenzierung als IT-Grundschutz-Auditor ist nach wie vor ungebrochen. So hat sich die Zahl dieser Experten für IT-Grundschutz im Jahre 2004 auf 125 erhöht. Sie sind für das BSI außerdem wichtige Multiplikatoren in die Fachöffentlichkeit.

Auch die Nachfrage nach einer Grundschutz-Zertifizierung steigt stetig. Dabei wurde deutlich, dass sich viele Institutionen noch in der Umsetzungsphase befinden, aber klar auf die Zertifizierung abzielen. Dies zeigt, das BSI geht den richtigen Weg: IT-Grundschutz ist durch Zertifikate nachweisbar. Dieser Weg muss in den nächsten Jahren weiter beschritten und ausgebaut werden.



3 Im Angebot: Produkte für höchste Ansprüche

Produkte des BSI haben sich in dem anspruchsvollen Umfeld der nationalen und internationalen Sicherheitstechnik durchsetzen können. Nicht nur die NATO, auch die EU bauen heute auf Leistungen aus dem BSI.

Ob es um Verschlüsselungstechnik geht, Spionageabwehr, die elektronische Kommunikation mit Behördennetzen oder ob schlicht eine Einschätzung verlangt ist, welche Schließ- oder Aufbewahrungssysteme genügend Sicherheit bieten – stets hat sich das BSI an höchsten Ansprüchen und an dem neuesten Stand der Technik zu orientieren. Dass die Bundeswehr ihre militärischen Einheiten mit dem vom BSI entwickelten ISDN-Kryptosystem Elcrodat 6-2 ausrüsten wird, spricht für sich selbst.

Auch der vor seiner Einführung stehende BOS-Digitalfunk für Polizei und Feuerwehr wurde vom BSI mit entwickelt. Er wird die Kommunikation der Sicherheitsbehörden abhörsicher machen. Experten des BSI prüfen und begleiten Baumaßnahmen für die öffentliche Hand, wenn es um einen wirksamen Abhörschutz und eine konsequente Lauschabwehr geht.

Das E-Government-Handbuch ist online verfügbar und enthält detaillierte Informationen, die Akzeptanz und Erfolg elektronischer Dienstleistungen betreffen.

3.1 Führend im Geheimschutz

Ob „Top Secret“, „Secret“ oder „Vertraulich“ – wenn es um klassifizierte Informationen der Regierung, der Verwaltung, des Militärs oder der dem Geheimschutz unterliegenden Industrie geht, gibt es keine Kompromisse.

An Verschlüsselungssysteme werden höchste Anforderungen gestellt, was ihre Vertraulichkeit und Integrität betrifft. Die Produkte des BSI haben sich in diesem anspruchsvollen Umfeld auch international durchsetzen können und werden sowohl bei der NATO als auch bei der EU eingesetzt.

Das ISDN-Kryptosystem Elcrodat 6-2 sichert nicht nur die Regierungskommunikation in Deutschland; inzwischen hat sich nach einer aufwändigen Auswahlprozedur auch die NATO für das innovative Produkt entschieden. Elcrodat 6-2 wurde im Auftrag des BSI durch die Firma Rohde & Schwarz SIT GmbH realisiert. Zahlreiche darauf aufbauende Weiterentwicklungen sind in Planung oder bereits beauftragt. Sie sichern die Zukunftsfähigkeit des Systems.

In der Entwicklung ist ein „Gateway“, also ein Bindeglied zwischen dem digitalen ISDN und bereits vorhandenen, auf analogen Netzen beruhenden Kryptosystemen. Ein Erweiterungsmodul für das Elcrodat 6-2 soll die kryptographischen und Interoperabilitätseigenschaften weiter verbessern sowie das Sicherheitsmanagement modernisieren und funktional erweitern.

In der EU-Verwaltung ist das Elcrodat 6-2 bereits im Einsatz und hat eine Zulassung bis EU-Secret erhalten. Einem noch breiteren Einsatz innerhalb der EU und ihrer Organe steht nichts mehr im Wege. Wegen des Erfolgs der Systeme in den Kommunikationsnetzen der NATO und der EU entscheiden sich immer mehr Mitgliedsländer für den Einsatz des Elcrodat 6-2 in ihrer nationalen Kommunikation. Das unterstreicht das gewonnene Vertrauen in das BSI und in die deutsche Kryptoindustrie.

Der taktische Militärtransporter A 400 M, an dessen Entwicklung mehrere europäische Länder beteiligt sind, wird mit Elcrodat-Verschlüsselungstechnik ausgerüstet.

Schwarz, sicher und kompakt – die neueste Version des Elcrodat 6-2 ist international im Einsatz und hat sich bewährt (links). Auch die EU hat sich für diese Verschlüsselungstechnik entschieden – rechts im Bild die Brüsseler Zentrale der EU-Kommission.

Produkt- und Systeminnovationen mit SINA

Mit SINA hat das BSI ein weiteres national wie international erfolgreiches Hochsicherheitsprodukt im Angebot: Die „Sichere Inter-Netzwerk Architektur (SINA)“ ist eine VPN-Lösung, mit der sich über das ansonsten unsichere Internet hochsichere Verbindungen aufbauen lassen.

In den vergangenen fünf Jahren ist um SINA herum eine ganze Produktfamilie gewachsen. So bieten sich weitere Ansatzpunkte für Produkt- und Systeminnovationen. Diverse Einsatzszenarien lassen sich mit der vom BSI und der Firma secunet Security Networks AG entwickelten Hochsicherheitslösung abdecken. 2004 wurde eine Basisversion der neuen „SINA Virtual Workstation (SINA-VW)“ fertiggestellt. Sie erlaubt einen hochsicheren Remote Access (Fernzugriff) zu Unternehmensnetzen über Festnetz und Mobilfunk. Der ebenfalls 2004 fertiggestellte Prototyp eines „SINA Encapsulated Encrypted Servers (SINA-E2S)“ ist ein weiteres Beispiel für eine Produktinnovation mit SINA im Serverbereich. Die Nachfrage nach SINA-Komponenten bei NATO und EU-Mitgliedsländern steigt stetig. Zahlreiche Systeme sind bereits im Einsatz oder es liegen Aufträge vor. Die EU zieht SINA-Komponenten für verschiedene zukünftige Anwendungen in Betracht. Die erforderliche EU-Zweitevaluierung steht kurz vor dem Abschluss.

Nachdem die Bundeswehr rund 8000 Stück des in SINA eingesetzten Kryptochips „PLUTO“ bestellt hat, ergeben sich enorme Einsatzperspektiven für die High-End-Version des Systems, die alle bisherigen Erwartungen übertrifft.

Das Auswärtige Amt wickelt die Kommunikation mit den 217 Auslandsvertretungen der Bundesrepublik Deutschland über das Internet ab. Die SINA-Technologie (Geräte dafür siehe links) garantiert, dass geheime Informationen auch geheim bleiben.

Moderne kryptographische Anwendungen und Sicherheitsmodule

Das BSI setzt künftig bei der Verschlüsselung von Daten weitgehend auf programmierbare Kryptokomponenten. Die moderne Chiptechnologie macht extrem leistungsfähige kryptographische Implementierungen für praktisch alle Anwendungszwecke möglich. Damit diese Verfahren genau so sicher und vertrauenswürdig sind wie herkömmliche, müssen intelligent gesicherte Misch-(Hybrid-)Systeme konzipiert werden. Das BSI arbeitet intensiv mit seinen Industriepartnern, aber auch mit Wissenschaftlern, an einsatzfähigen und flexiblen Lösungen. Dabei entstehen ganze Produktlinien sogenannter „Dedizierter Krypto Service Provider (DCSP)". Das sind speziell angepasste Bausteine, die in das jeweilige Kryptosystem integriert werden können.

Eine der größten Herausforderungen auf diesem Gebiet wird die Entwicklung eines hochmodularen „Infosec Moduls" für die neue Generation der „Software Defined Radios (SDR)" sein. Diese Funkgeräteplattformen sind für verschiedene Funkwellenformen ausgelegt, die als Software (nach-)geladen werden können. Die völlig neuen Anwendungsperspektiven, die sich damit eröffnen, werden den Funkgerätemarkt revolutionieren. Im BSI laufen die Planungen für ein solches Projekt derzeit auf Hochtouren.

BSI-System sichert künftigen digitalen Funkverkehr.
Ob Polizei, Feuerwehr oder Rettungswesen – alle „Behörden und Organisationen mit Sicherheitsaufgaben (BOS)" sollen in Zukunft über einen einheitlichen digitalen Funk kommunizieren. Das so entstehende größte kryptographisch gesicherte Funknetz Europas (BOS-Funk) wird dann wohl mit der kleinsten Kryptokomponente der Welt ausgestattet. Das Sicherheitssystem für den digitalen BOS-Funk wurde komplett vom BSI entwickelt und setzt Maßstäbe in Sachen skalierbare Sicherheit, Modularität, Wirtschaftlichkeit und Funktionalität. Dabei passt es auf eine handelsübliche SIM-Karte.

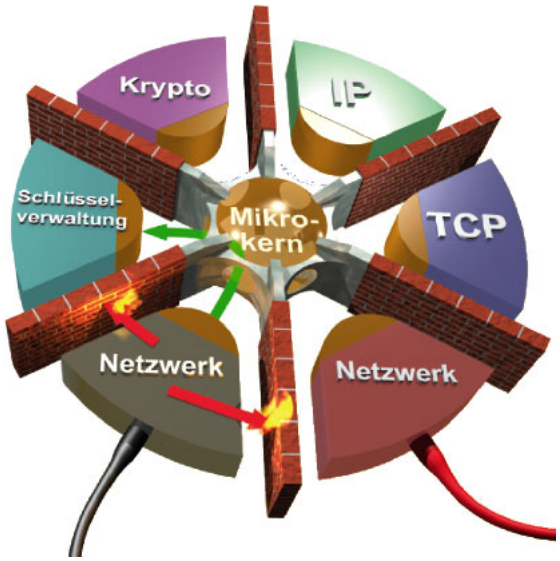
Auch Fregatten der Bundesmarine (im Bild links die „Bayern") sollen mit Hilfe des BSI mit Verschlüsselungstechnik ausgerüstet werden.

Hochsichere Informationsverarbeitung mit der „L4VM“ Plattform

Handelsübliche (auch Open Source-basierte) Betriebssysteme haben eine „monolithische Architektur“. Das bedeutet: Sie werden von einem ganzen zusammenhängenden Programmcode mit vielen Millionen Codezeilen gesteuert. Solche Systeme entziehen sich auf Grund ihrer Komplexität prinzipiell einer höherwertigen Evaluierung/Überprüfung und Zertifizierung.

Für hochschützenswerte IT-Anwendungen werden jedoch vertrauenswürdige Rechnerplattformen benötigt. Mit dem Projekt „L4VM“ soll eine völlig neue Betriebssystemarchitektur für Hochsicherheitsanwendungen entstehen. Ziel ist, ein bestehendes Betriebssystem auf einem anderen, besonders gesicherten Betriebssystemkern laufen zu lassen, dem Mikrokern. Dieser nutzt separate Adressräume des physikalischen Speichers für die Kapselung von Anwendungen. Er ist die zentrale Komponente, die als einzige mit den besten und sichersten Privilegien ausgestattet ist, die in der Rechnerarchitektur zur Verfügung stehen.

Die Kommunikationsinfrastruktur, die von einem Mikrokern bereitgestellt wird, besteht im Wesentlichen aus hochoptimierter nachrichtenbasierter Inter-Prozess-Kommunikation (IPC). Die geringe Funktionalität des Mikrokerns wird durch schlanke Applikationen erweitert. Diese Applikationen stellen unterschiedliche Dienste bereit und sind als Trusted Service Provider (TSP) Bestandteil der Trusted Computing Base der Plattform.



Schema für die Mikrokern-Architektur: Ankommende Informationen werden nur über den gesicherten Mikrokern weitergegeben. Firewalls schotten die einzelnen Programmsegmente wie Schlüsselverwaltung, Netzwerkprogramme und andere untereinander ab.

Das Ergebnis

Programmierfehler oder Angriffe führen auf einer mikrokernbasierten Plattform höchstens zum Ausfall einer entsprechenden Komponente, nicht aber zu einer Kompromittierung des Gesamtsystems.

Für den notwendigen Einsatz von Betriebssystemen auf dieser Plattform gibt es zwei Varianten. Ist die Anpassung eines bestehenden Betriebssystems an die L4-Schnittstelle möglich, zum Beispiel bei Open-Source, spricht man von Paravirtualisierung. Durch Paravirtualisierung entsteht nur ein geringer Verzögerungseffekt in der Laufzeit. Er ist für normale Büroanwendungen nicht spürbar.

Für proprietäre Betriebssysteme ist diese Vorgehensweise nicht möglich. Bei dieser Variante muss ein Monitor eine Virtualisierungsschicht bereitstellen und die Systemaufrufe des Betriebssystems an die Hardware weitergeben beziehungsweise privilegierte Instruktionen über den Mikrokern abwickeln. Durch eine eigens hierfür entwickelte „Virtuelle Maschine (L4VM)“ wird erreicht, dass der Benutzer weitgehend das gleiche „look and feel“ haben wird wie auf einer herkömmlichen Rechnerplattform.

Hardware im Hochsicherheitsbereich

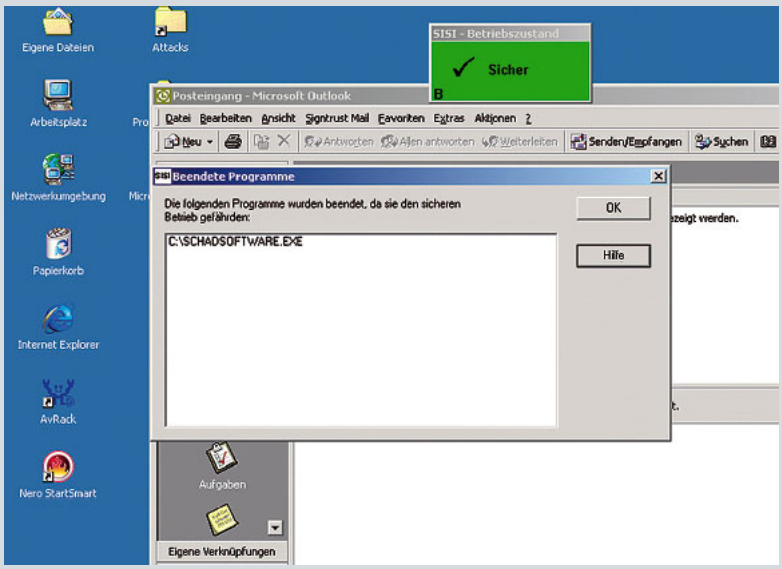
Während Sicherheitsmodule für den Hochsicherheitsbereich bisher typischerweise fest verdrahtete Chips (sog. Krypto-ASICs – Application Specific Integrated Circuit) verwenden, gewinnt bei Neuentwicklungen unter anderem aus Kosten- und Flexibilitätsgründen der Einsatz von rekonfigurierbarer (neu zu programmierender) Hardware an Bedeutung.

Besonders hervorzuheben sind FPGAs (Field Programmable Gate Arrays), deren Leistungsfähigkeit in den letzten Jahren deutlich gestiegen ist. Vom BSI in Zusammenarbeit mit Universitäten durchgeführte Studien und eigene Analysen zeigen, dass mit den heute verfügbaren FPGAs auch komplexe Kryptosysteme für Hochsicherheits- und Hochgeschwindigkeitsanwendungen entwickelt werden können.

Als „Sicherheitsanker“ und in Ergänzung zu den schnellen und flexiblen FPGAs bieten sich im Hochsicherheitsbereich Smart Cards an, die aus vertrauenswürdiger Fertigung stammen und mit einem zertifizierten Betriebssystem ausgestattet sind. Aufgrund der breit gefächerten Verwendung von Smart Cards in verschiedenen kommerziellen Sicherheitsanwendungen werden diese regelmäßig sicherheitstechnisch optimiert.

SISI – Sicherheit bei digitalen Signaturen

Das vom BSI mit der TC TrustCenter AG Hamburg entwickelte Programm „Sichere SignaturInfrastruktur" (SISI) beseitigt das Defizit bei der Bereitstellung eines sicheren Umgangs mit Signaturen in einer Standard-PC-Umgebung. Das Problem ist die Angreifbarkeit der Signatur-Software wegen der Schwachstellen von Standardbetriebssystemen. Eine Software, die in einer PC-Umgebung Sicherheit für digitale Signaturen garantiert, muss die wichtigsten Bedrohungen ausschließen können. Die SISI-Schutzsoftware ermöglicht es den PC-Benutzern, ein Programm zur Erstellung elektronischer Signaturen für Vertragsdokumente so zu betreiben, dass Manipulationen durch Schadsoftware weitestgehend erkannt und ausgeschlossen werden können. Die Schutzsoftware läuft unter einem der professionellen Microsoft-Windows-Betriebssysteme oder einer verbreiteten Linux-Distribution wie SuSE 9.0.



SISI passt auf: Die Signatursoftware läuft – wie hier im Bild – unter dem ganz normalen und weit verbreiteten Microsoft Outlook Programm.

3.2 Spionageabwehr und Abhörschutz

Das BSI befasst sich auch mit dem Schutz des gesprochenen Wortes. Betroffen ist dabei vor allem der Bereich des staatlichen Geheimschutzes.

Das klassische Instrument zum Ausspionieren von Gesprächsinhalten ist die „Wanze“. Derartige Abhörgeräte sind in so genannten Spy-Shops oder im Internet erhältlich. Ihr Besitz – und erst recht der Einsatz – sind selbstverständlich illegal. Ausreichende kriminelle Energie vorausgesetzt, lassen sie sich aber durchaus beschaffen und auch benutzen.

Während mit „klassischen“ Lauschgeräten Raum- oder Telefongespräche abgehört werden können, sind mittlerweile Miniatur-Funkkameras zur Übertragung von Bildinformationen erhältlich. Je nach Einsatzdauer und Einbaumöglichkeiten beziehen sie ihre Stromversorgung aus Batterien oder über Netz- beziehungsweise Telefonleitungen; diese werden auch zur Informationsübertragung genutzt – das ist unauffälliger als eine Funkverbindung und weniger riskant. Herkömmliche „Wanzen“ sind gewöhnlich an schwer zugänglichen Stellen versteckt oder in Gebrauchsgegenstände eingebaut.

Fremde Nachrichtendienste dagegen werden sich nicht auf derartige, für jedermann verfügbare Minispione beschränken. Sie führen ihre Angriffe mit hochprofessionellen Methoden aus, von langer Hand vorbereitet und aufwendig getarnt. So muss zum Beispiel damit gerechnet werden, dass Abhörgeräte gut versteckt in das vorhandene Leitungs- oder Datennetz integriert oder sogar schon während der Rohbauphase in die Bausubstanz geschmuggelt werden.

Sechste Etage Bundeskanzleramt: Blick in den Großen Kabinettssaal. Dass dieser Raum abhörsicher sein muss versteht sich von selbst.

Die drei Säulen der Lauschabwehr

1. Baulich-technische Schutzmaßnahmen

Das BSI begleitet Bauvorhaben, für die ein Abhörschutz erforderlich ist, schon in der Planungsphase. Lauschabwehrmaßnahmen sind mit hohem finanziellen und personellen Aufwand verbunden. Daher wird in Beratungsgesprächen mit dem späteren Nutzer des Gebäudes zunächst analysiert, in welchen Büro- und Besprechungsräumen sensitive, schützenswerte Gespräche stattfinden sollen. Nur für diese Räume werden dann Abhörschutzmaßnahmen vorgesehen. Ziel ist es, Abhörversuche zu verhindern oder zumindest zu erschweren und spätere Lauschabwehrprüfungen wirksam, aber mit vertretbarem Aufwand durchführen zu können. Beispiele:

- Ausreichende Schalldämmung von Wänden, Fenstern und Türen, um „direktes“ Abhören, zum Beispiel mit Richtmikrofonen, zu verhindern;
- Verschließen von Hohlräumen und Wanddurchbrüchen, die sich als Versteckmöglichkeit für Lauschgeräte eignen;
- Übersichtliche, effizient prüfbare Elektro- und IT-Installation.

Als Zusatzmaßnahme können besonders gefährdete Besprechungsräume mit einer elektromagnetischen Abschirmung versehen werden, die eine Signalübertragung eventuell vorhandener Lauschgeräte nach außen verhindert. Die Realisierung der Abhörschutzmaßnahmen wird durch Spezialisten des BSI während der gesamten Bauphase beratend begleitet.

2. Materielle und personelle Sicherungsmaßnahmen

Die Überprüfung abhörgeschützter Räume auf „Wanzenfreiheit“ kann, egal wie oft sie durchgeführt wird, immer nur eine Momentaufnahme darstellen. Daher muss ständig sicher gestellt werden, dass kein potenzieller Angreifer in abhörgeschützte Räume gelangen kann, um dort Lauschmittel zu deponieren. Das wird durch den ständigen Verschluss der Räume außerhalb der Nutzungszeiten sicher gestellt. Ein unbefugtes Eindringen muss in jedem Fall erkannt werden, beispielsweise durch eine Alarmanlage. Angehörige von „Fremdpersonal“, wie zum Beispiel Handwerker, dürfen sich nie ohne Aufsicht in den Räumen aufhalten.

In der TicTac-Dose ist eine „Wanze“ versteckt. Solche Geräte können unauffällig im Raum platziert, und die Informationen dann mit einem Handscanner empfangen werden.

3. Regelmäßige Lauschabwehrprüfungen

Die Lauschabwehrprüfungen dienen zur Kontrolle der baulich-technischen Schutzmaßnahmen (zum Beispiel auf ausreichende Schalldämmung) sowie zur Erkennung und Beseitigung eventuell vorhandener Abhörgeräte. Die Prüfungen werden erstmals nach Fertigstellung abhörgeschützter Räume und in der Folgezeit regelmäßig durchgeführt. Auch bei besonderen Anlässen ist eine Lauschabwehrprüfung fällig. Das BSI verfügt über drei erfahrene Prüfgruppen. Sie setzen hochwertige Spezialausrüstung ein. Der technische Fortschritt ermöglicht auf der einen Seite den Bau immer kleinerer und leistungsfähigerer Abhöranlagen, auf der anderen Seite bieten sich aber auch neue Möglichkeiten, versteckte Abhöranlagen besser zu erkennen. Unter Nutzung neuer Technologien entwickelt das BSI hochmoderne Geräte und Methoden zum Aufspüren professioneller Abhörgeräte.

Missbrauch von Telekommunikationsanlagen

Abhörangriffe erfordern nicht unbedingt den direkten Zugang des Angreifers zum zu überwachenden Raum. In jedem modernen Büro- und Konferenzraum befindet sich Kommunikationstechnik mit Mikrofonen, die etwa durch Manipulation von außen zum Abhören des Raumgesprächs missbraucht werden können. So bietet zum Beispiel jede Telekommunikationsanlage die Möglichkeit, über das eingebaute Freisprechmikrofon den Raumschall mitzuhören oder sich auf ein bestehendes Gespräch unbemerkt aufzuschalten. Unbefugte, die zum Beispiel über eine Fernwartungsschnittstelle in eine TK-Anlage eindringen, können derartige Leistungsmerkmale unauffällig aktivieren. Das BSI erarbeitet Schutzkonzepte, um TK-Anlagen abzuschirmen, und entwickelt automatische Prüftools, um sie regelmäßig kontrollieren zu können.

Bloßstellende Abstrahlung

Jedes elektronische Gerät, das Informationen verarbeitet, strahlt elektromagnetische Wellen ab. Experten nennen sie „bloßstellende Abstrahlung“. Fängt man sie aus einiger Entfernung mit einer Antenne auf, lässt sich die Information mittels Empfänger und nachgeschalteter Signalverarbeitung wieder rekonstruieren. Um diese Möglichkeit des Ausspähens von Daten zu unterbinden, entwickelt das BSI Messverfahren zum Nachweis der bloßstellenden Abstrahlung und setzt Vorgaben für entsprechende Grenzwerte. Geräte, die im Bereich des staatlichen Geheimschutzes eingesetzt werden, müssen diese Grenzwerte einhalten und erhalten dann eine Zulassung vom BSI.

Selbst Panzer werden im Referat „Abstrahlsicherheit“ des BSI untersucht. Dafür steht eine eigene zehn mal dreizehn Meter große Garage zur Verfügung.

3.3 Sichere Kommunikation im E-Government

Mit den Lösungen, die das BSI entwickelt hat, ist es ohne Probleme möglich, sicher elektronisch zu kommunizieren. Das ist eine wichtige Voraussetzung für die Weiterentwicklung von E-Government bei den Behörden des Bundes, der Länder und der Kommunen.

E-Government steht nach wie vor ganz oben auf der Agenda von Politik und Verwaltung. Als Inbegriff der Verwaltungsmodernisierung verspricht man sich davon eine stärkere Kundenorientierung und Einsparungen bei der Verwaltung. Erreicht werden soll dies durch den konsequenten Einsatz von Informationstechnik bei allen Dienstleistungen vom Kunden bis zum Sachbearbeiter. Gleichzeitig sollen Behördenvorgänge überprüft, neu gestaltet und durch „schlankere" Prozesse ersetzt werden.

Das BSI unterstützt die Initiativen Bund-Online 2005 (www.bund.de) und Deutschland-Online (www.deutschland-online.de). Die Einführung von E-Government geht einher mit

- der Öffnung von zuvor geschlossenen Behörden-Computer-Netzen zum Internet,
- dem Einsatz von zusätzlicher Informationstechnik zur Kommunikation über offene Netze und
- dem Übergang von papiergebundenen Dokumenten zu elektronisch geführten Akten.

Und in allen Punkten ist das Bundesamt für Sicherheit in der Informationstechnik gefordert. Das BSI hat die Aufgabe, auf kritische Aspekte hinzuweisen, dafür zu sorgen, dass die neuen Dienstleistungen sicher sind und dass sie von den Bürgern ohne die Befürchtung benutzt werden können, sie würden ihre informationelle Selbstbestimmung gefährden. Wichtig ist, rechtzeitig auf IT-Sicherheit zu achten, denn Nachrüsten ist teuer und bringt keine zufriedenstellenden Lösungen.

Basis aller E-Government-Dienstleistungen ist das Abrufen im Internet bereitgestellter Informationen. Beim E-Government kommuniziert eine Behörde mit ihren Kunden auf elektronischem Weg. Akzeptanz und Erfolg solcher elektronischen Dienstleistungen hängen ganz wesentlich von ihrer Nutzbarkeit (usability) ab. Das BSI hält dazu detaillierte Informationen bereit, die im Modul „Sichere Kommunikation im E-Government" in der kostenlosen Online-Version des E-Government-Handbuchs nachzulesen sind.

Eine besondere Gefährdung der elektronischen Kommunikation, sei es beim Versenden von E-Mails oder beim Ausfüllen von Web-Formularen, entsteht durch die leicht zu fälschenden Absenderadressen. Außerdem können übermittelte Informationen mitgelesen oder sogar manipuliert werden. Aus der Papierpost bekannte Schutzmechanismen wie zum Beispiel verschlossene Briefumschläge, manuelle („händische“) Unterschriften, geschwärzte Rückseiten bei vertraulichen Inhalten greifen hier nicht, dazu müssen kryptographische Schutzmechanismen eingesetzt werden.

Die Lösung bietet die virtuelle Poststelle, die vom BSI entwickelt wurde. Sie bietet für die elektronische Kommunikation einen sicheren und gleichzeitig komfortablen Weg. Denn Sicherheit wird nur dann akzeptiert, wenn die zu Grunde liegenden Mechanismen möglichst unauffällig im Hintergrund wirken. E-Mails und Web-Inhalte können durch die virtuelle Poststelle zentral in der Behörde ver- und entschlüsselt werden. Bürger wie Behörden können Signaturen anbringen, sie auf ihre Echtheit prüfen und anderes mehr. Ein Mitlesen durch Dritte, das Vortäuschen eines falschen Absenders oder ein unbemerktes Verändern der übermittelten Inhalte ist ausgeschlossen.

Speziell für Privatanwender oder besondere Berufsgruppen hat das BSI daran anknüpfend noch eine weitere Vereinfachung entwickelt: das so genannte Elektronische Gerichts- und Verwaltungspostfach. Dieses spezielle Kommunikationsprogramm basiert auf einer Signaturkarte und kann auf dem PC jedes Kunden, der mit der Behörde kommunizieren möchte, problemlos installiert und ohne spezielle technische Kenntnis für die verschlüsselte und signierte Kommunikation eingesetzt werden. Qualifizierte elektronische Signaturen machen es auf diese Weise möglich, rechtsverbindlich mit Behörden zu kommunizieren – vorausgesetzt der Nutzer verfügt über eine Signaturkarte. Dies sollte aber zumindest für Selbstständige und Unternehmen angesichts der mit E-Government verbundenen Einsparmöglichkeiten keine große Hürde sein.

Für die Kommunikation zwischen Behörden bietet das BSI weitere Lösungen an. Die SPHINX-kompatiblen E-Mail-Clients etwa garantieren absolute Ende-zu-Ende-Sicherheit. Für das Behördennetz IVBB (Informationsverbund Berlin-Bonn) ist das BSI verantwortlich. Das BSI stellt darüber hinaus spezielle Programme für die Verschlüsselung entsprechend geheim eingestufter Informationen bereit.

Kinderleicht und sicher sollen Bürger künftig mit ihrer Verwaltung Kontakt aufnehmen können.

Bund, Länder und Kommunen stehen hinter der Website „Deutschland-Online“ (links). Nach dem Prinzip „Einige für alle“ werden auf allen Ebenen Modellvorhaben im E-Government verwirklicht. „BundOnline“ ist Teil des Dienstleistungsportals des Bundes (www.bund.de). Alle onlinefähigen Dienstleistungen des Bundes sollen elektronisch verfügbar gemacht werden.

Die beiden markanten Türme gehören zum Dienstgebäude des Bundesministeriums des Innern.

IVBB – Entwicklungen und neue Dienste im Jahr 2004

Der Informationsverbund Berlin-Bonn (IVBB), der mit seinen zentralen Diensten Telefon, E-Mail und Internetnutzung bereits seit 1998 erfolgreich in Betrieb ist, wächst stetig weiter und muss laufend den Anforderungen der angeschlossenen Nutzer und den sich ändernden Rahmenbedingungen angepasst werden.

Im Jahre 2004 wurden besonders die E-Mail-Systeme erheblich erweitert, um das stark gestiegene Kommunikationsaufkommen problemlos bewältigen zu können. Ferner wurde eine leistungsfähige Spam-Filterung installiert. Da der Anteil der E-Mails, der durch Spam-Versender, Viren und Würmer verursacht wird, gegenüber regulären E-Mails stetig wächst, ist ein solcher Filter, der eingehende E-Mails analysiert und entsprechend kennzeichnet, unverzichtbar.

Außerdem ist es seit diesem Jahr möglich, zwischen den angeschlossenen Häusern nicht nur Daten auf geschütztem Wege auszutauschen, sondern auch verschlüsselt zu telefonieren. Zum Einsatz kommt dabei das im Auftrag des BSI entwickelte Produkt „Elcrodat 6-2M“. Neu ist das Bibliothekenportal, welches die Ressourcen der einzelnen Bibliotheken im IVBB bündelt, und ein zentrales Alarmsystem, das in Zusammenarbeit mit CERT-Bund im IVBB implementiert wurde.

Der Informationsverbund stellt außerdem ständig eine Reihe von Servicediensten zur Verfügung, darunter zentrale Voice-, Mail- und Faxdienste, den Betrieb einer Infoserverzone für Informationsangebote der angeschlossenen Häuser und den Zugang von und zu mobilen Arbeitsplätzen.
Die Leistungen des BSI garantieren, dass der IVBB den Anforderungen an ein sicheres und hochverfügbares Netz für die Kommunikation der Bundesregierung auch in Zukunft gerecht wird.

Videokonferenzen zwischen Bonn und Berlin gehören im IVBB zum Alltag. Blick auf eine solche Anlage bei der Eröffnung der CeBIT.

3.4 Materielle Sicherungstechnik

Bei der materiellen Sicherungstechnik geht es um Maßnahmen technischer, baulicher und organisatorischer Art, die dem Schutz von Informationen dienen, die im öffentlichen Interesse geheim zu halten und vor dem Zugriff Unbefugter zu bewahren sind.

Informationen, die geheim zu halten sind (Verschlusssachen – VS), fallen bei vielen öffentlichen Verwaltungen an. Deshalb ist bei den VS-verwaltenden Dienststellen des Bundes und der Länder ein einheitliches Sicherheitsniveau zu wahren. Das BSI unterstützt sie sowohl durch Beratung als auch durch technische Dienstleistungen.

Technische Sicherheitsmaßnahmen umfassen mechanische und elektrische oder elektronische Sicherungs- und Überwachungseinrichtungen. Dazu zählen zum Beispiel einbruchhemmende Türen und Fenster mit ihren Schließeinrichtungen ebenso wie Einbruchmeldeanlagen, Stahlschränke und Aktensicherungsräume. Auch Geräte zum zuverlässigen Vernichten von Akten beziehungsweise Löschen von Datenträgern gehören dazu.

Für den Anwender ist es kaum möglich, die Sicherheitseigenschaften dieser Produkte alle selbst zu bewerten. Um zu garantieren, dass sie auch die ihnen zugedachte Schutzfunktion erfüllen, erarbeitet das BSI technische Richtlinien und Prüfbedingungen. Damit stehen objektive Kriterien bereit, auf deren Grundlage Sicherungsanlagen geprüft und auf den neuesten Stand gebracht werden können. Die Prüfkriterien stützen sich bei einer Reihe von Sicherungseinrichtungen auf nationale oder europäische Normen und Standards, an deren Erstellung das BSI mitgearbeitet hat. Für solche Produkte, für die keine geeigneten öffentlichen Regelwerke existieren, erarbeitet das BSI eigene Kriterien.

Materialprüfung an einer Stahltür mit dem Schweißgerät. Technische Richtlinien definieren die Sicherheitseigenschaften, die eine Schließanlage aufweisen muss.

Die Anforderungen müssen so allgemein formuliert sein, dass sie für Anlagen der unterschiedlichsten Bauart anwendbar sind. Und sie müssen die speziellen Angriffsverfahren eines nachrichtendienstlichen Gegners berücksichtigen. Erfahrung, Geschicklichkeit und Fantasie sind deswegen bei einer solchen Sicherheitsprüfung unerlässlich. Gelegentlich ist es schon vorgekommen, dass zur allgemeinen Überraschung ein neuartiges High-Tech-Produkt mit einfachsten Mitteln, an die der Entwickler selbst nicht gedacht hat, „geknackt“ werden konnte.

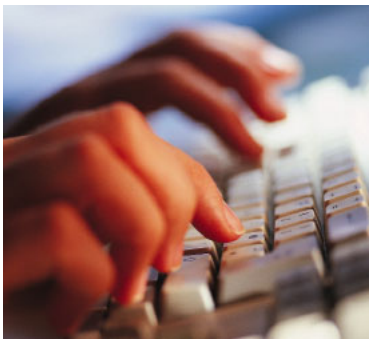
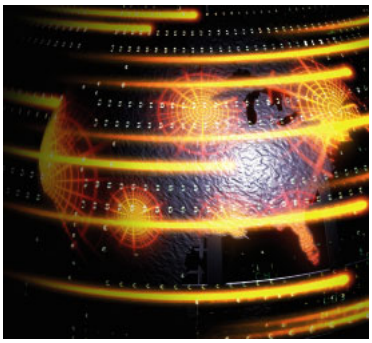
Technische Anforderungen des BSI liegen derzeit vor für:

- VS-Verwahrgelasse zur Aufbewahrung von Verschlusssachen,
- Schlösser und Schließsysteme,
- Einbruchmeldeanlagen und deren Komponenten,
- Zutrittskontrollanlagen,
- sonstige Sicherungseinrichtungen wie zum Beispiel Zäune.

Für Firmen und Anwender sind Produkte auf der Basis von allgemein verbindlichen Normen und Standards vorteilhaft, weil sie in der Regel für einen breiten Benutzerkreis bestimmt und deshalb häufig kostengünstiger herzustellen sind. Geprüfte und für den Geheimschutz geeignete Produkte sind in einer BSI-Druckschrift (BSI 7500) veröffentlicht. Dem Anwender von Sicherungseinrichtungen wird damit ein Mittel an die Hand gegeben, das ihm hilft, zuverlässig die Anlagen auszuwählen, die für seinen Bedarf geeignet sind.

Bei komplexen Sicherungssystemen wie etwa einer Einbruchmelde- oder einer Zutrittskontrollanlage bietet die Prüfung von Einzelkomponenten allein keine ausreichende Sicherheit. Hier wirkt das BSI schon in der Planungs- und Projektierungsphase mit. Bei der Abnahmeprüfung wird besonders darauf geachtet, dass die geeigneten Produkte verwendet wurden und die Sicherungseinrichtungen im jeweiligen Gesamtsystem in der beabsichtigten Weise zusammenwirken.

Bruchsichere Glasfassade (links) und ein geschützter Eingangsbereich.


4 Prävention: Gerüstet für den Notfall

Nur die modernsten Methoden sind geeignet, Schäden in IT-Systemen vorzubeugen. Staat, Wirtschaft und Gesellschaft können sich auf die Dienstleistungen des BSI auch verlassen, wenn es um Prävention geht.

„Würmer" bekämpft CERT-Bund erfolgreich durch gezielte Warnungen und Informationen, ob sie nun Sober, Mydoom oder Sasser heißen. Warnhinweise gehören zur Routine, und jedes Mal sind damit auch Tipps verbunden, welche Schutzprogramme sich die Nutzer herunterladen, und wie sie den Virus ausschalten können.

Der Schutz Kritischer Infrastrukturen gehört zu den wichtigsten Anliegen des BSI, ob es sich um Behörden, Energienetze oder Finanzdienstleistungen handelt. Der Staat allein kann die nationalen Infrastrukturen nicht schützen, denn der größte Teil dieser Einrichtungen liegt in der Hand der Wirtschaft. Eine enge Kooperation zwischen Staat und privatem Sektor ist daher unbedingt notwendig. Eines der wichtigsten Anliegen des BSI ist die Schärfung des Bewusstseins für die Notwendigkeit des Schutzes Kritischer Infrastrukturen und die aktive Risikovorsorge.

Wenn es sein muss, werden BSI-Experten sogar zu „Hackern". Auf Anfrage unternehmen sie den kontrollierten Versuch, von außen in ein Computernetzwerk einzudringen, um seine Schwachstellen aufzudecken. Das Penetrationszentrum des BSI bietet solche Tests an.

4.1 CERT-Bund – Teams für den Notfall

Computer-Notfallteams, sogenannte CERTs (Computer Emergency Response Teams), warnen und alarmieren bei Bedrohungslagen. Sie sind auf Informationsaustausch und eine gute internationale Zusammenarbeit angewiesen.

Informationen sind der Schlüssel für die Qualität jeder CERT-Dienstleistung. Nur in seltenen Fällen liegen alle Informationen aber originär bei einem einzelnen CERT vor. „Netzwerke“ haben deswegen eine überragende Bedeutung. Die beste Vernetzung nützt allerdings nichts, wenn aus dem Wissen keine Aktionen abgeleitet werden, wenn also Entscheider, Techniker und IT-Verantwortliche, die gewarnt und mit vorsorglichen Sicherheitsmaßnahmen bedient wurden, zögern oder gar nicht reagieren.

International kommunizieren – lokal handeln

Das Notfall-Team des Bundes ist in verschiedene internationale und nationale Netzwerke aktiv eingebunden, sei es in den internationalen Dachverband FIRST (Forum of Incident Response and Security Teams – www.first.org), in die europäische CERT-Gemeinschaft (TF-CSIRT) oder in die Gemeinschaft der europäischen Behörden-Notfallteams (European Government CERTs Group, EGC). Beim Aufbau des nationalen Verbundes war CERT-Bund zusammen mit dem DFN-CERT (DFN = Deutsches Forschungs-Netz) federführend. Damit verfügt das Notfallteam CERT-Bund über hervorragende Informationsbeziehungen im globalen „Web of trust“. Die beiden Strategien lauten:

- Prävention – tätig werden, bevor etwas passiert.
- Reaktion – tätig werden, wenn etwas passiert ist.

Kein Angriff, der nicht eine Sicherheitslücke auszunutzen versucht; kein Vorfall, ohne dass eine Sicherheitslücke tatsächlich existiert hat. Warnungen und Informationen sind unverzichtbare präventive Dienstleistungen. Sie betreffen nicht nur technische Aspekte, sondern auch die von den CERTs durch ihren Informationsaustausch gewonnenen Bewertungen: Wie gefährlich ist die neue Sicherheitslücke wirklich? Welches Risiko kommt da auf uns zu? Gesicherte Informationen dazu sind für die betreute Zielgruppe von entscheidender Bedeutung. In der heutigen Situation zwingt die Gefahr von gefährlichen Angriffen zu unmittelbarem Reagieren. Neu bekannt gewordene Sicherheitslücken können weltweit neuen Viren, Würmern oder trojanischen Pferden Zugang zu Systemen und Netzen verschaffen. Die Zusammenhänge zwischen Sicherheitslücken und Schadprogrammen können nur durch internationale Zusammenarbeit aufgedeckt werden.

Zielgruppengenaue Warnungen

Aber es reicht nicht aus, Informationen nur aufzubereiten oder zu bewerten. Sie müssen vom jeweiligen CERT für „seine“ Zielgruppe verifiziert, analysiert und bewertet werden. Dabei kann das Team Probleme mit den Informationen, zum Beispiel Unvollständigkeit oder Interpretationsmöglichkeiten, erkennen und beseitigen. Außerdem kann durch eine Konkretisierung der Bedrohungslage – wer ist wirklich betroffen? – vermieden werden, dass bei den Empfängern ein unnötiger Aufwand getrieben wird.

Die genaue Eingrenzung des Risikos ist häufig das Ergebnis weiterer Analysen und praktischer Tests. Hier kommen die nationalen und internationalen Netzwerke wieder ins Spiel, denn nur wenige CERTs verfügen über die notwendigen fachlichen und personellen Ressourcen, um jedes technische Detail ad hoc selbst zu überprüfen. Und jeder Vorfall, der verhindert werden kann, ist ein Gewinn für die CERT-Gemeinschaft, denn immer noch sind es die vielen nicht entdeckten kompromittierten Systeme, von denen eine ständige Bedrohung ausgeht.

Erfahrene Angreifer gehen in den seltensten Fällen direkt vor. Sie versuchen mit vielfältigen Mitteln ihre eigene Identität zu verschleiern und die Spuren zu verwischen. Die Angriffe folgen der Strategie: erst ein IT-System als „Opfer“ übernehmen und dann dieses übernommene IT-System als „Täter“ in den Angriff einbeziehen. Die Aufklärung dieser vernetzten Vorfälle ist aufwendig, CERTs sind bei der Analyse und Bewertung als fachliche Instanzen beteiligt.

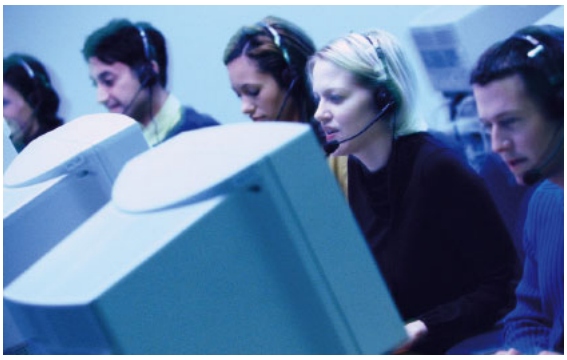
Wenn Viren die Sicherheit im Luftverkehr gefährden: Die Rechner bei der Deutschen Flugsicherung (DFS), einem Bundesunternehmen, müssen einwandfrei funktionieren.

Technik, Fachkompetenz und Erfahrung

Angriffe auf IT-Systeme ignorieren sowohl Unternehmens- als auch nationale Grenzen. Deswegen werden gewonnene Informationen so bald wie möglich dem internationalen CERT-Netzwerk zur Verfügung gestellt. Die Erkenntnisse fließen wiederum in die eigene Arbeit ein. Technische und organisatorische Schnittstellen ermöglichen den Informationsfluss zwischen den einzelnen CERTs. Gegenwärtig wird daran gearbeitet, ihn zu beschleunigen und die Arbeit damit noch effektiver zu machen.

CERT-Bund ist insbesondere bei der Förderung der deutschen CERTs aktiv, indem Projekte und Produkte entwickelt werden, die den anderen direkt oder indirekt zur Verfügung gestellt werden. CERT-Bund arbeitet jedoch nicht alleine in diese Richtung. Andere Mitglieder des Verbunds engagieren sich in ähnlicher Weise. Sie sind in verschiedenen Arbeitsgruppen organisiert, zum Beispiel zum Thema Frühwarnung oder Lagebild.

Nationale und internationale Zusammenarbeit ist ohne die effiziente Kombination aus Technik, Fachkompetenz und Erfahrung, getragen durch ein gemeinsames Verständnis, das Vertrauen ermöglicht, aber auch Kontrolle zulässt, nicht denkbar. Gemeinsam lässt sich besser und umfassender präventiv wirken. Und je früher neue Gefahren und Angriffsmöglichkeiten erkannt werden, desto schneller lassen sich geeignete Gegenmaßnahmen ergreifen.



IT-Systeme müssen weltweit und rund um die Uhr einsetzbar sein, wie zum Beispiel im Call-Center.

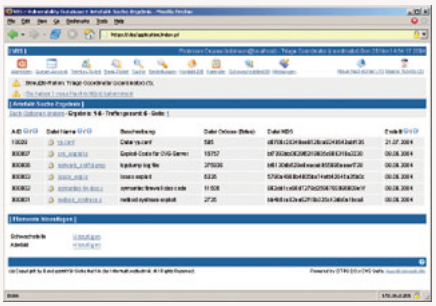
IT-gestützte Bearbeitungssysteme für sicherheitskritische Vorfälle

Das **VorfallBearbeitungsSystem (VBS)** ist ein Programm, das
- die strukturierte Ablage von Sicherheitsvorfällen steuert,
- die Basis für eine gemeinsame Dokumentation und Statistik bietet,
- eine Datenbank für Schwachstellen und Schadprogramme enthält sowie
- den Austausch von Informationen und Vorfallsdaten unterstützt.

Das **CERT-Bund AlarmierungsSystem (CBAS)**
- kann in kritischen Situationen auch außerhalb der Regelarbeitszeit die technische Administration und Entscheidungsebenen alarmieren,
- ist rund um die Uhr einsatzbereit,
- verfügt über flexible Alarmierungsketten mit Quittierungsfunktion und
- kann mit einem Knopfdruck ausgelöst werden.

Der **Warn- und Informationsdienst (WID)** bietet
- Informationen zu Schwachstellen und Sicherheitslücken,
- Empfehlungen von Sicherheitsmaßnahmen,
- ein umfangreiches Web-Archiv mit Suchfunktionen,
- webbasierte individuell angepasste Informationsangebote sowie
- den Versand von Warnungen über E-Mail.

So sehen die Computerschirme aus, wenn CERT-Bund aktiv wird:



Links: CERT-Bund meldet eine Schwachstelle (begrenzter Nutzerkreis).
Mitte: Das Vorfallbearbeitungssystem (VBS) mit Datenbankanbindung.
Rechts: Die Startseite des WID (Warn- und Informationsdienst).

4.2 Schutz Kritischer Infrastrukturen

Entscheidungsebenen in Staat, Wirtschaft und Gesellschaft, die im Bereich Kritischer Infrastrukturen (KRITIS) angesiedelt sind, brauchen die Unterstützung des BSI.

Nur so können sie ihren Aufgaben im vollen Umfang nachkommen, ohne befürchten zu müssen, dass sie sich durch den Einsatz von Informationstechnik selbst gefährden. Kritische Infrastrukturen – so lautet die offizielle Definition – sind „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten können".

Dazu gehören die Sektoren:
1. Transport und Verkehr
2. Energie
3. Gefahrenstoffe
4. Informationstechnik und Telekommunikation
5. Finanz-, Geld- und Versicherungswesen
6. Versorgung
7. Behörden, Verwaltung und Justiz
8. Sonstiges (wie Medien, Großforschungseinrichtungen, Kulturgüter)

Intensiv untersucht das BSI in diesen Bereichen Bedrohungen und Schwachstellen. Zu seinen Aufgaben gehört auch die Entwicklung von Konzepten zur Minimierung der Folgen möglicher Vorfälle.

Doch der Schutz Kritischer Infrastrukturen umfasst weit mehr als die Sicherheit der Informationstechnik. Es gilt, alle Aspekte des Infrastrukturschutzes in integrativen Sicherheitslösungen zu vereinen. So spielen auch der physische Schutz oder Organisationsfragen eine wichtige Rolle.

Aufgabe der ressortübergreifenden Projektgruppe (PG) KRITIS im Bundesministerium des Innern (BMI) ist die Erarbeitung solcher Lösungen. In dieser Projektgruppe sind neben BMI und BSI unter anderem auch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundeskriminalamt (BKA) und das Technische Hilfswerk (THW) vertreten.

Enge Kooperation zwischen Staat und privatem Sektor

Der Schutz Kritischer Infrastrukturen ist aber nicht allein Sache des Staates, zumal die Sektoren, die betroffen sind, zum überwiegenden Teil in der Hand der Wirtschaft liegen. Eine enge Kooperation zwischen Staat und privatem Sektor ist daher unbedingt notwendig. Das BSI hält eine Reihe enger Kontakte zu KRITIS-Betreibern, diese Kooperationen werden weiter ausgebaut und intensiviert.

Um die Probleme und den Bedarf der Wirtschaft möglichst genau zu erfassen, hat das BSI die „Wissensbasis KRITIS“ entwickelt und eine „Vorfalls-Datenbank“ eingerichtet. In dieser Datenbank werden öffentlich zugängliche Berichte über weltweite Vorfälle in Kritischen Infrastrukturen gesammelt und analysiert.

Eines der großen Anliegen des BSI besteht darin, in der deutschen Öffentlichkeit ein Bewusstsein für die Notwendigkeit des Schutzes Kritischer Infrastrukturen zu schaffen und wach zu halten. Und zwar auf allen Ebenen: Staat, Wirtschaft und Gesellschaft. BSI-Mitarbeiter halten Vorträge zu dem Thema bei Branchenverbänden oder in Bildungseinrichtungen. Die KRITIS-Webseiten des BSI bieten umfangreiche Informationen zum Schutz kritischer IT-Infrastrukturen in Deutschland, aber auch weltweit.

Die weltweite Vernetzung bringt es mit sich, dass der Schutz Kritischer Infrastrukturen nicht an den Landesgrenzen aufhört. Das BSI unterhält deshalb enge Kontakte zu anderen Staaten. Die USA, Schweiz, Schweden und Finnland etwa sind Länder, mit denen auf Expertenebene kooperiert wird. Ferner organisiert das BSI im nationalen wie im internationalen Rahmen fachspezifische Konferenzen sowie Workshops und ist in internationalen Fachgruppen und Gremien wie EU, G8 und NATO vertreten.

Kritische Infrastrukturen: Kernkraftwerke oder Banken sind Beispiele für Einrichtungen mit enormer Bedeutung für das Gemeinwesen. Bei ihrem Ausfall oder ihrer Beeinträchtigung können dramatische Folgen eintreten.

4.3 Hacken für die Sicherheit: der „Penetrationstest“

Im technischen Sprachgebrauch versteht man unter einem Penetrationstest den kontrollierten Versuch, von außen in ein bestimmtes Computersystem oder -netzwerk einzudringen, um Schwachstellen zu identifizieren.

Dazu werden die gleichen oder ähnliche Techniken eingesetzt, die auch bei einem realen Angriff verwendet werden. So können die dabei identifizierten Schwachstellen behoben werden, bevor unautorisierte Dritte ins IT-System eindringen und Schaden anrichten. Penetrationstests erlauben darüber hinaus, Sicherheitsschwachstellen in Netzwerken festzustellen und einzugrenzen. Auch das BSI bietet diese Tests für seine Kunden, etwa aus der Bundesverwaltung, an.

Penetrationstests sind Vertrauenssache. Wer auf verschiedene Arten versucht, über Sicherheitslücken an Zugriffsrechte zu gelangen, mit deren Hilfe Daten verändert oder entwendet werden könnten, muss für seine Kunden – besonders wenn es sich um Regierungsstellen oder Behörden handelt – absolut verlässlich sein.

Kommunikationsnetze gehören in Behörden und Unternehmen heute zum Alltag. So werden IT-Komponenten eingesetzt, um Geschäftsbeziehungen aufrecht zu erhalten oder um die Kommunikation mit den Bürgern effizienter und kundenfreundlicher zu gestalten. Dienstleistungen werden über IT-Anwendungen extern angeboten, früher geschlossene Systeme nach außen geöffnet. Die Sicherheit der eingesetzten IT wird so zunehmend für den Erfolg eines Unternehmens oder einer Behörde zu einer kritischen Größe.

Um trotz der verschiedenen Problemstellungen von den Vorteilen der IT profitieren zu können, werden Testmethoden benötigt, die sich aus dem Blickwinkel eines potenziellen Angreifers mit der Sicherheit der vorhandenen beziehungsweise geplanten IT-Anwendungen auseinandersetzen. Das ist der Sinn eines Penetrationstests. Einen besonderen Schwerpunkt nehmen für das BSI gegenwärtig Tests der Webauftritte von Behörden ein, da an sie besonders hohe Maßstäbe gelegt werden.

Die Erfahrungen aus vergangenen Sicherheitsüberprüfungen zeigen, dass Webauftritte insgesamt gesehen sehr typische Schwachstellen aufweisen können, wie zum Beispiel die fehlende Validierung von Benutzereingaben. Der Bürger, der auf den Webserver einer Behörde zugreift, erwartet Rechtssicherheit, Verbindlichkeit und absolute Vertraulichkeit. Er muss sich sicher sein können, dass seine von ihm eingegebenen persönlichen Daten durch keine noch so geschickte Manipulation ausspioniert oder sogar geändert werden können.

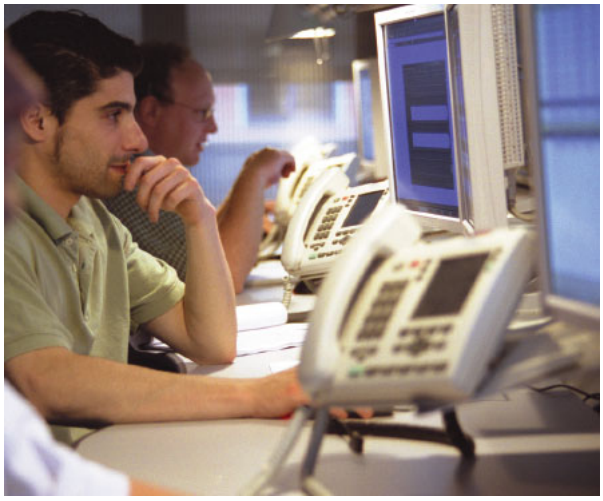
Neben den Bürgern könnten auch die Behörden selbst direkt von der fehlenden Überprüfung der Eingabewerte betroffen sein. Durch die zunehmende Anbindung von Webservern an interne Datenbanken können entsprechende Fehler in den Webapplikationen direkten Zugriff auf diese internen Datenbanken ermöglichen. Hat die Webapplikation Schreibrechte auf die Datenbank, wäre sogar eine Änderung interner Daten denkbar.

Um im Vorfeld mögliche Schwachstellen identifizieren und abstellen zu können, hat das BSI den „BSI Quick Check“ entwickelt. Er bietet eine entsprechend angepasste Prüftiefe und kann wegen seiner leichten Anwendbarkeit schneller eine größere Breitenwirkung als umfassende Penetrationstests erreichen.

Die Vorgehensweise orientiert sich an der BSI-Studie „Durchführungskonzept für Penetrationstests“. Ihre Vorgaben sind so flexibel, dass sie auch für den Test von Webapplikationen anwendbar sind. Für den „Quick Check“ einer Webanwendung wird die Vorgehensweise erheblich verkürzt. Eine einzelne Überprüfung sollte nicht länger als einen Arbeitstag dauern.

Außerdem orientiert sich die Vorgehensweise an den Vorgaben des „Open Web Application Security Project“ dessen Leitfaden „A Guide to Building Secure Web Applications“ beschreibt, was bei der Entwicklung sicherer Webanwendungen beachtet werden sollte.

Sicherheitsexperten führender Anbieter von IT-Sicherheitslösungen checken Netzwerke rund um die Uhr.



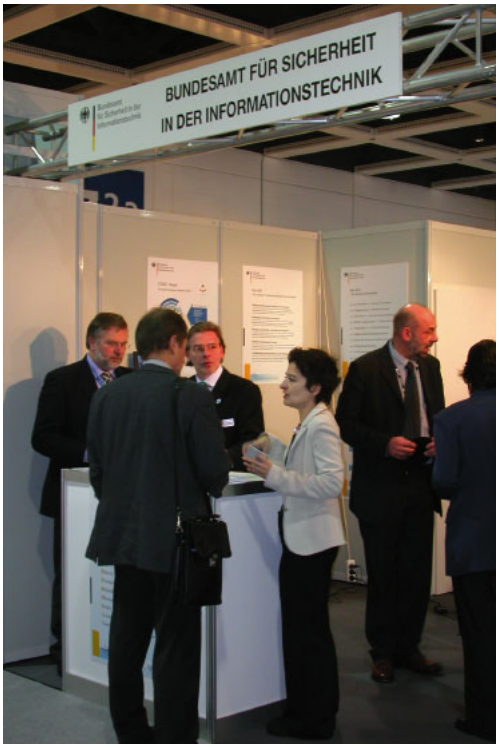
Blick ins Innere eines Rechenzentrums: Der „BSI Quick Check“ liefert Informationen über die Sicherheit von Webservern und -anwendungen.

Wie funktioniert der „BSI Quick Check“?

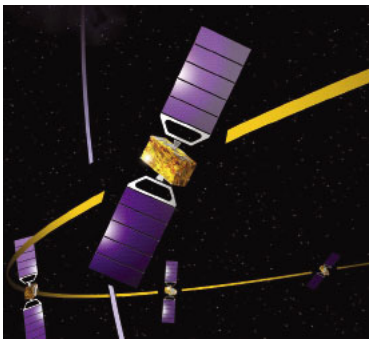
In der ersten Phase des „BSI Quick Check“ werden Informationen über die eingesetzten Webserver und zu testenden Webanwendungen gesammelt. Insbesondere ist es das Ziel dieser Phase, automatisiert die vom Webserver nach außen angebotenen Dienste zu finden und zu dokumentieren. Im Anschluss wird das zu testende System einer ganzen Reihe teilweise automatisierter Tests unterzogen. Diese Prüfungen beziehen sich einerseits auf das Betriebssystem und zum anderen auf die Anwendungen des Webservers. Die im „Quick Check“ vorgesehenen Tests sind nicht mit Risiken für das System verbunden. Destruktive Tests wie zum Beispiel „Denial of Service“-Attacken sind nicht Bestandteil des „BSI Quick Check“, sie sind ausdrücklich ausgenommen.

Ausgewählte Fehlerquellen werden durch die Mitarbeiter des BSI manuell und stichprobenartig nachgeprüft. Basierend auf einer Liste der häufigsten Schwachstellen in Webanwendungen werden beispielsweise die Eingabefelder mit fehlerhaften beziehungsweise ungültigen Daten ausgefüllt und das Antwortverhalten des Webservers analysiert. Derzeit weit verbreitete Störungsquellen, wie „Cross Site Scripting“ und „SQL Injection“, werden in die manuellen Tests mit einbezogen. Diese Testliste wird regelmäßig durch das BSI aktualisiert und orientiert sich an den im Internet bekannten und verbreiteten Angriffstechniken.

Abschließend werden die Ergebnisse des „BSI Quick Check“ zusammengefasst und schriftlich dem jeweiligen Anwender beziehungsweise Verantwortlichen zugesandt. Wegen der angestrebten zeitlichen Straffung des „Quick Check“ werden keine spezifischen Empfehlungen zur Beseitigung der aufgefundenen Fehler gegeben. Die Expertise kann daher nur verkürzt sein. Aber im Anschluss an den „Quick Check“ lässt sich natürlich eine ausführliche Beratung durch das BSI vereinbaren.



Auf der Messe „Moderner Staat“ vom 23. bis 24. November 2004 in Berlin erläutern BSI-Experten interessierten Behördenvertretern, wie sie den „BSI Quick Check“ anwenden können.



5 Technologie der Zukunft: Neue Herausforderungen

Technisch machbar ist vieles, aber ob die Datenerfassungs- und Übertragungssysteme der Zukunft auch sicher sind, das ist eine andere Frage. Das BSI prüft nach.

Biometrische Personenidentifikation, Funkchips an Waren, Geldscheinen oder Fahrzeugen, satellitengestützte Navigationssysteme für den europäischen Bedarf – das sind drei wichtige Zukunftstechnologien, die unseren Alltag künftig bestimmen.

Mit der umfangreichen Feldstudie „BioP“ legt das BSI seine Forschungen auf dem Gebiet der biometrischen Verfahren zur Gesichts-, Finger- und Iriserkennung vor. Dabei geht es vor allem um die Erprobung und Festlegung internationaler Standards.

RFID-Chips, also Identifikations- und Datenerfassungssysteme mit kontaktloser Datenübermittlung auf Basis der Radiofrequenztechnologie, werden unter anderem bereits bei Zutrittsystemen, zur Tieridentifikation und im Warenmanagement eingesetzt. Dabei hat sich gezeigt, dass Unternehmen, die ihre Kunden nicht aufklären, schnell in den Fokus von Datenschutz- und Bürgerrechtsorganisationen geraten.

Ohne hochleistungsfähige Kryptosysteme sind Satellitenortungs- und -navigationssysteme nicht zu steuern. Das BSI hat sich mit seinem herausragenden Expertenwissen auf diesem Gebiet erfolgreich in übergeordnete zivile und militärische Großprojekte integrieren können.

5.1 Biometrie und Innere Sicherheit

IT-Sicherheit steht bei biometrischen Verfahren, mit denen sich das BSI beschäftigt, im Vordergrund. Biometrie ist die maschinelle Erkennung des Menschen anhand einzigartiger Unterscheidungsmerkmale wie Iris, Fingerabdruck und Gesicht.

Den Schwerpunkt der Arbeit von Experten des BSI bei der Analyse von biometrischen Systemen bilden folgende Themenkomplexe:

- Was leisten die marktverfügbaren biometrischen Produkte bei der Erkennung biometrischer Merkmale?
- Wie sicher sind biometrische Systeme gegen Versuche, sie zu täuschen oder zu überwinden?
- Wie können biometrische Verfahren in elektronischen Ausweisen und Dokumenten berücksichtigt werden?

Im Jahre 2004 hat das BSI eine Vielzahl von Feldstudien und Labortests durchgeführt. Untersucht wurden unter anderem Gesichts-, Finger- und Iriserkennung. Die umfangreiche Feldstudie „BioP“ am Flughafen Frankfurt wurde Ende des Jahres 2004 abgeschlossen.

Eine wesentliche Rolle spielt bei allen Aktivitäten auf diesem Gebiet die Anpassung der biometrischen Produkte an die internationalen Anforderungen, etwa der Internationalen Zivilluftfahrt-Organisation (ICAO, mit Sitz in Montreal), einer Unterorganisation der UNO. Dabei geht es um biometrische Verfahren auf maschinenlesbaren Reisedokumenten.

Die Arbeit des BSI trägt zur Weiterentwicklung zwischenstaatlicher Standards entscheidend bei. Die internationale Zusammenarbeit bewährt sich auf Regierungsebene auch in gemeinsamen Projekten mit europäischen, US-amerikanischen und weiteren Partnern. Auch dabei geht es unter anderem um die Interoperabilität von Reisedokumenten. Die dabei gewonnenen Erkenntnisse dienen dazu, die für die jeweilige Anforderung am besten geeigneten Verfahren zu finden und in technische Standards zu integrieren.

Otto Schily, Bundesminister des Innern, präsentiert den digital lesbaren Pass. Er wird biometrische Daten auf einem Chip enthalten.

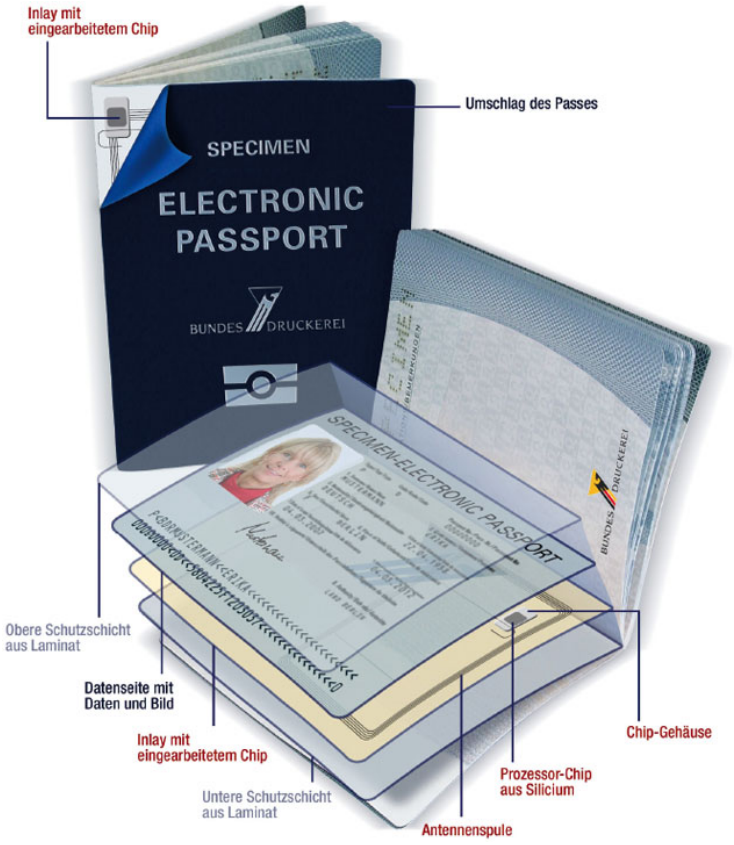
Standards für Biometrieverfahren gesucht

Die International Organization for Standardization (ISO) in Genf hat 2004 ein Joint Technical Commitee (Abkürzung: JTC1/SC37) für die anwendungsbezogene interoperable Standardisierung biometrischer Verfahren eingerichtet. Entsprechende nationale Gremien folgten. In beiden Bereichen arbeitet das BSI aktiv mit und gibt wichtige Impulse im Sinne der IT-sicherheitstechnischen Umsetzung biometrischer Systeme. Gleichwohl sind im Bereich Standardisierung der Templates für biometrische Merkmale noch nicht alle Herausforderungen endgültig gelöst.

Erprobt werden derzeit die unterschiedlichsten Biometrieverfahren. Sie sind fast so vielfältig wie die Anforderungen, die an sie gestellt werden. Individuell angepasste Anwendungskonzepte für den Bedarf der Nutzer gewährleisten einen optimierten und praxisorientierten Einsatz. Unter dieser Voraussetzung können wir diese Technologie gewinnbringend einsetzen.

Die erheblichen technischen Verbesserungen der marktverfügbaren biometrischen Produkte in den letzten Jahren, auch als Folge der Grundlagenarbeiten und Erprobungen durch das BSI, ermöglichen bereits heute eine erfolgreiche Anwendung für ausgewählte Anwendungsbereiche. Dazu tragen auch erste produktspezifische IT-sicherheitstechnische Bewertungen im Rahmen der Zertifizierung oder die Erstellung sogenannter Sicherheitsanwendungsprofile (Protection Profiles) bei. So wird unter anderem festgelegt, welche Sicherheitsstandards bei der zukünftigen Anwendung biometrischer Verfahren gelten. Damit werden auch die IT-Sicherheitsaspekte beim Einsatz der Biometrie hinreichend berücksichtigt.

Das BSI wird in den kommenden Jahren die Einführung biometrischer Verfahren speziell im Umfeld der Ausweisdokumente aktiv begleiten.



Die Abbildung zeigt den Aufbau eines maschinenlesbaren Ausweisdokumentes mit Chip und Antenne.

5.2 Radio Frequency Identification (RFID)

Die zunehmende Verbreitung der Radio Frequency Identification-Technologie (RFID-Technologie) findet weitestgehend unsichtbar statt. Allenfalls in Warensicherungsettiketten werden die einfachsten Formen dieser leistungsfähigen Technik vom Verbraucher wahrgenommen.

Bei der RFID-Technik kommen 1-bit-Transponder zum Einsatz, die unter Ausnutzung physikalischer Effekte ausschließlich eine Ja/Nein-Information speichern und nicht explizit beschreibbar beziehungsweise programmierbar sind. Darüber hinaus existiert eine Vielzahl weiterer Produkte. Diese besitzen oft deutlich mehr Funktionalitäten als einfache Artikelsicherungssysteme. Es handelt sich um leistungsfähige Identifikations- und Datenerfassungssysteme mit kontaktloser Datenübermittlung auf Basis der Radiofrequenztechnologie.

Anwendung findet diese Technik zur Zeit hauptsächlich in den Bereichen
- Industrieautomation,
- Zutrittssysteme,
- Tieridentifikation,
- Warenmanagement und
- Diebstahlschutz (zum Beispiel KFZ-Wegfahrsperren).

Ein RFID-System besteht dabei immer aus einem Transponder, der die zu speichernden und bei Bedarf zu übermittelnden Informationen enthält und einem Schreib-/Lesegerät.

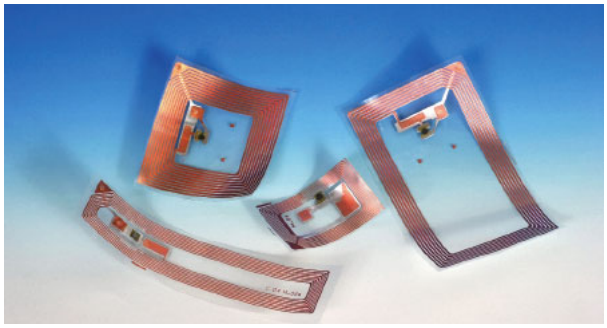
Schnittstellen-Technik

Bei Betrachtung der technischen Möglichkeiten moderner RFID-Technologie sowie der damit einhergehenden Gefährdungen wird klar, dass diese Technologie Schnittstellen zu den verschiedensten Ebenen der IT-Sicherheit und der Gesellschaft besitzt.

Bereits heute sind RF-Tags bei Zutrittskontrollanlagen kombiniert mit einem Firmenausweis im Einsatz, die Europäische Zentralbank plant die Verwendung von kleinsten RFIDs für Banknoten zur Erhöhung der Fälschungssicherheit. Verkehrsgesellschaften möchten die Fahrausweise ihrer Kunden mit Transpondern versehen, die einem zentralen Abrechnungssystem mitteilen, wie welche Verkehrsverbindungen genutzt werden.

Das Verhindern von Geldfälschung oder eine bequeme Abrechnung der ÖPNV-Nutzung sind sinnvolle Anwendungsgebiete von RF-Chips. Im Interesse des Bürgers steigt hier durch die RFID-Technik die Sicherheit und die Kundenfreundlichkeit. Bedenken gegen die unscheinbaren Sender bestehen trotz oder gerade wegen ihrer Unsichtbarkeit: Die immer noch aktuelle Diskussion um Pilotprojekte im Bereich Warenmanagement, in deren Umfeld RFIDs eingesetzt werden zeigt, dass ein Unternehmen, das seine Kunden über den RFID-Einsatz nicht rechtzeitig aufklärt, schnell in den Fokus von Datenschutz- und Bürgerrechtsorganisationen geraten kann.

Die neue Technologie bietet enorme Chancen, da RFID-Systeme in vielen Bereichen, darunter dem gesamten Logistikbereich und der Lagerbewirtschaftung, bereits heute nutzbringend eingesetzt werden. Was noch getan werden muss ist, den Technikeinsatz hinsichtlich seiner Auswirkungen in unterschiedlichsten Anwendungsfeldern zu untersuchen. Es gilt die Auswirkungen der RFID-Technologie abzuschätzen und zu bewerten sowie die sich ergebenden Chancen und Risiken zu benennen. Ziel ist dabei die Entwicklung von Handlungsempfehlungen für Politik, Industrie und Wissenschaft.



RFID-Tags: die kleinen schwarzen Punkte markieren die Chips, auf denen die Informationen gespeichert sind. In Schleifen gepackte Antennen funken sie zum Empfänger, wenn sie durch ein elektromagnetisches Feld aktiviert werden.

Studienreihe des BSI

Das BSI hat aus diesem Grund eine Studienreihe gestartet, die sich grundsätzlich mit der Allgegenwärtigkeit von Informationstechnologie im täglichen Leben beschäftigt. Im ersten Teil ist die RFID-Technologie das untersuchte Thema.

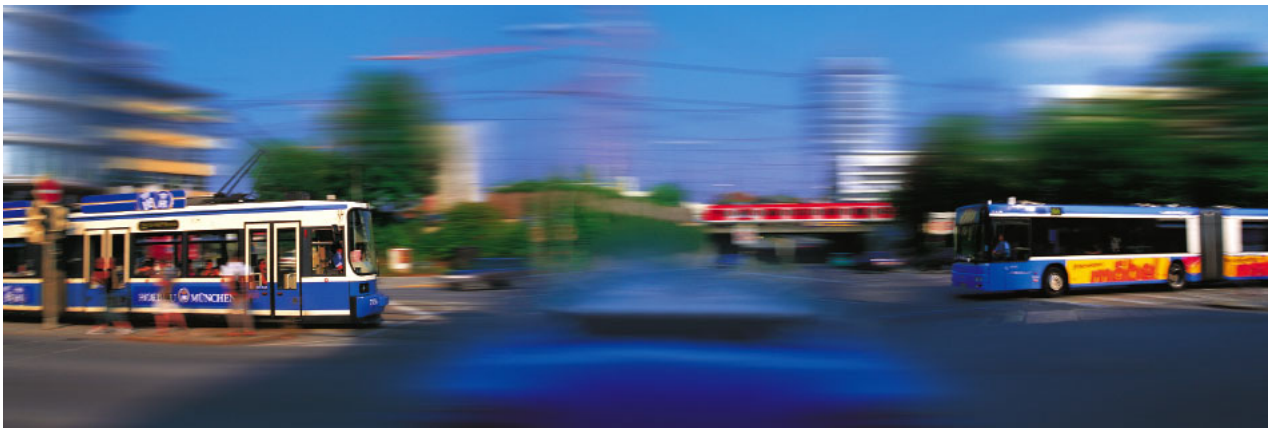
Die in der Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“ gefundenen Antworten sollen dabei einen Beitrag zur Versachlichung der Diskussion über den Einsatz der RFID-Technologie leisten und helfen, zu einem nutzbringenden und datenschutzkonformen Technikeinsatz zu gelangen.

Zu diesem Zweck geben die Arbeitsergebnisse des BSI einen Überblick über die technischen Grundlagen, die Anwendungspotenziale und insbesondere über neue Sicherheitsmaßnahmen zur Reduzierung von Risiken im Kontext von RFID-Systemen. Der Schwerpunkt der Arbeit liegt in der Analyse möglicher Bedrohungslagen, die aus der Anwendung von RFID-Systemen hervorgehen, einschließlich der Einschätzung der Wirksamkeit bestehender und zukünftiger, bereits konzipierter Sicherheitsmaßnahmen.

Im Gegensatz zu den bisher durchgeführten Betrachtungen zum Risikopotenzial wurden nicht nur gängige Bedrohungen, wie Verlust der Location Privacy betrachtet, sondern auch neue Szenarien berücksichtigt. Zu nennen sind hier experimentelle Ansätze zum Abhören der Kommunikation zwischen RFID-Tag und Lesegerät genauso wie die Auswirkungen des Einsatzes von Blocker-Tags und Störsendern. Im Bereich der Konzeption möglicher Sicherheitsmaßnahmen wird Wert auf eine große Praxisnähe gelegt. Neben wünschenswerten Maßnahmen, wie der gegenseitigen Authentifizierung bei hochwertigen Tags, wird auch das recht breite Spektrum der einfacheren RFID-Systeme betrachtet.

Aufgrund der aktuellen politischen Diskussion und der augenblicklichen Arbeitsschwerpunkte des BSI wird die Anwendung „maschinenlesbare Personaldokumente“ aufgearbeitet. Der Hintergrund: Derzeit werden weltweit verschiedene Ansätze getestet, um RFID-Transponder in Personalausweise und Reisepässe zu integrieren. Diese Transponder werden sowohl verwendet, um elektronische Fälschungsschutzmechanismen umzusetzen und damit erweiterte Echtheitsprüfungen zu ermöglichen als auch biometrische Merkmale – beispielsweise das Gesicht oder einen Fingerabdruck – im Ausweissystem (zum Beispiel Reisepass) zu speichern. Insgesamt kann festgestellt werden, dass durch die Aktivitäten der Bundesregierung innerhalb dieses Anwendungsfeldes ein sehr hohes Maß an IT-Sicherheit erreicht wurde.

Um die Chancen und Risiken von RFID-Systemen zu bewerten, wird zudem eine Einschätzung der wesentlichen technologischen, ökonomischen, rechtlichen und gesellschaftlichen Entwicklungen im Kontext von RFID-Systemen vorgenommen, die einen Zeithorizont bis etwa 2010 aufspannen.



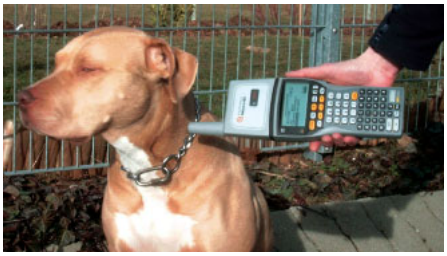
Bequem und kundenfreundlich: RFID-Chips, die künftig in Tickets für den öffentlichen Nahverkehr integriert werden sollen, machen funkgesteuert eine präzise Abrechnung der Fahrtkosten möglich.

Gibt es eine Antwort auf die Frage nach den Risiken und Chancen der RFID-Technologie?

Natürlich ist eine pauschalisierte Antwort auf eine so komplexe Frage nicht möglich. Herausgestellt hat sich jedoch, dass es zur Nutzung der Chancen von RFID-Technik notwendig ist, die Bedrohung für die Persönlichkeitssphäre so gering wie möglich zu halten. Weiterhin müssen die Grundsätze eines zeitgemäßen Datenschutzrechts in RFID-Systemen bereits frühzeitig im Design-Prozess und in der Markteinführung umgesetzt werden.

Der Fokus der BSI-Aktivitäten liegt dabei neben der Beurteilung neuer technologiespezifischer Risiken auf der Konzeption neuer Sicherheitsmaßnahmen. Dabei geht es vor allem um die Herausforderung, Sicherheitsmechanismen für ressourcenbeschränkte Systeme zu definieren und Ihre Implementierung auf Seiten der RFID-Hersteller zu begleiten. Ziel einer solchen Vorgehensweise ist das Bereitstellen von sicheren Hard- und Software-Systemen, die durch den Bürger ohne Bedenken genutzt werden können.

Die Einsatzmöglichkeiten von RFID-Chips sind sehr vielfältig. Zum Leistungsspektrum gehören beispielsweise die Identifikation von Produkten im Handel (links), von Entsorgungsgütern oder von Tieren (unten).



5.3 Galileo und SAR-Lupe – Sichere Satellitensysteme

Die Wahrung der Informationssicherheit bei Satellitensystemen beschränkt sich nicht auf die zu übertragenden Daten. Schutzbedürftig sind auch die Daten zur Überwachung (Telemetrie) und Kontrolle (Telecommand) des mechanischen Himmelskörpers.

Bei der Festlegung jeder informations- und kommunikationstechnischen Architektur für ein solches System sind alle Bereiche der IT-Sicherheit zu bedenken. Das BSI wirkt im Rahmen seines gesetzlichen Auftrags auch bei der Spezifikation von IT-Sicherheitskonzepten und -architekturen für Satellitensysteme mit. Auch bei der anschließenden Prüfung der technischen Realisierung in nationalen und internationalen Projekten ist das BSI eingebunden. So hat das BSI im Jahre 2004 seine Expertisen in die Satellitensysteme GALILEO und SAR-Lupe eingebracht.

Schema des Galileo-Satellitensystems. Nach ESA-Angaben wird Europa damit ab 2008 über ein eigenes, sicheres und geprüftes GPS verfügen.

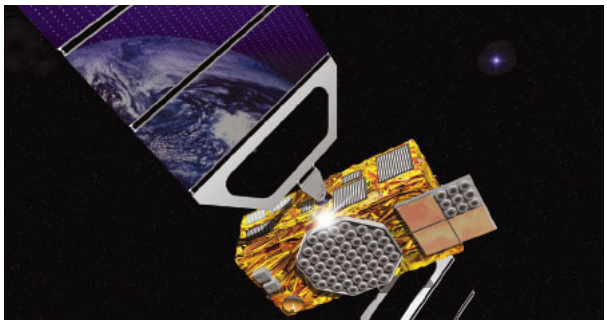
GALILEO

Das europäische satellitengestützte Navigationssystem GALILEO ist ein Gemeinschaftsprojekt der Europäischen Kommission und der europäischen Raumfahrtbehörde ESA (European Space Agency). GALILEO wird ein europäisch kontrolliertes Satellitennavigationssystem für die zivile und kommerzielle Nutzung sein – im Gegensatz zum US-amerikanischen Satellitennavigationssystem GPS (Global Positioning System), das für die militärische Nutzung konzipiert wurde. Die Mitarbeit des BSI in den Arbeitsgruppen des Projekts GALILEO mit Bezug zur Informationssicherheit hatte im Jahre 2004 folgende Themen zum Schwerpunkt:

- In der INFOSEC-Arbeitsgruppe wurden mit den europäischen Partnernationen verschiedene Alternativen für den Kryptoalgorithmus diskutiert, der im Dienst von GALILEO-PRS (Public Regulated Service) für die Nutzdatenverschlüsselung einzusetzen ist. Man einigte sich auf einen Kryptoalgorithmus, der bereits im Vorfeld gemeinsam vom BSI und von den europäischen Partnern entwickelt worden war. Weitere Themen der INFOSEC-Arbeitsgruppe waren die Erstellung einer Richtlinie für die Implementierung von Kryptoalgorithmen und die Abstimmung des Schlüsselverteilkonzepts sowie einer Evaluierungs- und Akkreditierungsstrategie.

- Die Mitarbeit im „National Experts Team“ bestand aus der Prüfung des Systemkonzepts, das von der GALILEO-Industrie während der Phase C Null (gemeint ist die Vorphase Entwicklung) erstellt wurde, und aus der Fortschreibung der Risiko- und Bedrohungsanalyse.

- Im übergeordneten Steuerungsgremium „GALILEO Security Board“ wurden die deutschen Vertreter aus dem Bundesministerium des Innern (BMI) und aus dem Bundesministerium für Verkehr, Bau- und Wohnungswesen (BMVBW) in Fragen der Informationssicherheit fachlich unterstützt.



Sonnensegel für Galileo: Informationstechnik richtet Satellitensysteme automatisch nach dem Sonnenstand aus.

SAR-Lupe

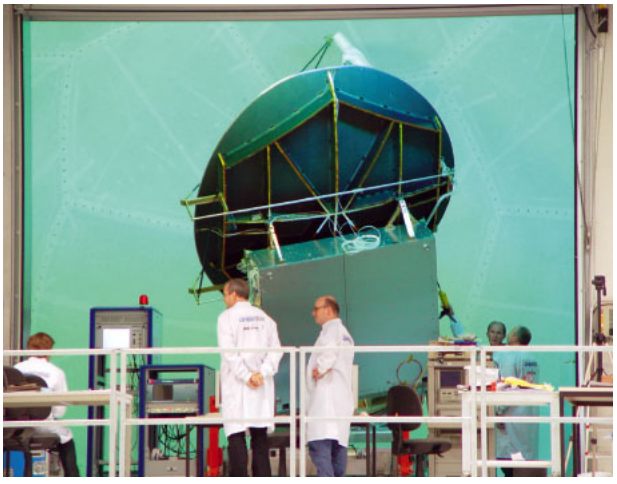
Das Satellitensystem SAR-Lupe (SAR = Synthetic Aperture Radar) ist ein hochauflösendes militärisches Radarsystem unter deutscher Kontrolle, das von der Firma OHB Technology AG im Auftrag der Bundeswehr entwickelt wird. Das BSI bringt in dieses Projekt ebenfalls seine Expertise im Bereich der Informationssicherheit ein. Der Arbeitsschwerpunkt im Jahr 2004 lag bei der Evaluierung der implementierten Kryptotechnik. Dazu wurden durch Messungen am Ingenieurmodell des Satelliten gewonnene Daten überprüft und bewertet. Als Ergebnis ist festzuhalten, dass die Evaluierung der Kryptotechnik für den Nutzdaten-Download erfolgreich abgeschlossen werden konnte. Die Evaluierung der Kryptografie für den Upload von Schlüssel-, Telemetrie- und Telecommand-Daten befindet sich derzeit kurz vor dem Abschluss.

Ein weiterer Schritt im Projekt SAR-Lupe besteht in der sogenannten Europäisierung dieses Systems. Darunter versteht man die Schaffung der Möglichkeit, SAR-Lupe auch durch europäische Partner nutzen zu lassen – unter Beachtung der nationalen Politik zum Schutz von Nutzdaten sowie von Telemetrie- und Telecommand-Daten. 2004 wurden folgende Schwerpunkte bearbeitet:

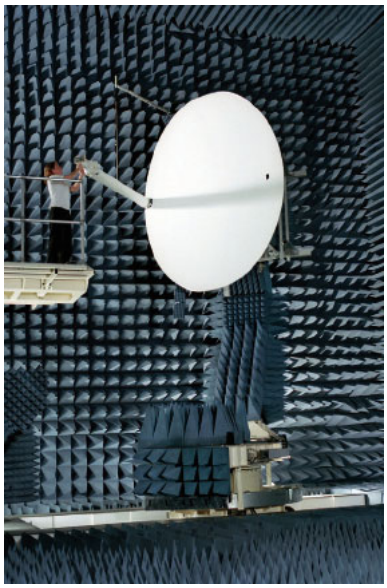
- Das Kryptokonzept Version 1.0. wurde im April nach der Abstimmung mit Nutzer und Auftragnehmer verabschiedet.

- IT-Sicherheitsspezifikationen, zum Beispiel die Systemspecific Security Requirements Specification (SSRS), wurden erstellt und im Oktober 2004 in der Version 1.0 verabschiedet. Die erforderliche Abstimmung der Dokumente mit den Partnern wird sich in der nächsten Phase anschließen.

Satellitenortungs- und -navigationssysteme benötigen hochleistungsfähige, international abgestimmte Kryptotechnik. Das BSI hat sich mit seinen Leistungen und seinem herausragenden Expertenwissen auch 2004 erfolgreich in übergeordnete zivile und militärische Großprojekte integrieren können.



Das erste satellitengestützte Aufklärungssystem Deutschlands soll 2005 mit einer russischen Rakete ins Weltall gebracht werden. SAR-Lupe wird hochauflösende Bilder aus nahezu allen Teilen der Welt liefern.



1. CD-ROM

Die vom BSI im Internet veröffentlichten Informationsangebote stehen allen Interessierten auch in Form einer kostenlosen CD-ROM zur Verfügung, gegen Einsendung eines Rückumschlags (DIN C5, Porto 1,44 Euro) beim BSI CD-Versand, Postfach 20 10 10, D-53140 Bonn

Das Infoangebot für Bürger findet sich ständig aktualisiert unter www.bsi-fuer-buerger.de. Das Webportal wird auch als CD-ROM auf Messen verteilt sowie als Heftbeilage verbreitet. Außerdem sind die Inhalte der CD-ROM auf bestimmten PCs vorinstalliert.

2. BSI-Newsletter

Möchten Sie den fünfmal jährlich erscheinenden Online-Newsletter des BSI abonnieren? Dann senden Sie eine E-Mail an newsletter@bsi.bund.de. Der E-Mail-Newsletter „SICHER•INFORMIERT“ versorgt den privaten Computernutzer alle 14 Tage mit den wichtigsten Sicherheitsnachrichten. Zur Anmeldung zum Newsletter gelangen Sie über www.bsi-fuer-buerger.de/newsletter/

3. <kes> – Die Zeitschrift für Informations-Sicherheit

Amtliche Nachrichten werden im BSI-Forum der Zeitschrift <kes> veröffentlicht.

<kes> – Die Zeitschrift für Informations-Sicherheit
(ISSN 1611-440X)
Preis je Ausgabe: 23 Euro, erscheint zweimonatlich. Internet: www.kes.info

Kontakt:
Redaktion <kes>,
Lise-Meitner-Str. 4,
D-55435
Gau-Algesheim
oder
Postfach 1234,
D-55205 Ingelheim
Tel: 06725-93 04-0,
E-Mail:
info@secumedia.de

4. Fachinformationen

Das **IT-Grundschutz-handbuch** wird als Loseblattsammlung vertrieben.
DIN A4, rund 2.000 Seiten in drei Ordnern, mit CD-ROM, Preis: 148 Euro
ISBN 3-88784-915-9
Zu bestellen beim Bundesanzeiger Verlag, Postfach 10 05 34, D-50445 Köln, Fax: 0221-97 66 82 78, E-Mail: vertrieb@bundesanzeiger.de

Leitfaden IT-Sicherheit
Stand: 2004, circa 72 Seiten
Download als PDF-Datei möglich unter www.bsi.bund.de/gshb/Leitfaden/

E-Government-Handbuch
ISBN 3-89817-180-9
BSI-Schriftenreihe zur IT-Sicherheit, Band 11, Loseblattsammlung, 1.200 Seiten, 3 Ordner, DIN A5, Preis: 98 Euro
Zu bestellen beim Bundesanzeiger Verlag, Postfach 10 05 34, D-50445 Köln, Fax: 0221-97 66 82 78, E-Mail:vertrieb@bundesanzeiger.de

„Risiken und Chancen des Einsatzes von RFID-Systemen“ – Studie, erstellt in Zusammenarbeit mit dem Institut für Zukunftsstudien und Technologiebewertung (IZT) und der Eidgenössischen Materialprüfungs- und Forschungsanstalt (EMPA). Die Studie kann zum Preis von 58 Euro über den Secumedia Verlag bezogen werden (ISBN 3-922746-56-X). Seit Dezember 2004 ist die Studie auch auf den Internetseiten des BSI veröffentlicht.

Das Faltblatt „Sicherheit in der Informationstechnik – Expertenwissen für Behörden und Wirtschaftsunternehmen“ bietet einen Überblick über alle Leistungen des BSI.
Bezug über das BSI, Postfach 20 10 10, D-53140 Bonn

Hinweise zu weiteren Veröffentlichungen des BSI finden Sie im Internet unter www.bsi.bund.de

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 I – Sicherheit in Anwendungen, Kritischen Infrastrukturen und im Internet

Dr. Gerhard Schabhüser, Leiter der Abteilung II – Sicherheit in Netzen, Kryptologie, wiss. Grundlagen der IT-Sicherheit

Bernd Kowalski, Leiter der Abteilung III – Abhörsicherheit, Zertifizierung, Zulassung, Akkreditierung

Horst Samsel, Abteilungsleiter Z – Zentrale Aufgaben

Anja Hartmann, Referatsleiterin Öffentlichkeitsarbeit
E-Mail: anja.hartmann@bsi.bund.de

Michael Dickopf, Pressesprecher
E-Mail: michael.dickopf@bsi.bund.de

Das Bürger-Portal:
www.bsi-fuer-buerger.de

Hier finden Sie unter anderem Informationen zu den Themen
- Datensicherung
- Viren und Spione
- Kinderschutz im Netz
- Einkaufen im Internet

sowie einen Downloadbereich, zum Beispiel mit
- Verschlüsselungstool
- Virenscanner
- PC-Firewall-Programm und
- Bildschirmschoner

Das Portal für IT-Profis:
www.bsi.bund.de

Fachleute und Experten finden hier Informationen unter anderem zu den Themen
- Internetsicherheit
- IT-Grundschutz
- Zertifizierung
- E-Government
- CERT-Bund
- Kritische Infrastrukturen
- Schadprogramme

sowie Hinweise auf Veranstaltungen, Schulungen und Publikationen

Herausgeber/Bezugsstelle
Bundesamt für Sicherheit in der Informationstechnik – BSI / Referat III.21
Godesberger Allee 185-189, D-53175 Bonn
Telefon: +49-(0)228-95 82-0
E-Mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de

Texte und Redaktion
Tobias Mikolasch, BSI
Thomas Presse & PR, Berlin/Bonn

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

Bildnachweis
Berufsfeuerwehr Frankfurt/Main, Pierre Boom, BSI Referat Öffentlichkeitsarbeit, Bundesbildstelle, Bundesdruckerei GmbH, Deutsche Bahn AG, Deutsche Bank AG, Deutscher Bundestag, Andreas Ernst, European Commission Audiovisual Library, European Space Agency/ESA, Fraport AG, Fujitsu Siemens Computers, Hans Georg Gaul, Infineon, Informations- und Medienzentrale der Bundeswehr, Paul Langrock/Zenit, Münchner Verkehrsverbund, OHB Technology AG, Jan Pauls, Marcus Posthumus, Presse- und Informationszentrum Marine Glücksburg, Rohde & Schwarz, Sälzer GmbH, Secunet Security Networks, Siemens Pressebild, Sony Ericsson, Symantec Corporation, Texas Instruments Inc., Warok Computer & Software GmbH, Frank Weihs

Stand
August 2005