Bundesamt
für Sicherheit in der
Informationstechnik

Jahresbericht 2003



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

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist der zentrale IT-Sicherheitsdienstleister des Bundes. Zur Förderung der IT-Sicherheit in Deutschland berät und unterstützt das Amt eine Vielzahl von Zielgruppen: IT-Hersteller und Anwender, Datenschutzbeauftragte, Sicherheitsberater, Gutachter, Prüfstellen, Forschungseinrichtungen und Normungsgremien.

Die Realisierung eigener Sicherheitsprodukte, die Trendforschung und die Mitarbeit in internationalen Organisationen sind weitere Arbeitsschwerpunkte. Als Zertifizierungs- und Zulassungsstelle entwickelt das BSI zudem Kriterien, Verfahren und Werkzeuge für die Evaluation der Sicherheit von IT-Systemen.

Auch die privaten PC-Nutzer profitieren von der Arbeit des BSI. Auf einer speziellen Website können aktuelle Informationen über mögliche Gefahren und Schutzmaßnahmen abgerufen werden. Eine Zusammenstellung der wesentlichen Inhalte auf CD-ROM wird über verschiedene Kooperationspartner millionenfach vertrieben. Gerade weil die Informationstechnik zunehmend alle Lebensbereiche erfasst, ist die IT-Sicherheit für Bürger ein wesentliches Anliegen des BSI.

Das Bundesamt für Sicherheit in der Informationstechnik stellt mit dem Jahresbericht 2003 seine Aktivitäten, Aufgaben- und Tätigkeitsschwerpunkte erstmals in gebündelter Form dar. Der Bericht bietet einen Überblick über die wesentlichen Entwicklungen des BSI in 2003.

Dienstleistungen des BSI

Information
- Aufklärung und Sensibilisierung von Bürgern
- Zukunfts- und Trendanalysen

Beratung und Unterstützung
- IT-Grundschutz, IT-Sicherheitsberatung für Behörden
- E-Government und Initiative BundOnline2005
- 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 Teams)
- Technische Koordination des IVBB (Informationsverbund Berlin-Bonn)
- Verwaltungs-PKI, Schlüsselmittelherstellung für Kryptogeräte

Gremien
- Mitarbeit in nationalen und internationalen Gremien und Standardisierungsorganen für Deutschland

Jahresbericht 2003

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

Prüfen, bewerten, forschen und schützen — der BSI-Jahresbericht

Liebe Leserinnen und Leser,

das Zeitalter der Globalisierung lebt von der Informationstechnik. Mit ihrem Potenzial hat sie die enorme wirtschaftliche und gesellschaftliche Entwicklung in den vergangenen Jahren erst möglich gemacht. Längst gehört deswegen eine zuverlässige und leistungsfähige Informationstechnik zur grundlegenden Infrastruktur moderner Industrienationen. Ihr Schutz ist eine Frage der nationalen Sicherheit.

Als Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) habe ich 2003 eine engagierte und erfolgreich agierende Behörde übernommen. Mit dem Anspruch, die bisherige Entwicklung nicht nur fortzuführen, sondern weiter auszubauen, habe ich mein neues Amt angetreten. Als zentraler IT-Dienstleister des Bundes setzen wir uns nachhaltig für eine sichere Informationstechnik in Deutschland ein. Risikovorsorge, Qualitätsprüfung und Zertifizierung von IT-Produkten sowie ein umfassender IT-Grundschutz sind die vordringlichen Aufgaben. Das BSI sorgt damit für IT-Sicherheit in unserer Gesellschaft.

Unser Bundesamt kann auf eine erfolgreiche Tätigkeit zurückblicken. Der vor Ihnen liegende Jahresbericht vermittelt einen Eindruck über unsere vielfältigen Arbeitsgebiete.

Die besondere Herausforderung besteht heute darin, viele unterschiedliche Aufgaben gleichermaßen wahrzunehmen. Die Rahmenbedingungen für unsere Arbeit sind weit gespannt: angefangen vom rasanten technischen Fortschritt über die enorme marktwirtschaftliche Bedeutung der IT-Sicherheit bis hin zum Beitrag zur Inneren Sicherheit reicht das zu bewältigende Spektrum. Unser Ziel ist es dabei, die Entwicklung der Sicherheit in der Informationsgesellschaft aktiv mitzugestalten. So wird das BSI mit der öffentlichen Verwaltung und

der Wirtschaft auch in Zukunft maßgeblich in Fragen der IT-Sicherheit in Deutschland zusammenarbeiten.

Wer die Herausforderung annimmt, den Schutz der modernen Informationstechnik zu organisieren, muss sich ihrer Vielfalt und Dynamik anpassen. Zu unserem Leistungsspektrum gehören zum Beispiel: die Aufklärung und Sensibilisierung von Bürgern, Qualitätsprüfung und Zertifizierung von Produkten nach internationalen Kriterien, die Unterstützung der Initiative BundOnline 2005, die Entwicklung von kryptographischen Produkten oder der Betrieb des Computer Notfallteams CERT-Bund (Computer Emergency Response Team) – um nur einen kleinen Ausschnitt der Tätigkeiten zu nennen.

Aus den unterschiedlichen Arbeitsgebieten ergeben sich intensive Beziehungen zu allen Beteiligten in der Informationstechnik: Sowohl mit IT-Nutzern als auch mit IT-Security-Anbietern steht das BSI im regen Informationsaustausch. Dabei nimmt das BSI die Position einer steuernden, vertrauenswürdigen Instanz ein. Die Stellung als neutrale Fachbehörde macht es möglich, Gefährdungslagen und Schutzmaßnahmen interessenunabhängig zu prüfen.

Der Erfolg des BSI ist nur durch seine motivierten und engagierten Mitarbeiterinnen und Mitarbeiter möglich. Ihnen gilt mein ganz besonderer Dank.

Bonn, im März 2004

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

Inhaltsverzeichnis

Inhalt

Historie

In Verbindung bleiben: das geht auch mit einer Schnur und zwei Konservenbüchsen — das Dosentelefon

RÜCKBLICK: GRÜNDUNG UND AUFBAU DES BUNDESAMTES FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK – BSI

Mit den Aufgaben gewachsen

Die Informationstechnik (IT) entwickelt sich schnell. Ungebremst steigt schon seit Jahren die Leistungsfähigkeit der einzelnen Systeme. Innovative Produkte drängen in den Markt, ersetzen bestehende Lösungen oder ergänzen sie. Auf der Suche nach immer besseren Produkten erfolgt die technische Entwicklung im Einzelfall zwar zielgerichtet, im großen Kontext aber spontan und unkoordiniert.

Das Ergebnis dieses Prozesses sind immer mächtigere IT-Systeme. Zugleich entsteht eine Vielzahl technologischer Inseln, konkurrierender Standards und inkompatibler Netze. Heute hat die Komplexität der Informationstechnik ein nur noch schwer zu fassendes Ausmaß erreicht.

Gleichzeitig hat sich die Informations- und Kommunikationstechnik (IuK-Technik) sowohl zum wirtschaftlichen als auch zum gesellschaftlich herausragenden Entwicklungsfaktor moderner Volkswirtschaften heraus gebildet. Für IT-Sicherheit zu sorgen, ist deshalb nicht nur eine anspruchsvolle, sondern vor allem eine wichtige Aufgabe. In Deutschland trägt diese Verantwortung das Bundesamt für Sicherheit in der Informationstechnik – BSI.

Gegründet wurde das BSI 1991 mit Sitz in Bonn. Es ist dem Geschäftsbereich des Bundesministeriums des Innern zugeordnet. Zur Erfüllung seines gesetzlichen Auftrages – für IT-Sicherheit zu sorgen – muss das BSI mit

dem Entwicklungstempo der Informations- und Kommunikationstechnik mithalten. In bestimmten Bereichen gibt das BSI die Richtung und den Schritt selbst vor.

Wachsende Aufgabenbereiche, neue Schwerpunktthemen und stets auf dem neuesten Stand zu bleiben – das fordert Ressourcen. Deshalb ist das BSI mit der allgemeinen Entwicklung der Informationstechnik gewachsen, sowohl personell als auch in Bezug auf das verfügbare Finanzvolumen.

So vielschichtig die Probleme im IT-Sicherheitsbereich sind, so komplex ist das Aufgabenspektrum des BSI.

Die Präsidenten des BSI: Gründungspräsident Dr. Otto Leiberich (rechts), sein Nachfolger Dr. Dirk Henze (links) und der amtierende Präsident Dr. Udo Helmbrecht.

Aufgabenspektrum des BSI

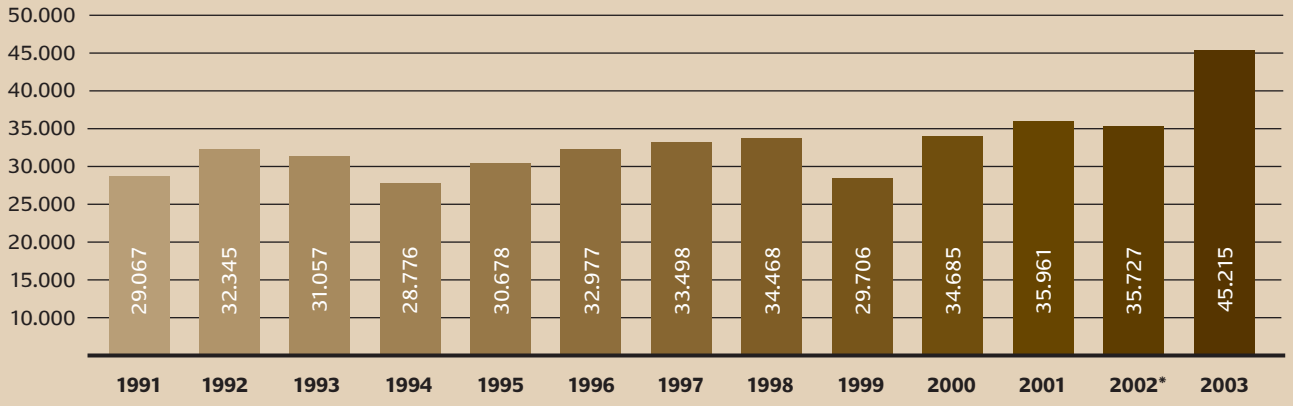
Prüfung und Bewertung der Sicherheit von IT-Systemen

Die Evaluierung und Zertifizierung nach internationalen Kriterien macht die Sicherheitseigenschaften von Produkten transparent. Dies ist für die Konkurrenzfähigkeit im hart umkämpften Markt ein wichtiges Zugpferd; für die Zulassung in Sicherheitsbereichen von Staat und Industrie ist es Voraussetzung.

Entwicklung von IT-Schutzvorkehrungen

Das BSI entwickelt und vertreibt selbst IT-Sicherheitssysteme, angefangen von Produkten für den Umgang mit klassifizierten Informationen bis hin zu Administrationstools für Unix oder die Umsetzung des IT-Grundschutzes. Die Produkte werden teilweise in enger Kooperation mit Partnern aus der Industrie entwickelt.

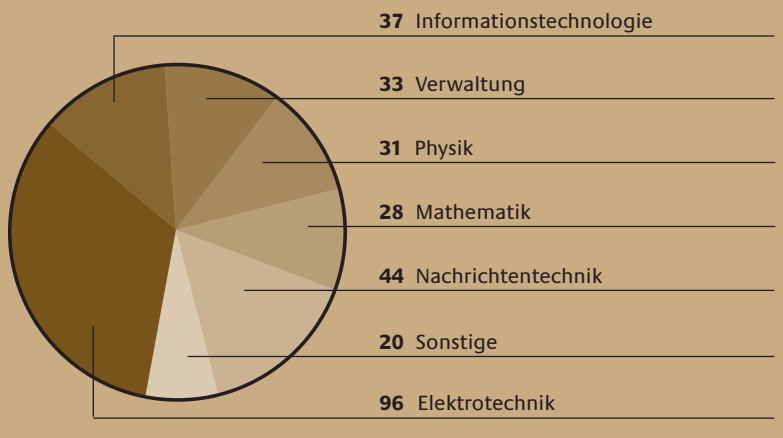
BSI-Haushalt 1991 bis 2003
in Tausend Euro



*Im Jahr 2002 kamen zusätzlich Anti-Terror-Paket-Mittel i.H. v. rd. 10,7 Mio Euro hinzu

Seit der Gründung des BSI 1991 ist der Etat bis heute um mehr als 50% gestiegen. Das entspricht den wachsenden Aufgabenbereichen.

Fachrichtungen im BSI
Anzahl der Mitarbeiter, höherer und gehobener Dienst



Die komplexen Strukturen der Informationstechnik fordern zwar in erster Linie naturwissenschaftlich ausgebildete Mitarbeiter. Aber die vielseitigen Verknüpfungen der IuK-Technik in alle Lebensbereiche hinein führen auch zum Bedarf nach verschiedenen anderen Fachrichtungen, insbesondere nach Juristen, Verwaltungs- und Wirtschaftswissenschaftlern.

Historie

Beratung von Herstellern, Vertreibern und Anwendern von IT-Systemen

Die Aufklärungs- und Beratungsleistungen richten sich an private Anwender, IT-Verantwortliche in Behörden und Unternehmen sowie an Hersteller von IT-Produkten. Damit wird gewährleistet, dass alle Beteiligten von Anfang an IT-Sicherheitsaspekte bei Entwicklung und Einsatz der Systeme beachten können.

Mitarbeit in internationalen Gremien

Das BSI vertritt und unterstützt mit seiner Gremienarbeit, z. B. in der Nato und in der EU, die Interessen Deutschlands im Hinblick auf IT-Sicherheitsaspekte. Mit dem Einfluss des BSI sollen Fehlentwicklungen verhindert, der Informationsaustausch gefördert und internationale Kontakte gepflegt werden.

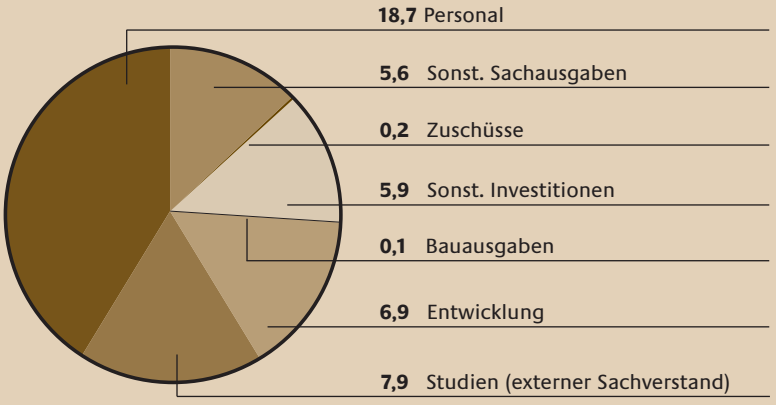
Trendforschung und Projektarbeit zu neuen technologischen Ansätzen

Die frühzeitige und möglichst präzise Vorhersage von zukünftigen Entwicklungen ermöglicht rechtzeitiges, umsichtiges Handeln.
Aus diesem Grund beschäftigt sich das BSI in Arbeitsgruppen und Projekten mit allen wichtigen Themen in Bezug auf die kommende IT-Sicherheit. Zu nennen sind hier z.B. „Open Source Software“, die IT-Implementierung in biometrischen Systemen oder die Aktivitäten der Trusted Computing Group (TCG). Ziel dieser Industrievereinigung ist es, einen Sicherheitschip „TPM“ (Trusted Platform Module) zur Absicherung verschiedener IT-Geräte – z.B. PCs, Smartphones oder PDAs – zu entwickeln.

Die Ansprechpartner im BSI. Von links nach rechts: Anja Hartmann, Leiterin Öffentlichkeitsarbeit, Michael Dickopf, Pressesprecher, Dr. Udo Helmbrecht, Präsident des BSI und Michael Hange, Vizepräsident.

Anteil der BSI-Ausgaben für Sachgebiete 2003

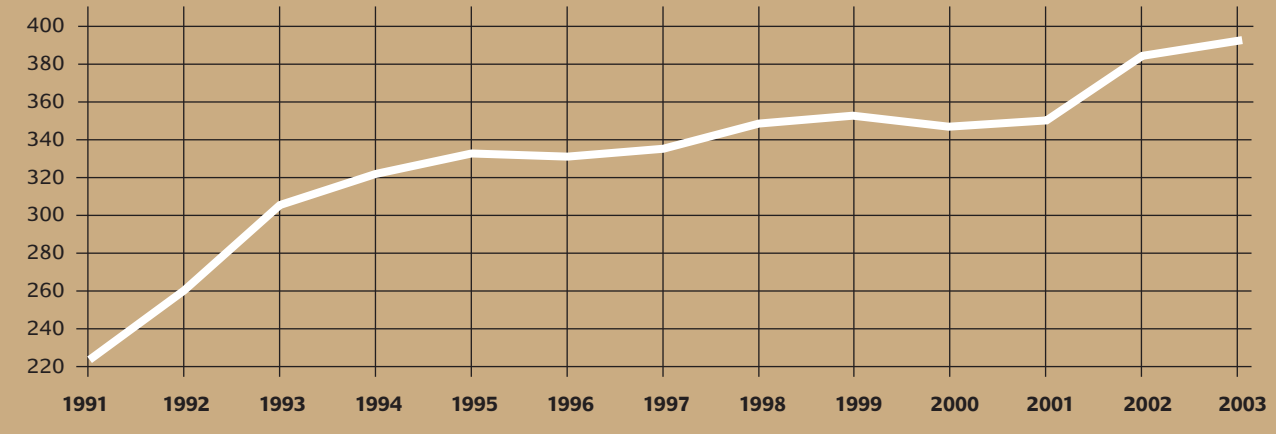
in Milionen Euro



Neben den Ausgaben für Personal (18,7 Mio Euro) ist der stärkste Haushaltsposten der Etat für Studien und Entwicklung (14,8 Mio Euro = 33%).

Mit dem Anwachsen der Tätigkeitsfelder und der Komplexität der einzelnen Aufgaben stieg die Personalstärke kontinuierlich an. Das enorme Entwicklungstempo der Informationstechnik fordert dabei den vollen Einsatz der Mitarbeiter. Über 200 in 2003 laufende Projekte müssen neben dem Tagesgeschäft betreut und vorangetrieben werden. Trotz der Belastung bietet das dynamische und abwechslungsreiche Umfeld ein sehr gutes Arbeitsklima.

Zahl der BSI-Mitarbeiter 1991 - 2003



Das BSI versteht sich mit seinen Angeboten primär als IT-Sicherheitsdienstleister des Bundes. Traditionell bietet es Bundes-, aber auch Landes- und Kommunalbehörden umfangreiche Dienstleistungen an. Zu den Zielgruppen gehören selbstverständlich nicht nur Organisationen des öffentlichen Sektors. Viele auf die Bedürfnisse der jeweiligen Anwender zugeschnittene Produkte stehen auch für kleine und mittelgroße Unternehmen zur Verfügung. Denn hier ist der Nachholbedarf an Risikovorsorge – anders als bei den meisten großen Firmen – durch IT-Schutzmaßnahmen besonders groß.

IT-Sicherheit schon bei der Produktentwicklung

Dies betrifft ebenso die zahlenmäßig größte Gruppe in Deutschland: die privaten, technisch weniger versierten IT-Anwender. Mit speziellen Angeboten wendet sich das BSI an den Bürger, da schon alleine durch die vielen möglichen Betroffenen das Schadenspotenzial beträchtlich ist. Aufklärung und Sensibilisierung für die möglichen Gefahren und Schutzmaßnahmen sind daher für das BSI sehr wichtig.

Auf der anderen Seite stehen die IT-Hersteller und die maßgeblichen Forschungseinrichtungen im Fokus der BSI-Aktivitäten. Ziel ist es, maßgeblich auf die zukünftige Gestaltung von IT-Systemen Einfluss zu nehmen und schon im Vorfeld der Produktentwicklungen für ausreichende IT-Sicherheit zu sorgen. Allerdings gibt es IT-Sicherheit nicht kostenlos – weder für die Anbieter noch für die Anwender. Der Prozess beginnt auch nicht zwangsläufig beim Sicherheits-Design der Produkte: Denn nur wenn die Kunden konsequent Sicherheit fordern – und einen höheren Preis in Kauf nehmen – gibt es entsprechende Angebote. Aus diesem Grund sind Aufklärung und Sensibilisierung ein wesentlicher Beitrag zur Schaffung einer höheren IT-Sicherheit auch für die Hersteller und Forschungslabore.

Für das BSI ist der ständige Kontakt zu Wirtschaft und Forschung entscheidend für den Erfolg seiner Arbeit. Nur durch intensiven Erfahrungsaustausch lassen sich die gestiegenen Anforderungen an die Sicherheitseigenschaften der Produkte erfüllen. Die Bedürfnisse der Kunden – aus deutschen Behörden, Wirtschaft, internationalen Organisationen – müssen in einem ständigen Prozess erhoben und in die Entwicklungen einbezogen werden. Damit wird das BSI als Einkäufer externen Sachverstandes und von Produktionsmitteln sowohl zum Kunden als auch zum Partner und zum Anbieter von Systemen und Beratungsleistungen.

Teilnahme am internationalen Erfahrungsaustausch

Die Arbeit des BSI beschränkt sich wegen des internationalen Charakters der IuK-Technik nicht nur auf Deutschland. Die Mitarbeit und Unterstützung in IT-Sicherheitsfragen umfasst europa- und weltweit agierende Gremien sowie Projektarbeiten z.B. auf EU- oder Nato-Ebene. Ziel ist es, Einfluss auf sicherheitsrelevante Entwicklungen auszuüben, Informationen zu beschaffen und das vorhandene Know-how bereitzustellen.

Diese vielfältigen Aktivitäten führen zu genauen Kenntnissen darüber, was sowohl am Markt, vom Bürger als auch im staatlichen Umfeld gefordert wird. Für das BSI bedeutet dies, dass es als Schnittstelle zu allen Beteiligten neutral, verantwortungsvoll und kompetent zugleich handeln muss.

Meilensteine von der Gründung bis heute

Die Gründungsgeschichte des BSI reicht in das Jahr 1986 zurück. Zu diesem Zeitpunkt wurde in der Vorgängerorganisation ZfCh (Zentralstelle für das Chiffrierwesen) eine Arbeitsgruppe aufgebaut, die sich vor dem Hintergrund der schnellen Entwicklung der IuK-Technik mit den Sicherheitsfragen beschäftigte. Bis dahin hatte sich die ZfCh auf die zentrale Aufgabe Kommunikationssicherheit konzentriert. Die Arbeitsgruppe vergrößerte sich bald auf 70 Mitarbeiter. Sie befassten sich mit der Evaluierung und Zertifizierung von IT-Produkten und -systemen. Vor allem die Zertifizierung war schließlich der Auslöser für die Gründung einer eigenständigen Behörde, des BSI. 1990 wurde vom Bundestag die Errichtung im Geschäftsbereich des Bundesministeriums des Innern beschlossen.

Die wichtigsten Daten in chronologischer Reihenfolge

1986 wird der Zentralstelle für das Chiffrierwesen zusätzlich der Aufgabenbereich „Computersicherheit“ übertragen, soweit es um die Bearbeitung von Verschlusssachen geht.

1987 wird der „Interministerielle Ausschuss für die Sicherheit in der IT“ (ISIT) unter der Federführung des Bundesministers des Innern gebildet.

1989 wird die Zentralstelle für das Chiffrierwesen wegen der erweiterten Aufgabenstellungen in die Zentralstelle für die Sicherheit in der Informationstechnik (ZSI) umgewandelt.
Es erfolgt die Veröffentlichung der deutschen IT-Sicherheitskriterien.

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

Der unmittelbare Vorgänger des BSI – damals noch ZSI – veranstaltet den ersten deutschen IT-Sicherheitskongress in Bonn-Bad Godesberg.

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

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

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

1994 Beginn der Umsetzung einer breit angelegten Kryptoinnovationsstrategie im BSI, in deren Folge bis heute wesentliche kryptographische Systeme wie Elcrodat 6-2, Kryptosystem für den BOS-Digitalfunk, PLUTO Hochleistungskryptomodul, Elcrodat 4-2 Funksystem, SINA Architektur und zahlreiche Innovationen auf dem Gebiet der Public-Key-Kryptographie entstanden.
Unterstützung der Deutschen Bundesbank bei der Evaluierung von elektronischen Zahlungsverkehrssystemen.

1996 Veröffentlichung der ersten Common Criteria in der Version 1.0.

1998 Das neue Referat „Internetsicherheit“ trägt der wachsenden Bedeutung des World Wide Web Rechnung.
Aufnahme der Geschäftsführung des Interministeriellen Ausschusses für Kritische Infrastrukturen und Beginn der Zukunftsforschung mit den Trendstudien.

1999 Beim „Jahr 2000-Problem“ stellte das BSI umfangreiche Services und Informationen zur Verfügung, z.B. eine spezielle Bürgerbroschüre. Es erfolgt der Aufbau und die Unterstützung der Public-Key-Infrastruktur.

Veröffentlichung der Common Criteria (CC) Version 2.1 als ISO-Standard.
Damit erfolgt die Einführung der CC in das Zertifizierungsschema des BSI und erste Protection Profile Entwicklungen beginnen.

Mit dem Start des Regierungsnetzes IVBB (Informationsverbund Berlin-Bonn) übernimmt das BSI die technische Koordination des Netzes.

2001 Bundesinnenminister Otto Schily setzt neue organisatorische, personelle und fachliche Rahmenbedingungen für die Weiterentwicklung des BSI zum zentralen IT-Sicherheitsdienstleister des Bundes in Kraft.
Das E-Government-Handbuch wird zum ersten Mal herausgegeben.
Die Einrichtung von CERT-Bund geht zurück auf eine Initiative der Task-Force „Sicheres Internet“ des BMI als Reaktion auf die DoS-Angriffe im Februar 2000. Der formalen Einrichtung des Referats „CERT-Bund“ 2001 gehen die Aktivitäten der Projektgruppe CERT-Bund im BSI voraus.

Im Rahmen des Antiterrorpakets wird das Referat „IT-Penetrationszentrum“ und die Biometrie-Projektgruppe gegründet.
Außerdem startet die Unterstützung der Migration auf Open-Source-Software mit Herausgabe eines Migrationsleitfadens, von Studien, Eigenentwicklungen und aktiven Beratungsleistungen.

Das Referat „Kritische Infrastrukturen“ startete umfangreiche Sektorenanalysen als Reaktion auf die Terroranschläge.
Das BSI übernimmt die Gründungspräsidentschaft des „Common Criteria Mangement Committee“.

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

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

Die Welt der Bits & Bytes erstreckt sich über den ganzen Globus und erfasst zunehmend alltägliche Lebensbereiche.

Sicherheit durch Zusammenarbeit

Ob auf nationaler oder auf internationaler Ebene – Informationsnetzwerke sind Sicherheitsrisiken ausgesetzt. Das BSI arbeitet an einer neuen „Kultur der Sicherheit“, stellt für den staatlichen Bereich Sicherheitskonzepte bereit und berät die privaten Anwender.

Gebündelte Erfahrungen mit IT-Sicherheit kann das BSI sowohl in internationalen Gremien als auch in der Kommunikation mit dem Bürger zur Verfügung stellen. In jahrelanger Arbeit sind Erkenntnisse gewachsen, die sich auf allen Gebieten der IT-Sicherheit heute auszahlen.

Das BSI stellt für den staatlichen Bereich Sicherheitskonzepte bereit. Und es berät und informiert den privaten Anwender in allen Fragen der Datensicherung und im Umgang mit vertraulichen Daten. Warnhinweise, Online-Angebote und weitere aktuelle Informationen sind über die Homepage des BSI jederzeit abrufbar. Ein eigenes Web-Portal mit leicht fassbaren Informationen ist für die breite Öffentlichkeit gedacht. Außerdem veranstaltet das Bundesamt selbst Kongresse und Foren für die Fachöffentlichkeit.

Im Mai 2005 findet bereits der neunte IT-Sicherheitskongress mit internationaler Beteiligung in Bonn statt. Von San Francisco über München bis Berlin ist das BSI auch auf allen wichtigen Messen vertreten, seien es die RSA Conference, die CeBIT oder Fachmessen wie „Moderner Staat“.

1. Internationale Kooperation

Die weltweite Vernetzung der Kommunikations- und Informationssysteme zwingt zu international abgestimmtem Handeln, gerade im Bereich der IT-Sicherheit.

Deshalb engagiert sich das BSI aktiv in Gremien z.B. der EU oder NATO. Durch die Mitarbeit sollen die Entwicklungen der Informationssicherheit frühzeitig erkannt und damit Sicherheitsrisiken entgegengewirkt werden. Die Arbeit des BSI hat Gewicht: Deutschland gehört auf dem Gebiet der IT-Sicherheit zu den führenden Staaten; ausgewiesen durch eine jahrzehntelange Erfahrung im staatlichen Bereich, beachtliche Forschungsergebnisse und begründet durch die Leistungsfähigkeit der einschlägigen Industrie. Dieses Potenzial zu fördern – und den Einfluss weiter auszubauen – ist ein vordringliches Ziel der internationalen Zusammenarbeit. Ein weiterer Aspekt liegt in der Förderung der Marktchancen deutscher Hersteller.

Neben der traditionell intensiven Beteiligung des BSI in Gremien und Projekten der NATO gewinnt das Engagement im Zusammenhang mit der europäischen Integration zunehmend an Bedeutung. Das BSI ist die akkreditierte nationale INFOSEC-Behörde beim Generalsekretariat des Ministerrates der EU. Es unterstützt die Europäische Union bei der Gestaltung und der Umsetzung der Sicherheitsvorschriften für klassifizierte Informationen. Der Bedarf ergibt sich aus der Aufgabe des Generalsekretariats, die gemeinsame Außen- und Sicherheitspolitik der EU zu koordinieren. Die Mitarbeit erfolgt in vielfältiger Weise: Beratungsleistungen für neue Netzwerke, Projekte und Serviceleistungen, Angebot und Evaluierung von Kryptogeräten und Akkreditierung von Systemen.

Die Erfahrungen in der Zusammenarbeit mit EU und NATO eröffnen im Rahmen der Erweiterung der Europäischen Union und des Nordatlantischen Bündnisses eine Reihe von fruchtbaren, bilateralen Kontakten. Sie begünstigen die Verbreitung der BSI-Sicherheitsphilosophie und erschließen Märkte für die durch das BSI geförderten Sicherheitsprodukte. Ergänzend hierzu bietet die neue Beteiligung am OECD-Programm zur Förderung einer „Culture of Security“ die Ausgangsbasis für den Aufbau weiterer Beziehungen.

Auch die EU nimmt die Beratungsleistungen des BSI in Anspruch. Im Bild: Straßburg, Sitz des EU-Parlaments.

Plattform für Experten

FIRST (Forum of Incident Response and Security Teams) ist ein internationaler Zusammenschluss von ca. 100 staatlichen und privaten CERTs (Warn- und Informationsdiensten für IT- Gefährdungslagen). FIRST bietet eine Plattform für den Erfahrungsaustausch über die Erkennung und Behandlung von IT-sicherheitsrelevanten Vorfällen. Durch die Mitarbeit des BSI werden Informationen für die eigenen Aktivitäten im Bereich CERT-Bund zusammengetragen und ausgewertet.


FIRST TIMES

THE NECESSARY EVOLUTION OF FIRST TIMES

2003-2004

Sichere IT-Systeme für die NATO

Die NATO und das Auswärtige Amt benötigen weltweit interoperable, sichere und leistungsfähige Kommunikations- und Informationssysteme. Ein großer Teil der Gesamtausgaben der NATO fließt in die Beschaffung und Erhaltung dieser Systeme, die unter dem „NATO Security Investment Program“ in Auftrag gegeben werden.

Auch die EU baut ihre Kommunikationsnetze mit dem selben hohen Sicherheitsbedarf aus. Sowohl in der NATO als auch der EU ist Deutschland einer der Hauptbeitragszahler. Das BSI bietet zusammen mit den Industriepartnern Rohde & Schwarz (Elcrodat) und Secunet (Sina-VPN) leistungsfähige Systeme für den Bedarf der NATO und der EU an.

2. IT-Sicherheit: Ein Thema, das alle angeht

Die zielgruppengerechte Aufklärung über Fragen zur IT-Sicherheit hat für das BSI hohe Priorität. Nur wenn die Risiken der Informationstechnik und angemessene Schutzvorkehrungen bekannt sind, können sich Anwender vor den drohenden Gefahren wirkungsvoll schützen.

Da die IT zunehmend alle Lebensbereiche erfasst, wendet sich das BSI mit einer wachsenden Palette von Informationen an Bürger, Behörden und Unternehmen. Die unterschiedlichen Anforderungen dieser Zielgruppen erfüllt das BSI mit einer Reihe von bedarfsspezifisch aufbereiteten Informationen und Kommunikationskanälen.

Die zahlenmäßig größte Gruppe stellen die eher unerfahrenen Anwender, die Bürger, dar. Sie sind über die drohenden Gefahren und die möglichen Abwehrmaßnahmen oft nur unzureichend aufgeklärt. Mit fatalen Folgen: Ohne Schutzsysteme stehen private Surf-PCs für Angreifer völlig offen, es fehlen Back-Ups, oder die vorhandene Sicherheits-Software wird falsch eingesetzt und schlecht gepflegt.

Kurzweilige Texte und Illustrationen zeichnen das Bürger-Portal aus. Die Informationen sind auf das Wesentliche konzentriert, um leicht nachvollziehbar IT-Sicherheit für Bürger zu vermitteln.

Anfang 2003 hat das BSI deshalb das Web-Portal www.bsi-fuer-buerger.de eingerichtet. Das Portal ist wie ein Handbuch lesbar: Verschiedene Unterkapitel erläutern den Schutz vor Viren und Würmern, andere Kapitel beschreiben die Datensicherung oder zeigen den Umgang mit vertraulichen Daten. Eine Toolbox mit Programmen, ein Glossar und viele nützliche Links bieten das Rüstzeug, um unbeschwert das Internet nutzen zu können.

Kooperation mit der Stiftung Warentest. Dieser Spezialausgabe lag die BSI-CD „Ins Internet – mit Sicherheit!“ bei.

Über verschiedene Kooperationspartner hat das BSI die Inhalte des Bürger-Portals großflächig vertrieben: Fujitsu-Siemens Computers beispielsweise stellt die Inhalte auf jedem neuen Consumer-PC der Scaleo-Reihe schon vorinstalliert zur Verfügung. Über Messen und Zeitschriftenbeilagen – so im Sonderheft der Stiftung Warentest, in „Chip“ oder in der „PC-Welt“ – ist das Bürgerportal auf CD schon über 1.640.000 Mal verteilt worden.

Würmer, Viren, Dialer, Spam – wer sich mit dem „Wachhund“ des BSI versteht, braucht sich darum keine Sorgen zu machen.

Fachwissen für IT-Profis

IT-Anwender mit Vorkenntnissen und IT-Profis finden aktuelle Informationen unter www.bsi.bund.de. Inhaltlich stellt das BSI dort die gesamte Bandbreite seiner Fachthemen zur Verfügung: Projekte, Studien, Hintergrundinformationen, Angebote zu IT-Grundschutz, Internetsicherheit, E-Government, die Projekte SINA und SPHINX, die Produkt-Zertifizierung und viele andere Themen mehr. Zum Online-Service gehört auch der periodisch erscheinende Newsletter, der auf Wunsch von jedem zu beziehen ist.

Warnhinweise und Informationsangebote

Damit IT-Verantwortliche rechtzeitig über Gefährdungen informiert sind und Präventionsmaßnahmen ergreifen können, stellt das BSI umfangreiche Warn- und Informationsangebote zur Verfügung. Diese werden auf der BSI-Webseite veröffentlicht oder nach Anmeldung bei CERT-Bund (Computer Emergency Response Team) automatisch verschickt.

Die kompakte Übersicht über die wichtigsten Sicherheitsmaßnahmen.

Vom Standardwerk bis zum Faltblatt

Neben den Onlineangeboten bietet das BSI eine Vielzahl von Printpublikationen an. Dazu zählen u.a. die Standardwerke zu IT-Grundschutz oder E-Government, der „Leitfaden IT-Sicherheit“, Studien, Faltblätter und Broschüren.
Alle Veröffentlichungen befinden sich auch auf einer CD, die gegen einen frankierten Rückumschlag kostenlos erhältlich ist. Diese CD richtet sich mit ihren Inhalten – anders als das Bürger-Portal – an das Fachpublikum.

BSI setzt auf Partnerschaften

Bei der zielgruppengerechten Ansprache setzt das BSI auf Partnerschaften mit Wirtschaft, Verwaltung, Medien und Wissenschaft: Das BSI informiert periodisch über aktuelle Themen der IT-Sicherheit im BSI-Forum in der Fachzeitschrift „<kes> – Die Zeitschrift für Informations-Sicherheit".

Seit dem 1. Juli 2003 verbreitet das BSI seine aktuellen Informationen zusätzlich über das Heise-Sicherheitsportal (www.heisec.de). Damit ist gewährleistet, dass viele Personen der Zielgruppen erreicht werden.
2003 organisierte das BSI eine Reihe von Veranstaltungen beispielsweise zusammen mit der Gesellschaft für Informatik, der Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW) oder BITKOM.

Messeauftritte gehören dazu

Darüber hinaus ist das BSI auf allen wichtigen Messen mit Bezug zu seinen Themen vertreten: Auf der CeBIT, der Security sowie auf der RSA-Conference in San Francisco. Die IT-Security Area auf der Münchner „SYSTEMS" wird vom

In Zusammenarbeit mit dem Verlag Secumedia erscheint das BSI-Forum in der <kes> als offizielles Organ des BSI.

Typischer Warnhinweis auf der Website von heise online, einem weiteren Kooperationspartner des BSI.

Auf den Messen präsentiert das BSI Arbeitsergebnisse und Aufgabenschwerpunkte. Durch den persönlichen Kontakt findet ein intensiver Informationsaustausch mit den Kunden und Partnern des BSI statt.

Secumedia Verlag organisiert und steht unter der Schirmherrschaft des BSI. Als Aussteller, aber auch durch zahlreiche Vorträge in den technischen und managementorientierten Foren hat das BSI auf der IT-Security Area mitgewirkt.
Bei der Fachmesse „Moderner Staat“ in Berlin ist das BSI Partner für den Bereich der IT-Sicherheit. Neben persönlichen Gesprächen steht die Präsentation wichtiger IT-Sicherheitsthemen und aktueller Arbeitsschwerpunkte im Vordergrund der Veranstaltungen.

Kongress „IT-Sicherheit im verteilten Chaos“

Alle zwei Jahre veranstaltet das BSI zudem den Deutschen IT-Sicherheitskongress. Er hat sich in den vergangenen Jahren zu dem zentralen Treffen der IT-Sicherheitsfachleute entwickelt. Unter dem Motto „IT-Sicherheit im verteilten Chaos“ zog der dreitägige Kongress 2003 in Bonn rund 700 hochkarätige Teilnehmer an. Auf einer kongressbegleitenden Ausstellung präsentierten 30 Aussteller neue Entwicklungen und Lösungen. Der neunte Kongress findet im Mai 2005 statt. Auch hier bietet das Programm wieder einen fundierten Überblick über das, was zukünftige Impulse in der IT-Sicherheit setzt.

Tagungsort Bonn

Den Deutschen IT-Sicherheitskongress veranstaltet das BSI im zweijährigen Rhythmus. Er gilt als zentrale Veranstaltung im IT-Sicherheitsbereich in Deutschland.
Der achte Kongress unter dem Motto „IT-Sicherheit im verteilten Chaos“ fand 2003 in Bonn-Bad Godesberg statt und konnte an die erfolgreiche Entwicklung der vorangegangenen Jahre anknüpfen.

Risiken / Gefahren

PCs können sich nicht selbst verteidigen – sie brauchen Schutz.

Risiken vorbeugen – Gefahren erkennen

Prävention statt Nachsorge – das ist das zentrale Anliegen des BSI in punkto Schadensvermeidung.

Computerviren können sich heute so schnell verbreiten, dass jede Warnmeldung bereits zu spät sein kann.

Das BSI hat ein eigenes Computer-Notfall-Team für die Bundesverwaltung aufgestellt. Das „Computer Emergency Response Team (CERT)“ hat die Aufgabe, präventiv auf Sicherheitslücken in den Computersystemen hinzuweisen. CERT-Bund kann rund um die Uhr und sieben Tage in der Woche auf mögliche Gefährdungen und Angriffe reagieren und kurzfristig Gegenmaßnahmen einleiten.

Genauso wichtig ist der richtige IT-Grundschutz. Das BSI bietet mit seinem IT-Grundschutz-Handbuch, das mittlerweile auf über 2000 Seiten angewachsen ist, ein ganzheitliches Konzept an, das bereits in zahlreichen Behörden und Unternehmen umgesetzt wurde. Das Handbuch hat sich national wie international als Standard etabliert.
Vor dem Einsatz von IT-Produkten sollte man sich davon überzeugen, dass die Systeme sicher sind. Aufgabe des BSI ist es, die Angebote, die auf dem Markt vorhanden sind, hinsichtlich ihrer Sicherheitseigenschaften zu prüfen und zu zertifizieren.

Dass die Daten und nicht die Bürger laufen sollen – das ist das Ziel aller modernen E-Government-Aktivitäten. Ob auf Bundes- oder Landesebene: Das BSI ist bei dem Vorhaben, Dienstleistungen der Behörden internet-tauglich zu machen, nicht wegzudenken. Nur wenn Datensicherheit garantiert ist, werden die Bürger E-Government-Dienstleistungen akzeptieren.

1. Das Computer-Notfallteam: CERT

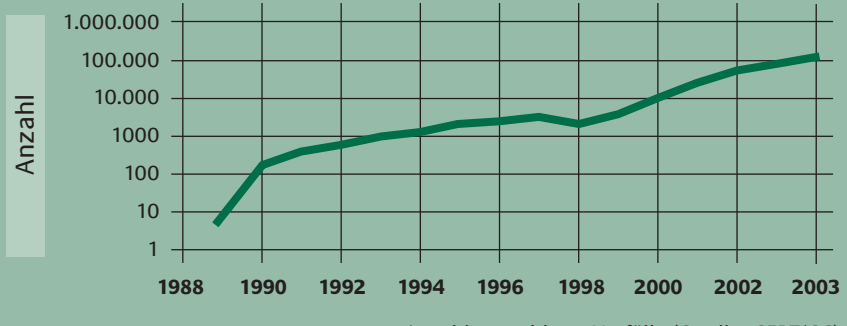
Sobig.F und Lovsan haben es 2003 allen eindringlich vor Augen geführt: Frühzeitige Warnungen und zielgerichtete Hinweise auf die verfügbaren Maßnahmen gegen Computerviren, Würmer und Trojanische Pferde haben eine besondere Bedeutung für mehr IT-Sicherheit.

Im Bereich der Bundesverwaltung übernimmt diesen zentralen Informationsservice das im BSI angesiedelte CERT-Bund (Computer Emergency Response Team). Zwischen dem Start eines Angriffs und der Schädigung der verwundbaren Systeme liegen oftmals nur noch sehr kurze Laufzeiten. Sie lassen kaum noch Reaktionsmöglichkeiten zu. Beispielsweise infizierte der „Slammer-Wurm“ im Februar 2003 innerhalb von nur zehn Minuten weltweit 90 Prozent aller anfälligen Systeme. Im August desselben Jahres verursachte auch der Blaster-Wurm („Lovsan“) weltweit Millionenschäden.

In beiden Fällen stand jedoch rechtzeitig ein Sicherheits-Update zur Verfügung. Leider waren die Updates in vielen Fällen nicht installiert. Ungeklärte Zuständigkeiten, mangelndes Wissen über geeignete Informationsquellen oder die Überlastung vieler Systemadministratoren verhinderten, dass sie sich über die aktuell bekannt gewordenen Sicherheitslücken ihrer Systeme informierten. Als Konsequenz wurden und werden Probleme nicht erkannt und verfügbare Sicherheits-Updates („Patches“) nicht implementiert.

Auch die Bundesverwaltung ist vielfach Angriffen oder Angriffsversuchen auf ihre IT-Systeme ausgesetzt. Daher wurde im September 2001 das Computer-Notfallteam für die Bundesverwaltung (CERT-Bund) als Kompetenzstelle für den Bereich der Rechner- und Netzwerksicherheit eingerichtet.

Sicherheitsvorfälle verzehnfacht



Anzahl gemeldeter Vorfälle (Quelle: CERT/CC)

Zwischen den Jahren 2000 und 2003 haben sich die gemeldeten Sicherheitsvorfälle mehr als verzehnfacht. Die zentrale Anlaufstelle für die Sammlung, Auswertung und die zielgerechte Weitergabe von Warnmeldungen ist für die deutsche Bundesverwaltung das CERT-Bund im BSI.

Fachmesse „Moderner Staat“ 2003 in Berlin. Günther Ennen vom BSI erläutert die Risiken vernetzter Systeme in der Informationstechnik.

CERT-Bund erfüllt folgende Kernaufgaben:

Erstens

Bereitstellung einer ständig erreichbaren zentralen Ansprechstelle

- Innerhalb der Bürozeit: telefonische Hotline 01888CERTBUND bzw. 01888-23782863
- Außerhalb der Bürozeit: Rufbereitschaft für den geschlossenen Nutzerkreis
- Jederzeit: E-Mail certbund@bsi.bund.de oder per Fax 0228-308 96 25.

Zweitens

Eingehende Vorfallsmeldungen werden fachkompetent analysiert und bewertet. Durch die enge Zusammenarbeit mit nationalen und internationalen Computer-Notfallteams wird die schnelle Verfügbarkeit und die Qualität dieser Auswertungen gesteigert.

Drittens

Eventuell anstehende Untersuchungen der Vorfälle und die Wiederaufnahme des Betriebs werden unterstützt und koordiniert und bei Bedarf sogar vor Ort betreut.

Viertens

Die qualitätsgesicherten Informationen, im Fachjargon „Advisories“ genannt, werden in digital signierten Meldungen an die verantwortlichen Ansprechpartner in den Behörden übermittelt. Dabei kommt dem Warn- und Informationsdienst (WID) von CERT-Bund eine besondere Bedeutung zu.

Von Januar bis September 2003 hat CERT 85 wichtige Warnmeldungen veröffentlicht. Über den im September neu eingerichteten Service der Kurzmeldungen informierte CERT innerhalb der folgenden zwei Monate bereits über 88 Sachverhalte per E-Mail.

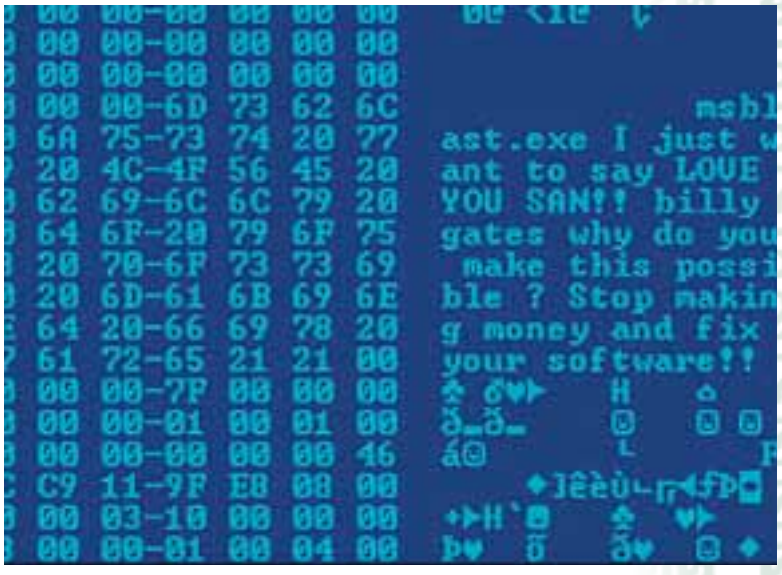
Die einzelnen beratenden Dienstleistungen stehen in erster Linie den Bundesbehörden zur Verfügung. Anfragen von Unternehmen, Privatpersonen oder privaten Institutionen werden nur im Rahmen verfügbarer Ressourcen bearbeitet. CERT-Teams können Administratoren entlasten und einen wesentlichen Beitrag zum Schutz der IuK-Technik leisten. Ihre Aufgabe ist es, die notwendigen Informationen über Sicherheitslücken zu erfassen und die erforderlichen Gegenmaßnahmen bedarfsgerecht an die jeweilige Zielgruppe zu kommunizieren.

Sie beantworten Anfragen zu Themen der IT-Sicherheit, warnen präventiv vor Schwachstellen und informieren über sicherheitsrelevante Ereignisse. Aufgrund dieser Informationen können zeitnah konkrete Schritte seitens der verantwortlichen Systembetreuer oder Endnutzer zur Gefahrenabwehr ergriffen werden. So werden schon im Vorfeld mögliche Schäden vermieden.

Vorbeugung ist die beste Verteidigung gegen Computerviren

Auch wenn ein Computervirus bereits Schaden angerichtet hat, können die CERT-Teams helfen. Sie bieten auch reaktive Dienstleistungen an, um die Auswirkungen des Angriffs zu mildern, die Beseitigung der Schäden zu unterstützen oder um die Sicherheitsvorfälle unmittelbar aufzuklären und zu bereinigen.

CERTs sind für sich alleine betrachtet nur ein Baustein im Kampf gegen IT-Sicherheitsvorfälle. Sie ersetzen keine robusten IT-Sicherheitskonzepte oder eine vernünftige Vorausplanung für den Notfall. Sie ergänzen jedoch das Spektrum geeigneter Einzelmaßnahmen und dienen als überaus wertvolle Informationsquellen und Unterstützungszentren.



Da hilft selbst die aktuellste Antivirensoftware nichts. Über einen standardmäßig installierten, aber leider fehlerhaften Dienst in Windows 2000 und XP verbreitete sich der Blaster-Wurm in kürzester Zeit massenhaft. Millionen von weltweit Betroffenen hätte ein von Microsoft rechtzeitig zur Verfügung gestellter Patch geholfen.

Angriffe durch Hacker

Neben den breit gefächerten, ungezielten Schädigungen durch Viren und Würmer erfolgen auch immer wieder zielgerichtete Angriffe durch Hacker.
Die Motive für diese Angriffe sind sehr vielschichtig und aufgrund der sehr hohen Dunkelziffer nur schwierig zu analysieren. Einige Beispiele:

- **„Sportsgeist“** – die Befriedigung, komplexe Sicherungsmechanismen überwinden zu können und somit die eigene Überlegenheit zu demonstrieren;

- purer **Vandalismus** – der Angreifer will neben der Demonstration seiner Überlegenheit zusätzlich möglichst hohen willkürlichen Schaden verursachen;

- **persönliche Bereicherung**, wie sie durch den Missbrauch von Kreditkarteninformationen oder anderen Passwörtern möglich ist;

- **Industriespionage** oder allgemeiner die Erlangung von Wettbewerbsvorteilen;

- zielgerichtete ideelle, finanzielle oder physische **Schädigung** eines Gegners.

Die Hacker nutzen bekannt gewordene Schwachstellen aus, um die Kontrolle über die ungeschützten Systeme zu erlangen. Aufgrund der hohen Komplexität der Betriebssysteme und Applikationen werden ständig neue Sicherheitslücken bekannt.

Die Angriffsmethoden und Angriffswerkzeuge werden ständig weiterentwickelt und verfeinert. Daher ist die Härtung und Absicherung der IuK-Technik kein einmaliger Vorgang, sondern muss regelmäßig wiederholt werden.

2. Grundlage der Risikovorsorge: IT-Grundschutz

Moderne Geschäftsprozesse sind heute in Wirtschaft und Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. Eine zuverlässig funktionierende Informationstechnik ist für die Aufrechterhaltung des Betriebes unerlässlich.

Daher stellt eine mangelhaft geschützte Informationstechnik einen häufig unterschätzten Risikofaktor dar, der für manches Unternehmen existenzbedrohend sein kann. Zwar gibt es sehr gute Sicherheitssysteme für die unterschiedlichen Anforderungen. Diese werden aber gerade in kleinen und mittelgroßen Unternehmen oft nur unzureichend ein- und umgesetzt. Dabei ist eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen.

Allerdings bedeutet bedarfsgerechter IT-Grundschutz weit mehr als das bloße Anschaffen von Antivirensoftware, Firewalls oder Backupsystemen. Ein ganzheitliches Konzept ist wichtig: Nur so kann ausgehend von einer Ist-Analyse der Schutzbedarf der eigenen Institution festgestellt und daraus dann die spezifischen Maßnahmen abgeleitet werden. Hierfür hat sich das IT-Grundschutzhandbuch (GSHB) des BSI national wie auch international als Standard etabliert. Das schon seit 1994 ständig weiterentwickelte, mittlerweile über 2000 Seiten starke Werk beschreibt detailliert mögliche Gefahren und Schutzvorkehrungen. Es enthält eine systematische Methodik zur Erarbeitung von IT-Sicherheitskonzepten und praxiserprobte Standard-Sicherheitsmaßnahmen, die bereits in zahlreichen Behörden und Unternehmen erfolgreich eingesetzt werden.
Das GSHB ist mit der 5. Ergänzungslieferung seit Ende 2003 um Beiträge zu Outsourcing, Elektronischer Archivierung sowie zum Microsoft Internet Information Server, Apache Webserver und Microsoft Exchange Server erweitert worden. Das Werk ist als Loseblattsammlung über den Bundesanzeiger Verlag erhältlich, die elektronische Fassung stellt das BSI seit Februar 2004 über das Internet zur Verfügung.

Basis für den Webkurs des BSI ist das Grundschutzhandbuch (GSHB). In Kooperation mit Partnern werden die GSHB-Angebote kontinuierlich erweitert.

Die Vorgehensweise nach IT-Grundschutz gliedert sich grob in folgende Bereiche:

IT-Systemerfassung / Strukturanalyse

Die Erstellung und Umsetzung eines Sicherheitskonzepts beginnt bei der Untersuchung des vorhandenen bzw. geplanten IT-Verbundes. Neben den Softwareanwendungen oder der Hardware sind hier z.B. auch die Serverräume, vorhandene Gebäude und die spezifischen Rollen der Mitarbeiter zu erfassen. Ziel ist die Schaffung einer soliden Grundlage, in der alle sicherheitsrelevanten Parameter beschrieben sind.

Feststellung des Schutzbedarfs

Ist der IT-Verbund ausreichend dokumentiert, geht es im zweiten Schritt um die Bewertung der Daten. Die Frage ist, wie wichtig bzw. kritisch welche der gespeicherten oder verarbeiteten Informationen sind. Hieraus leitet sich ab, ob z.B. Standard-Schutzmaßnahmen genügen oder spezielle Sicherheitssysteme zum Einsatz kommen müssen.

Basissicherheitscheck

In diesem Schritt wird festgestellt, welche Sicherheitsmaßnahmen schon umgesetzt sind.

Modellierung nach IT-Grundschutz

Aus den erfassten Bestandsdaten zum IT-Verbund und den Anforderungen an die IT-Sicherheit müssen nun die entsprechenden Sicherheitsmaßnahmen aus dem Grundschutzhandbuch zusammengetragen werden. Diese Abbildung des praktischen Umfeldes auf die Einzelmaßnahmen beschreibt die Modellierung anhand systematischer, kategorisierter Module. Anschließend erfolgt die Umsetzung der noch nicht realisierten Sicherheitsmaßnahmen.

IT-Grundschutz-Zertifikat

In vielen Fällen ist es wünschenswert, das erreichte Sicherheitsniveau nach innen und außen transparent zu machen. Das IT-Grundschutz-Zertifikat dokumentiert dies glaubwürdig. Es zeigt, dass verantwortungsvoll mit Informationen umgegangen wird und die Organisation aktive Risikovorsorge betreibt.

Eine seriöse Zertifizierung setzt immer eine vorhergehende Prüfung des jeweiligen Untersuchungsgegenstands voraus. So wurde auch beim IT-Grundschutz-Zertifikat ein detailliertes Prüfschema erarbeitet, das den Prüf- und Auditprozess ausführlich beschreibt. Auf der Grundlage eines solchen IT-Grundschutz-Audits entscheidet sich, ob ein IT-Grundschutz-Zertifikat für einen IT-Verbund vergeben werden kann. Die Qualität eines IT-Grundschutz-Audits hängt aber nicht nur vom Prüfschema, sondern auch wesentlich von den Fachkenntnissen und Erfahrungen des Auditors ab. Hierzu hat das BSI ein Lizenzierungsschema für IT-Grundschutz-Auditoren eingeführt. Voraussetzung für eine Lizenzierung als GS-Auditor sind Berufserfahrung im Bereich IT-Sicherheit und Projekterfahrung mit dem GSHB. Inzwischen wurden über 100 Auditoren durch das BSI lizenziert.

Für Nicht-Profis bietet das BSI seit 2003 einen Webkurs an, um einen leichten Einstieg in das umfassende Thema zu ermöglichen. In etwa vier Stunden führt er Neulinge in leicht nachvollziehbarer Form an das Thema IT-Grundschutz heran. Der Webkurs zeigt auf, wie für einen IT-Sicherheitsprozess die notwendigen Analysen durchzuführen und Dokumente auszuarbeiten sind. An einem Beispiel wird die Anwendung des GSHB auf einen vollständigen IT-Verbund nachvollzogen. Durch zahlreiche Anleitungen, Beispiele, Übungen und Hilfsmittel werden die Lernenden so trainiert, dass sie eigene Sicherheitskonzepte gemäß GSHB erstellen können. Der Webkurs steht auf den Internetseiten des BSI kostenlos zur Verfügung.

Ergänzend hierzu bietet das BSI ebenfalls seit 2003 den Leitfaden „IT-Grundschutz Kompakt“ an: Bewusst wird hier auf die Detailfülle des GSHB verzichtet, um einen kompakten und allgemeinverständlichen Überblick über die wichtigsten IT-Sicherheitsmaßnahmen zu schaffen. Insbesondere kleineren Organisationen wird damit der Einstieg in IT-Grundschutz erleichtert. Mit dem Leitfaden können die Leser schnell erarbeiten, was die für sie wesentlichen Sicherheitsmaßnahmen sind und wo noch dringender Handlungsbedarf besteht.

Die vom BSI erstellten Grundlagen und Hilfsmittel rund um das IT-Grundschutzhandbuch decken ein breites Themenspektrum ab. Dabei stehen nicht nur fachliche Aspekte im Vordergrund. Auch organisatorische Verfahrensabläufe wie der Know-how-Transfer zu den Anwendern und die praktische Umsetzung der empfohlenen Methoden werden behandelt. In der sich schnell entwickelnden IT-Welt ist es von enormer Bedeutung, auf die geänderten Bedingungen schnell zu reagieren. Besonders der intensive Erfahrungsaustausch mit den registrierten Anwendern und Auditoren trägt dazu bei, die Produkte des BSI ständig an die aktuellen Bedürfnisse anzupassen und das GSHB permanent weiterzuentwickeln.

Für die Realisierung des IT-Grundschutzes bietet das BSI mit dem Kooperationspartner Mummert das Softwarewerkzeug GS-Tool mittlerweile in der Version 3.1 an. Dem Anwender hilft es bei der Erstellung, Verwaltung und Fortschreibung von IT-Sicherheitskonzepten. Die gesamte Vorgehensweise nach GSHB wird durch das Tool von der Systemerfassung bis hin zur Zertifizierung nach IT-Grundschutz unterstützt. Zum Kennenlernen kann die Software in einer kostenlosen Probeversion von der Webseite des BSI heruntergeladen werden.

Für die gesamte Geschäftswelt ist ein funktionierender IT-Grundschutz unverzichtbar.

Lizenzen für Auditoren

Sichere IT ist ein Wettbewerbsfaktor. Die Umsetzung von IT-Grundschutz zeigt Kunden, Lieferanten und Partnern, dass die Organisation aktive Risikovorsorge betreibt. Um die Realisierung des IT-Grundschutzes nach außen hin glaubwürdig zu dokumentieren, wurde schon Anfang 2002 das Zertifizierungsschema zum IT-Grundschutz vorgestellt. Dieses sieht die drei Qualifizierungsstufen „Selbsterklärung Einstiegsstufe“, „Selbsterklärung Aufbaustufe“ und „IT-Grundschutz-Zertifikat“ vor.

Das 100. Grundschutz-Zertifikat hat Holger von Rhein, SRC GmbH, Bonn erworben.

IT-Grundschutz-Zertifikat

Der Erteilung eines IT-Grundschutz-Zertifikates geht eine Überprüfung durch einen lizenzierten Auditor voraus. Das Interesse am Lizenzierungsverfahren als IT-Grundschutz-Auditor ist erfreulich groß. Anfang 2002 wurden die ersten 20 Auditoren lizenziert, im September 2003 wurde der 100. Auditor (Foto oben) zugelassen. Darüber hinaus liegen mittlerweile 12 IT-Grundschutz-Selbsterklärungen vor, die ersten drei IT-Grundschutz-Zertifikate sind vergeben worden und weitere Zertifizierungen sind angekündigt.

3. Qualität amtlich beglaubigt: Zertifizierte IT-Produkte

Vertrauenswürdigkeit ist das entscheidende Kriterium für den Einsatz von IT-Produkten. Für IT-Verantwortliche ist es aber fast unmöglich, selbst die Sicherheitseigenschaften zu bewerten.

Der Hersteller allein tut sich schwer damit, glaubwürdig die Sicherheit seiner Produkte zu belegen. Er ist auf Referenzen oder unabhängige Tests angewiesen.

Diesen Nachweis der vertrauenswürdigen Realisierung von IT-Produkten schaffen die Evaluierung (Prüfung und Bewertung) und Zertifizierung. Diesem Verfahren liegen objektive Kriterien wie z. B. der Common Criteria (CC) Standard zugrunde. Es wird von neutralen Stellen wie dem BSI und akkreditierten Prüfstellen durchgeführt. Ziel der Zertifizierung ist es, IT-Produkte und -Systeme hinsichtlich ihrer Sicherheitseigenschaften transparent und vergleichbar zu bewerten.

Ob Smartcards, Betriebssysteme, Firewalls oder Produkte zur Datenübertragung – grundsätzlich zertifiziert werden können IT-Produkte unterschiedlichster Art (Software und/oder Hardware), sofern bei ihnen Sicherheitsfunktionen im Zusammenhang mit der

- Verfügbarkeit von Daten und Dienstleistungen,
- Vertraulichkeit von Informationen,
- Unversehrtheit / Integrität von Daten,
- Authentizität von Daten

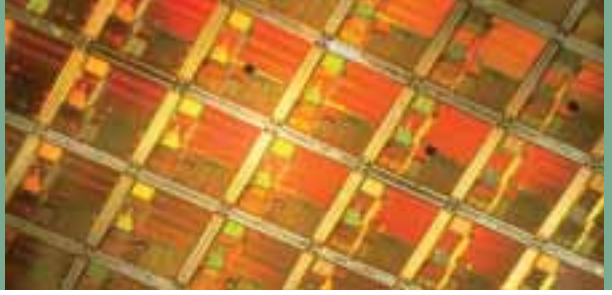
vorhanden sind. Anstoßen kann die Zertifizierung ein Hersteller, ein Händler oder eine Bundesbehörde als Anwender. Der Antrag wird bei der Zertifizierungsstelle des BSI eingereicht.

Die Common Criteria bieten Anwendergruppen und Herstellern die Möglichkeit, die jeweiligen Anforderungen für Produkt-/Systemklassen (z. B. Firewalls, Geldkarten, Betriebssysteme) in Schutzprofilen (Protection Profiles) festzulegen.

Schutzprofile geben Anwendern die Möglichkeit, ihre jeweiligen Sicherheitsanforderungen zu spezifizieren. Hersteller können so ihre Produktentwicklung gezielt am Kundenbedarf orientieren.

Die Evaluierung der Produkte wird in der Regel von akkreditierten und lizenzierten Prüfstellen durchgeführt. Alle beteiligten Stellen sind zur Wahrung der Vertraulichkeit von Firmengeheimnissen verpflichtet und garantieren durch vielfältige Maßnahmen die Einhaltung dieser wichtigen Voraussetzung.

Auch für Hard- und Software gelten internationale Standards.



Ein gemeinsames Logo

Neben dem BSI gibt es in Deutschland auch private Zertifizierungsstellen. Die Voraussetzungen für die Anerkennung der Zertifikate sind in bilateralen Verträgen geregelt. Die vom BSI anerkannten Zertifikate sind an dem gemeinsamen Logo „Deutsches IT-Sicherheitszertifikat“ erkennbar.

Stufenweise Sicherheit

In den Common Criteria sind Vertrauenswürdigkeitsanforderungen in hierarchisch angelegten Stufen (Evaluation Assurance Level - EAL) zusammengefasst. Es existieren insgesamt sieben Stufen, angefangen von geringen Anforderungen – Stufe 1 – bis hin zu den Anforderungen für den Einsatz im Bereich hochsensibler Daten auf der siebten Stufe. Mit wachsender Vertrauenswürdigkeit nehmen die Prüftiefe und der Aufwand natürlich zu.

Prüfverfahren bereits in der Entwicklungsphase

Die Länge des Verfahrens der Evaluierung und Zertifizierung kann – in Abhängigkeit von der Komplexität des Produkts und der angestrebten Evaluationsstufe – stark differieren. Bei einem PC-Sicherheitsprodukt sind i.d.R. drei Monate, bei einem mittleren Betriebssystem sechs bis neun Monate für eine Erstevaluierung anzusetzen. Die Evaluierung kann entwicklungsbegleitend erfolgen, so dass gleichzeitig mit dem Erscheinen des Produktes auf dem Markt das Zertifikat erteilt werden kann.

Ob dieses Timing eingehalten werden kann, hängt von der Qualität der beim Hersteller vorliegenden Entwicklungsmethodik und -dokumentation ab.

IT-Produkte sind meist für den weltweiten Markt bestimmt. Um die Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten zu vermeiden, können IT-Sicherheitszertifikate gegenseitig anerkannt werden. Hierzu sind folgende Vereinbarungen getroffen worden:

ITSEC und CC-Zertifikate

Das europäische Abkommen bezieht sich auf Zertifikate aller Evaluierungsstufen. Sofern eine Nation über keine eigene Zertifizierungsstelle verfügt, handelt es sich um eine einseitige Anerkennung. Alle vom BSI herausgegebenen Zertifikate werden europaweit anerkannt.

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, der gemeinsamen Zertifizierungsstelle Australiens und Neuseelands, Japan, Finnland, Griechenland, Italien, Niederlande, Norwegen, Spanien, Israel, Schweden, Österreich und Ungarn.

CC-Zertifikate basieren auf international abgestimmten Kriterien.

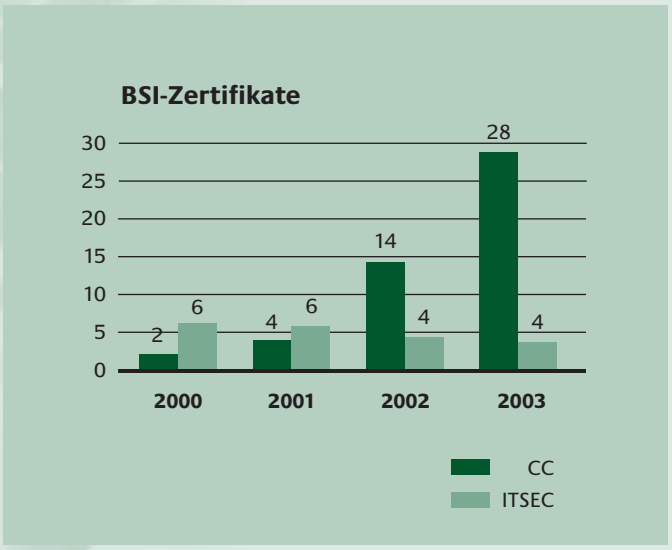
Im Rahmen der gegenseitigen Anerkennung wird auf die zertifizierten Produkte der anderen Zertifizierungsstellen hingewiesen bzw. diese werden mitveröffentlicht. Die zugehörigen Zertifizierungsreporte werden ausgetauscht. Darüber hinaus stimmen die Zertifizierungsstellen die gemeinsame Vorgehensweise regelmäßig untereinander ab.

Das BSI verfügt in diesem Bereich über einen großen Einfluss, weil es von Anfang an die Entwicklung der CC geprägt hat. Zudem liegen reichhaltige Erfahrungen mit Zertifizierungsverfahren vor. Diese resultieren nicht zuletzt aus den vielen an ausländische Hersteller ver-

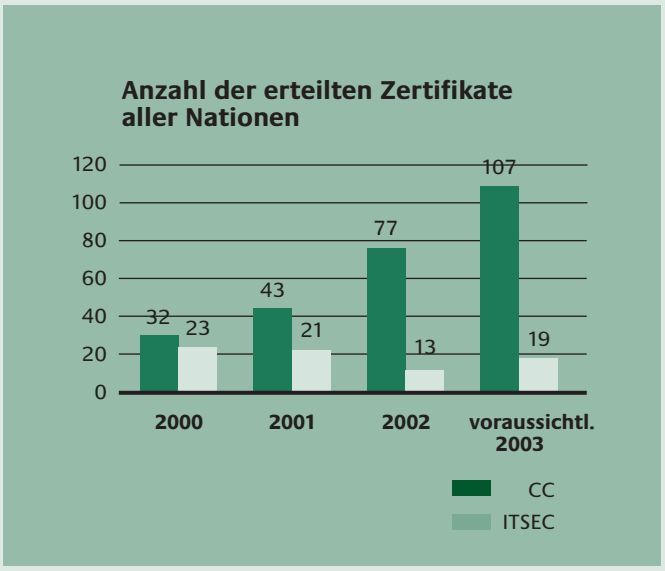
gebenen Zertifikaten und aus der aktiven Grundlagenarbeit, z.B. zur Evaluierung von Smartcards oder Zufallszahlengeneratoren.

Im internationalen Umfeld wird die Zertifizierung immer wichtiger. In den USA gilt seit Juli 2002, dass der Einsatz zertifizierter Produkte in der öffentlichen Verwaltung zwingend erforderlich ist. In Australien ist es vorgeschrieben, dass im Rahmen der Einführung von E-Government-Anwendungen zertifizierte Produkte eingesetzt werden müssen. In Frankreich kommen in öffentlichen wie privatwirtschaftlichen Bereichen nur zertifizierte Smartcard-Produkte zum Einsatz. Zunehmend werden für die öffentliche Verwaltung auch verschiedenste Systeme auf Basis der CC zertifiziert.

Diese neuen Impulse und die erfolgreiche Entwicklung lassen die Zertifizierung in Zukunft immer bedeutender für Hersteller und Anwender werden.



Das BSI zertifiziert IT-Produkte und IT-Systeme nach den internationalen Kriterien der Common Criteria (CC) oder den europäischen ITSEC.



2003 sind voraussichtlich fast ein Viertel aller Zertifikate weltweit durch das BSI vergeben worden.

Internationale Experten-Konferenz

Vom 7. bis zum 9.9.2003 fand die vierte ICCC (International Common Criteria Conference) statt. Sie ist die bedeutendste Konferenz der international anerkannten Common Criteria (CC) zur Bewertung von IT-Sicherheit. Mehr als 300 Experten trafen sich in Stockholm, um über die Anwendung und kontinuierliche Weiterentwicklung des Kriterienwerkes zu diskutieren.

Der Präsident des BSI, Dr. Udo Helmbrecht, überreichte auf der Konferenz insgesamt fünf durch das BSI ausgestellte CC-Zertifikate. Philips Semiconductors erhielt ein Zertifikat für den Smartcard Microcontroller SmartXA2.

Die belgische Firma Banksys konnte die Evaluierung ihres Hardware-Sicherheitsmoduls durch die Entgegennahme des Zertifikats erfolgreich abschließen. Neben der Microsoft Corporation, die ein Zertifikat für den Microsoft ISA Firewall Server erhielt, wurden der IBM Zertifikate für das Betriebssystem AIX 5.2 und den Directory Server überreicht.

Die Tatsache, dass auch große amerikanische Unternehmen das BSI als Zertifizierungsstelle wählen, macht einmal mehr deutlich, dass das internationale Abkommen zur Anerkennung von CC-Sicherheitszertifikaten wirksam und erfolgreich ist. Die nächste ICCC wird 2004 vom BSI in Berlin ausgerichtet.

4. Sicheres E-Government

Die Initiative BundOnline 2005 soll alle internetfähigen Dienstleistungen der Bundesverwaltung online zur Verfügung stellen. Das zwischen Bund, Ländern und Kommunen vereinbarte Projekt „Deutschland-Online“ zielt darauf ab, die Dienstleistungen aller Behörden schneller, einheitlicher und effizienter über das Internet zugänglich zu machen.

Damit eröffnet sich den Bürgern die Möglichkeit, rund um die Uhr an sieben Tagen in der Woche fast das gesamte Spektrum der Dienstleistungen online zu nutzen, sei es auf Bundes-, Landes- oder kommunaler Ebene. Der traditionelle Behördengang wird durch einen komfortablen Zugangsweg ergänzt.

Akzeptanz und Erfolg von E-Government-Dienstleistungen hängen essentiell von der Qualität und Benutzerfreundlichkeit der Kommunikation ab. Datensicherheit ist dabei das zentrale Qualitätsmerkmal.

Die Informations- und Kommunikationssicherheit gehört zum Aufgabenspektrum des Kompetenzzentrums Datensicherheit im BSI. Ende des Jahres 2002 wurde das Zentrum unter Einbeziehung der Firmen Secunet und Secartis eingerichtet. Anfang 2003 nahm es seine Servicetätigkeit auf.

Im Vordergrund der Arbeit stehen der Schutz der Vertraulichkeit der Daten, der Schutz vor unbemerkter Veränderung sowie die zuverlässige Identifikation des Urhebers. Das sind die primären Sicherheitsziele.

Im sicherheitsrelevanten Datenverkehr werden heute durchgängig Verschlüsselung, Signaturen und Zertifikate als kryptographische Mechanismen eingesetzt, die auf Public-Key-Verfahren beruhen. Sender und Empfänger verfügen hier jeweils über zwei Schlüssel. Der eine ist geheim und nur ihnen zugänglich. Frei zugänglich – z.B. über ein öffentliches Verzeichnis – ist der andere Teil des Schlüsselpaares.

Mit diesen beiden Schlüsseln ist es unter Mithilfe einer vertrauenswürdigen, dritten Partei möglich, drei Eigenschaften der Kommunikation sicherzustellen: Vertraulichkeit und Manipulationsfreiheit der Nachrichten sowie die Authentizität des Senders.

Um eine gesicherte Kommunikation zwischen Behörden und Bürgern, zwischen Behörden und Wirtschaft sowie zwischen Behörden untereinander über das Internet zu gewährleisten, wird derzeit die „Basiskomponente Datensicherheit“ durch das BSI entwickelt. Sie soll die elektronische Kommunikation der Behörden deutlich vereinfachen und vermeiden, dass Entwicklungs- und Implementierungskosten mehrfach aufgewendet werden müssen.

Garant für Datensicherheit: die virtuelle Poststelle (VPS)

Kernelement der Basiskomponente ist die Virtuelle Poststelle (VPS). Sie übernimmt die Abwicklung der sicheren, nachvollziehbaren und vertraulichen Kommunikation. Dabei wird sowohl die E-Mail- als auch die Web-basierte Kommunikation unterstützt. Die VPS stellt innerhalb der Behörde zentral Funktionen wie Ver- und Entschlüsselung, Signaturerstellung und -prüfung sowie Authentisierung zur Verfügung. Über offene Schnittstellen können weitere Systeme wie Virenscanner eingebunden werden. Neben der indirekten E-Mail-Kommunikation mit einer zentralen Adresse in den Behörden unterstützt die Basiskomponente auch eine strikte Ende-zu-Ende-Sicherheit mit einzelnen Sachbearbeitern. Die Anbindung externer Trustcenter an die VPS wird ebenfalls unterstützt.

VPS startete im Sommer 2003

Die erste Projektphase wurde im Frühjahr 2003 mit der Erstellung des Fachkonzeptes und des DV-technischen Grobkonzeptes durch IBM abgeschlossen. Mit der Realisierung der VPS wurde im Frühsommer 2003 begonnen. Für die Web- und Kernkomponente der VPS liegt der Fortent-

Fortsetzung auf S. 44

„Moderner Staat 2003“ – Am gemeinsamen Messestand von Secunet und BSI.

Die Firmen Secunet und Secartis sind Partner des BSI im „Kompetenzzentrum Datensicherheit“.

BundOnline 2005

Ämter gehen ins Internet

Bei der Initiative „BundOnline 2005“ sollen bis 2005 alle internetfähigen Dienstleistungen des Bundes online zur Verfügung stehen. Das BSI unterstützt mit einer Reihe von Aktivitäten die Umsetzung der Maßnahme, z.B. mit der „Virtuellen Poststelle“ oder dem Betrieb des „Kompetenzzentrums Datensicherheit“.

Wenn die Daten statt der Bürger laufen sollen, kommt es darauf an, dass sich keine Verwechselungen einstellen und Betrug ausgeschlossen ist. Bei vielen Behördengängen muss sich der Bürger sicher legitimieren können. Grundlage der Virtuellen Poststelle und eine der möglichen Lösungen in der Frage der elektronischen Unterschrift: die Legitimation via Chipkarte, die am heimischen PC in ein spezielles Lesegerät gesteckt wird.

Präsident Dr. Udo Helmbrecht erläutert Bundesinnenminister Otto Schily, wie eine Virtuelle Poststelle arbeitet.

wicklung das Produkt Governikus der Firma Bremen Online Services zugrunde, für die E-Mail-Kommunikation fiel die Wahl auf das Produkt „Julia“ der Firma ICC. Eine erste Version der VPS wird Anfang 2004 bei BundOnline-2005-Pilotanwendern lauffähig sein. Eine breit einsatzfähige Ausbaustufe, die wesentliche Teile des Konzepts umsetzt, soll im IV. Quartal 2004 verfügbar sein.

E-Government-Handbuch fortgeschrieben

Als methodische Basis stellt das BSI das E-Government-Handbuch zur Verfügung. Im Vordergrund stand 2003 erneut die Fortschreibung des Handbuches. So wurde der Phasenplan durch die Veröffentlichung der Phasen 5 (Realisierung und Test) und 6 (Einführung und Inbetriebnahme) fertiggestellt.
Der Phasenplan richtet sich an die E-Government-Koordinatoren in den Behörden und beschreibt Schritt für Schritt, wie eine Behörde E-Government einführen kann.

Leitfaden für Behörden

In Kooperation mit anderen Behörden konnten drei Module zu den Themen „Rechtliche Rahmenbedingungen für E-Government“, „Datenschutzgerechtes E-Government“ und „Leitfaden E-Shop“ für das Handbuch aufbereitet werden. Auch das im Auftrag der KBST (Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung) erstellte Dokument SAGA (Standards und Architekturen für E-Government-Anwendungen) konnte in der Version 1.1 ins Handbuch aufgenommen werden; das BSI unterstützt in diesem Zusammenhang aktuell die Fertigstellung der Version 2.0.

Barrierefreier Zugang

2003 sind zudem die Module „Sichere Integration von E-Government-Anwendungen (SIGA)“ und „Barrierefreies E-Government“ fertig gestellt worden. Ferner werden Module zu den Themen „Sichere Zahlungsverfahren für

Fortsetzung auf S. 46

E-Government geht einher mit dem Eingriff in bestehende Infrastrukturen der Informationstechnik. Für die Realisierung von E-Government-Dienstleistungen müssen bisher abgeschottete IT-Systeme der Verwaltung so über das Internet verfügbar gemacht werden, dass keine Sicherheitslücken auftreten. Für die Übertragung sensibler Daten über das Internet gilt es, vertrauenswürdige Infrastrukturen zu schaffen, Verwaltungsprozesse neu zu strukturieren und vorhandene Anwendungen der Behörden mit geeigneten Sicherheitslösungen auszustatten. Das E-Government-Handbuch des BSI stellt mit seinem umfassenden Ansatz Instrumente für Analyse, Konzeption und Reorganisation der Prozesse gleichermaßen zur Verfügung wie für die Neubewertung der Themenfelder Datenschutz, IT-Sicherheit und Schutz der elektronischen Kommunikation. Damit wird eine reibungslose, rechtsverbindliche und vertrauliche Online-Kommunikation von Bürgerinnen und Bürgern und der Wirtschaft mit der Verwaltung ermöglicht und eine sichere innerbehördliche Kommunikation gewährleistet.

Den Umzug online anmelden

E-Government“ und „Sichere Client-Server-Architekturen für E-Government" über die Jahreswende hinaus bearbeitet.

Neues zum Thema E-Government

Das E-Government-Handbuch kommt parallel in drei Fassungen heraus. Die Erstveröffentlichung erfolgt stets im Rahmen des BSI-Web-Auftritts „Sicheres E-Government“, der von der Projektgruppe kontinuierlich aktualisiert wird. An gleicher Stelle erscheinen zeitversetzt englische Übersetzungen der wichtigsten Module. Schließlich veröffentlicht der Bundesanzeiger Verlag das Handbuch als Loseblattsammlung; 2003 sind zwei Ergänzungslieferungen hinzugekommen.

Wachsender E-Mail-Verteiler

Direkten Kontakt zu den Anwendern hält das BSI in erster Linie über E-Mail-Rundbriefe, in denen das Amt auf neue Veröffentlichungen, Veranstaltungen und Ausschreibungen hinweist. Mehr als 1200 Personen haben sich bereits als Nutzer registrieren lassen. Fast täglich kommen neue Leser dazu. Über die Beratungsprojekte des „Kompetenzzentrums Datensicherheit“ schließlich erhält das BSI wertvolles Feedback über die Umsetzungspraxis.

Spart Nerven und Geld: Elektronische Kommunikation mit der Verwaltung von zu Hause aus.

Der Bund liegt im Plan

Knapp 260 der nach letztem Stand 449 für internetfähig befundenen Dienstleistungen des Bundes waren Ende 2003 im Netz. „BundOnline 2005“ hat zum Ziel, bis Ende 2005 alle entsprechenden Dienstleistungen des Bundes online zur Verfügung zu stellen.

Das Bundesinnenministerium rechnet mit Einsparungen von 400 Millionen Euro pro Jahr an Verwaltungskosten, wenn der Plan erfüllt ist. So versteigert bereits heute der Zoll sichergestellte Gegenstände unter *www.zoll-auktion.de*. Online lassen sich Patente anmelden, Anträge auf BAföG-Rückzahlungen stellen, und auch das Auswärtige Amt nimmt Bewerbungen für den höheren Dienst via Internet-Formular entgegen. Was genau online möglich ist, lässt sich im Fortschrittsanzeiger unter *www.bundonline2005.de* nachschlagen.

Fortschrittsanzeiger BundOnline 2005

Realisierte Dienstleistungen	bis 2002	2002	2003	insgesamt
Bereitstellungen von Informationen	21	99	38	158
Beratung	0	6	3	9
Vorbereitung von politischen Entscheidungen	0	0	1	1
Zusammenarbeit mit Behörden	2	6	9	17
Antragsverfahren	1	11	10	22
Förderungen	1	1	4	6
Beschaffungsvorhaben	0	1	5	6
Durchführung von Aufsichtsmaßnahmen	0	4	4	8
Sonstige Dienstleistungen	5	12	12	29
Dienstleistungen insgesamt	**30**	**140**	**86**	**256**

Stand: 17.12.2003

Zukunft

Anschluss gefunden: Wer sich an das BSI wendet, bewegt sich bei der IT-Sicherheit im Trend.

1. Wissen, was kommt: Trends
2. Mobile Kommunikation
3. Verschlüsselungstechnik
4. Der Mensch in Bits & Bytes: Biometrie
5. Schutz Kritischer Infrastrukturen

Der Blick in die Zukunft

Wer an der Geschichte der Zukunft mitschreiben will, muss sich schon jetzt an der Spitze der technischen Entwicklung bewegen. Wenn es um IT-Sicherheit geht, ist das BSI an den wesentlichen Zukunftstrends maßgeblich beteiligt.

Zwar kann niemand die Zukunft exakt voraussagen, doch Prognosen erlauben zumindest Annäherungswerte und lassen Wahrscheinlichkeiten erkennen. Wer davor die Augen verschließt, kann Gefährdungslagen nicht rechtzeitig erkennen.

Die drahtlosen Kommunikationssysteme, die bereits dabei sind, sich überall durchzusetzen, bieten für den Nutzer große individuelle Freiheiten, bergen aber auch Gefahren. Funknetze sind leichter anzugreifen und schwerer zu schützen. Das BSI beschäftigt sich intensiv mit der „mobile security“ und ist dabei, Schwachstellen zu finden und technische Standards für die drahtlose Kommunikation aufzustellen.

Leistungsfähige Verschlüsselungssysteme werden nicht nur für diese Art der Kommunikation gebraucht. Eine der Aufgaben des BSI besteht darin, moderne kryptographische Systeme für den Austausch sensitiver Informationen im Bereich der Bundesverwaltung und der Sicherheitsbehörden zur Verfügung zu stellen.

Staat, Wirtschaft und Gesellschaft müssen sich darauf verlassen können, dass die Informationstechnik auch in Krisenzeiten funktioniert. Der Schutz Kritischer Infrastrukturen – Energie, Gesundheit, Rettungswesen — ist eine Herausforderung, der sich das BSI mit der Erarbeitung eines „Nationalen Plans zum Schutz IT-abhängiger Kritischer Infrastrukturen“ stellt.

1. Wissen was kommt: Trends

Was sind die entscheidenden Entwicklungen, die unsere Wirtschaft und Gesellschaft zukünftig verändern und bestimmen? Welche Technologien prägen unser Leben in den nächsten zehn Jahren?

In der sich rapide entwickelnden Informationstechnik reicht es nicht aus, bestehende Systeme genau zu kennen. Bei Gefährdungslagen ist es wichtig, schnell und kompetent reagieren zu können. Zukünftige Ereignisse müssen anhand von Prognosen bereits möglichst früh und präzise vorhergesagt werden, um in kritischen Situationen darauf vorbereitet zu sein.

Mit Hilfe von unterschiedlichen Prognoseverfahren (quantitativ/qualitativ) wird eine Aussage zur Wahrscheinlichkeit zukünftiger Entwicklungen ermittelt. Ein Ausgangspunkt von Trendanalysen können die zyklischen Gesetzmäßigkeiten der Konjunkturtheorie sein. Neben anderen kurz- und mittelfristigen Schwankungen folgen nach der Theorie von Kondratieff langfristige Wellen in einem Zeitraum von etwa 50 bis 60 Jahren aufeinander. Auslöser für diese langen Zyklen sind bahnbrechende Innovationen wie die Dampfmaschine oder die Elektrizität und in jüngster Vergangenheit eben die Informationstechnologie. Derartige Innovationen treten nicht kontinuierlich, sondern nur phasenweise auf und stoßen so Konjunkturwellen an.

„Planetengetriebe“ für miniaturisierte Motoren mit hoher Drehzahl. Solche Nanomotoren kommen u.a. in Minidisc-Playern und in der Chirurgie zur Anwendung.

Die Jahre des Booms in der Kommunikations- und Informationstechnik (IuK-Technik) neigen sich heute dem Ende zu. Wir befinden uns zu Beginn des 21. Jahrhunderts in einer Abschwungbewegung, d.h. der Zenit des fünften Kondratieff-Zyklus ist bereits überschritten. Der Übergang von einem Konjunkturzyklus zum nächsten ist stets mit einer starken Instabilität der Weltwirtschaft verbunden.

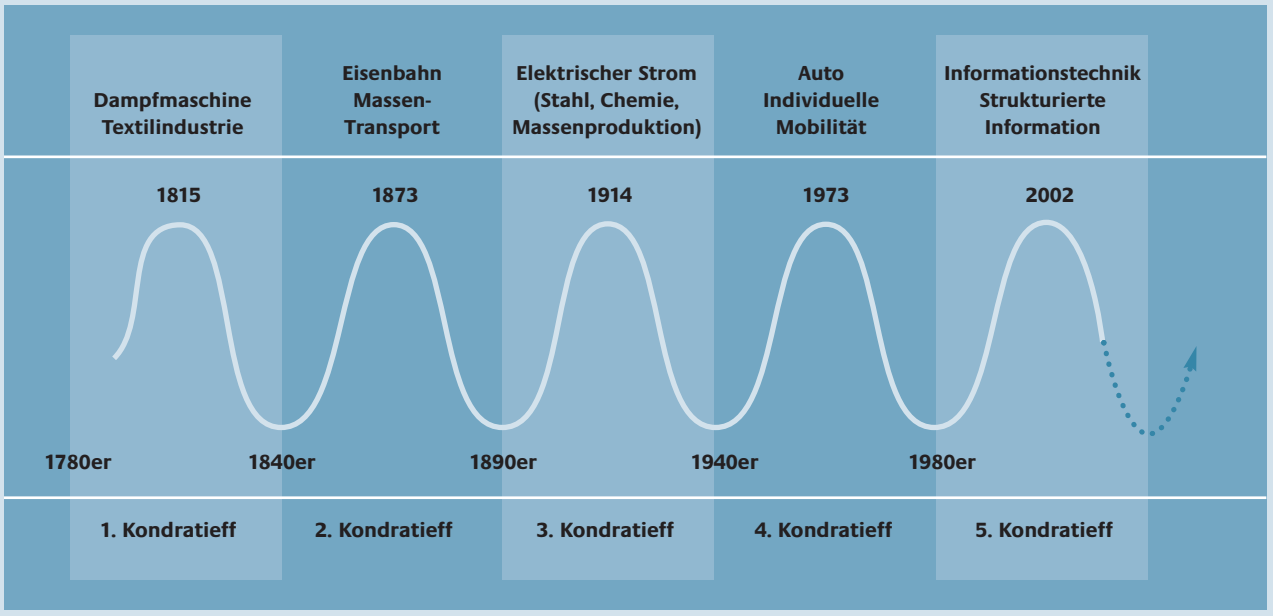
Insgesamt sind die fünf Kondratieff-Wellen durch folgende bahnbrechende Erfindungen gekennzeichnet:

- Dampfmaschine/Baumwolle (1793 – 1847)
- Stahl/Eisenbahn (– 1893)
- Elektrotechnik/Chemie (– 1939)
- Petrochemie/Automobilbau (– 1984)
  und
- derzeit die IuK-Technik.

All diese Erfindungen lösten in der Weltwirtschaft einen enormen Aufschwung aus. Die IuK-Technik allein reicht heute nicht mehr aus, die zukünftigen gesellschaftlichen Anforderungen und Bedürfnisse der Menschen zu bewältigen. Es wird eine weitere Basisinnovation folgen müssen, die wiederum große weltwirtschaftliche Wirkungen auslöst und auf lange Sicht unsere Gesellschaft konjunkturell wesentlich verändert.

Konjunkturzyklus nach Kondratieff

Die Weltwirtschaft bewegt sich in kurz-, mittel- und langfristigen Konjunkturzyklen. Für das BSI sind von besonderem Interesse die ca. 50-60 Jahre dauernden langen Zyklen nach der Theorie von N. D. Kondratieff (1926). Sie werden ausgelöst durch entscheidende Innovationen, wobei sich in der heutigen Zeit die Wellenlänge zunehmend verkürzt. Der wiederkehrende Verlauf erlaubt eine Prognose kommender Wirtschafts- und Technologieentwicklungen.



Welcher Trend bestimmt den sechsten Zyklus?

Über den nächsten langfristigen, den sechsten Kondratieff-Zyklus besteht in der Trendforschung noch keine abschließende Einigkeit. Die Diskussion beherrschen derzeit folgende Themen:

- Allgegenwärtige Informationsnetze,
- Miniaturisierung – Mikrosystemtechnik und Nanotechnologie,
- Nanorobotik, Quantencomputer,
- Biotechnologie, Medizintechnik, Gentechnologie,
- Optische Technologie,
- Umwelt, Energietechnologie,
- Gesundheit, Bildung und vernetztes Wissen.

Welche dieser Basisinnovationen bestimmt das Tempo und die Richtung der Weltwirtschaft entscheidend über mehrere Jahrzehnte? Führt sie zu einem kräftigen Wachstumsprozess der gesamten Wirtschaft?

Baustein für die Zukunft: IuK-Technik

Die Weiterentwicklung der IuK-Technik wird sicher ein Baustein dieses Prozesses sein. In Verbindung mit der Bio- und Nanotechnologie wird sie vielleicht den nächsten High-Tech-Boom auslösen. Prognosen spezifischer technologischer IuK-Entwicklungen und die Identifikation neuer Anwendungsgebiete sind deshalb von ganz erheblicher Bedeutung.

In der neuesten Trendstudie des BSI werden gerade die besonders relevanten Entwicklungen auf den Gebieten der IuK-Technologien intensiv diskutiert.

Die Studie gliedert sich in die vier Technologiebereiche:

- Rechnertechnik, Rechnernetze und -kommunikation, Softwaretechnik,
- Datenbanken und Wissensmanagement,
- Anwendungsbereiche,
- Sicherheitstechnologien.

Was wird die Schlüsseltechnologie

für das 21. Jahrhundert?

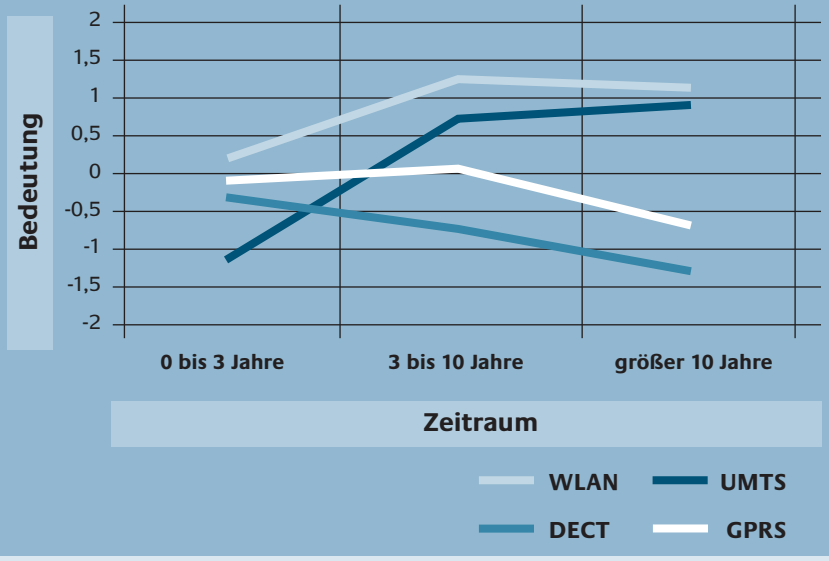
Ein Kandidat ist die Biotechnologie.

Für diese Bereiche werden übergreifende Trends – etwa Konvergenz, Komplexität und Mobilität – einbezogen und analysiert. Spezifische technologische Betrachtungen, Analysen der Triebkräfte und übergreifende Untersuchungen der Zusammenhänge erklären das Geschehen. Als Ergebnis zeichnet sich ein deutliches Bild der zukünftigen Trends ab.

Eines ist schon sicher: Egal, welches die nächste Schlüsselinnovation sein wird, wieder werden neben den neu erschlossenen wirtschaftlichen und gesellschaftlichen Potenzialen mögliche Sicherheitsrisiken die Diskussion beherrschen. Die Trendanalysen geben heute schon Aufschluss darüber, wie die Antworten aussehen könnten.

Das BSI verfolgt aufmerksam die Entwicklungen in der Informationstechnologie und die bestimmenden Faktoren für zukünftige Ereignisse. Informationen zu neuesten Trends bietet die 2003 veröffentlichte Studie „Kommunikations- und Informationstechnik 2010+3“: Neue Trends und Entwicklungen in Technologie, Anwendungen und Sicherheit.

Bedeutung von Übertragungstechnologien für IP-basierte Anwendungsprotokolle im Bereich der Mobilkommunikation



Mobile Kommunikation

Mit der Anzahl von mobilen Anwendungen steigt die Bedeutung insbesondere breitbandiger IP-basierter Übertragungstechnologien wie WLAN oder UMTS.

(Expertenbefragung des BSI im Jahre 2002 unter Berücksichtigung von 185 Fragebögen)

2. Mobile Kommunikation

Nach der weltweiten Vernetzung der Wirtschaftsregionen haben mobile Anwendungen ihren Siegeszug angetreten. Die zugehörigen Endgeräte – wie Laptops, PDAs, Organizer oder Handys – sind bereits heute ein wichtiger Bestandteil des alltäglichen Lebens.

Die Verfügbarkeit immer kleinerer und leistungsfähigerer Produkte trägt ihr Übriges dazu bei, dass drahtlose Kommunikationssysteme zur Selbstverständlichkeit werden. Die neu gewonnene Freiheit birgt allerdings auch Risiken. Durch den Einsatz im privaten und im geschäftlichen Umfeld steigt mit der Menge an zeitkritischen oder sensiblen Daten die Verwundbarkeit. Die Bedeutung von sicheren Internet- und Mobilfunkdiensten wächst daher kontinuierlich.

Die Parameter für die IT-Sicherheit ändern sich durch die rasche technische Entwicklung ständig. Über zellulare Mobilfunknetze (GPRS, UMTS), stationäre LANs und WLANs, Satelliten-Netzwerke oder über Telefon-Netze können heute die Geräte mit anderen Komponenten in einer verteilten Umgebung kommunizieren. Zusammen bilden sie ein weltumspannendes, mobiles System. Dabei wurden für die mobilen Endgeräte spezielle Standards für Applikationsprotokolle entwickelt. Sie ermöglichen den Zugriff auf Internetdienste wie E-Mail, das Surfen sowie das Herunterladen von aktiven Inhalten bereits für sehr kleine mobile Geräte.

In offenen Netzen — wie z.B. dem Internet — bestehen viele Sicherheitsrisiken. Bei den mobilen Anwendungen kommen noch einige spezifische Gefahrenmomente hinzu. Das sind zunächst die Schwachstellen, die sich aus den charakteristischen Eigenschaften der kleinen mobilen Endgeräte ergeben. Dazu gehört zunächst die Portabilität an sich: Kleine, leichte Endgeräte erleichtern einerseits Diebstahl und Verlust, können andererseits aber auch zum unbemerkten Aufzeichnen und/oder Abhören von Gesprächen missbraucht werden.
Die mobilen Geräte bringen oft nur beschränkte Ressourcen mit. Dadurch bestehen Risiken im Softwarebereich, z.B. durch das Nachladen von schädlichem Code oder den reduzierten Aufwand für Sicherheitskontrollen. Die Personalisierung des Gerätes lässt die Erstellung von sicherheitskritischen Nutzungsprofilen zu, und Bewegungsprofile können erfasst werden.

Aus den drahtlosen Zugangsnetzen resultieren zusätzliche Risiken, beispielsweise durch leichteres Abhören unverschlüsselter Verbindungen. Die Liste der Gefahren ist lang und ließe sich noch erweitern, zum Beispiel um die Gefahr der Ausschaltung der Verschlüsselung oder um das Risiko von unberechtigten Zugriffen auf Netze.

Wegen dieser Schwachstellen kommt der IT-Sicherheit eine zentrale Bedeutung zu. Aufgrund des Zugriffs mobiler Endgeräte auf mobile und verteilte Infrastrukturen spricht

man auch von „mobile security“. Der erste Schritt vor dem Aufbau einer sicheren mobilen Infrastruktur ist die Erstellung eines umfassenden Sicherheitskonzeptes, das durchgängig alle mobilen Plattformen erschließt – vom PDA bis zum Telearbeitsplatz. Hierzu gehören beispielsweise die Analyse der Sicherheitsrisiken und Abwehrmaßnahmen. Zur Sicherstellung der Vertrauenswürdigkeit mobiler Applikationen müssen folgende grundlegende Anforderungen erfüllt sein:

- Vertraulichkeit der Daten,
- Authentizität der Akteure,
- Datenintegrität,
- (Rechts-) Verbindlichkeit,
- Verfügbarkeit des Systems,
- digitales Rechte-Management.

Das BSI beschäftigt sich intensiv mit den aufgeworfenen Fragestellungen. Zu nennen sind folgende Aktivitäten der „mobile security“ in drahtlosen Netzen:

- Erarbeiten von Grundlagenwissen über Standards, Netzaufbau und Funktionsweise,
- Aufbau von eigenen Netzen für Untersuchungszwecke,
- Analyse von Schwachstellen und Methoden des Angriffs auf drahtlose Netze,
- Beschaffung, Entwicklung, Modifikation und Analyse von Angriffs-Demosystemen in Soft- und Hardware.

Die Systemuntersuchungen finden im Labor oder in Feldversuchen statt. So erfolgen Risikoanalysen für die aktuellen Standardversionen der drahtlosen Kommunikationssysteme WLAN 802.11x, Bluetooth, DECT, HomeRF, HiperLAN/2, ZigBee, drahtlose Tastaturen und Mäuse, IrDA.

Die gewonnen Erkenntnisse fließen direkt in die Erstellung von Informationsschriften, in die Beratungstätigkeit bzw. in die Formulierung von technischen Richtlinien und Prüfvorschriften ein. Sie helfen zudem der öffentlichen Verwaltung und der Wirtschaft bei der Auswahl von mobilen Systemlösungen. Die Entwicklung von technischen Richtlinien (TRn) sowie die darauf aufbauende Entwicklung von Prüfverfahren von Produkten ist ein in 2003 neu im BSI umgesetztes Arbeitsgebiet. Schließlich entwickelt das BSI selbst Werkzeuge, um Angriffe zuverlässig erkennen zu können und zu verhindern.

Bequem vom Sofa aus mit einem schnurlosen Surfterminal.

Projekte 2003

LWC (Local Wireless Communication)

Im Rahmen des Projektes wurde die Sicherheit der drahtlosen lokalen Kommunikationssysteme (WLAN 802.11x, Bluetooth, DECT, HiperLAN/2, HomeRF, Zigbee, drahtlose Tastaturen und Mäuse sowie IrDA) untersucht. In Informationsbroschüren sowie Veröffentlichungen und Vorträgen wurden die Ergebnisse einem breiten Publikum vorgestellt. Praktische Angriffsdemonstrationen führten den Zuschauern die Risiken plastisch vor Augen. Die entwickelten Gegenmaßnahmen und die erarbeiteten Grundlagen für die technische Richtlinie für WLANs sind Basis für mehr Sicherheit in drahtlosen Kommunikationssystemen.

MDS (Modulares Funk-Detektions-System)

Grundlage für dieses Projekt sind die bisherigen Untersuchungen von vernetzten Mobilfunkdetektoren. Sie dienen der Erkennung des Abhörens von Raumgesprächen mittels GSM-Mobilfunktelefonen. In der Machbarkeitsstudie werden darauf aufbauend die technischen Möglichkeiten der Funküberwachung auch für die Funkstandards UMTS, DECT, WLAN und Bluetooth analysiert.

TRC-DigID (Technische Richtlinien für die Chipkartenplattform im Bereich Digital-IDs)

Zum Schutz der Mobilität von Menschen (Zutrittskontrolle, Zeiterfassung, sicherer mobiler Rechner-/Netzzugang u.v.m.) kommt der Chipkarte eine besondere Bedeutung zu. Damit die Chipkarten sicher, interoperabel und vielfältig einsetzbar sind, verfolgt dieses Projekt das Ziel, einen einheitlichen, technischen Standard für unterschiedliche Anwendungsprofile zu schaffen.

TR-S-WLAN (Technische Richtlinie Sicheres WLAN)

In der TR des BSI werden konkrete Handlungsempfehlungen für die Planung, Beschaffung, Installation, Konfiguration, Abnahme, Administration und Außerbetriebnahme von sicheren WLANs zusammengefasst. Damit kann der notwendige Einkauf von Expertenwissen für die Beschaffung und Abnahme sicherer Systeme in Behörden und kleinen und mittleren Unternehmen deutlich reduziert werden.

SME (Sicherheit mobiler Endgeräte)

Im Rahmen einer einjährigen Studie wird untersucht, inwieweit mit den heutigen technischen Möglichkeiten mobile Endgeräte unter Sicherheitsaspekten in unternehmensweite Geschäftsprozesse eingebunden werden können.

Mobilität — mit Sicherheit

Die Zukunft der mobilen Anwendungslösungen hängt zum einen von der Bewältigung der Sicherheitsprobleme ab. Zum anderen kommen ökonomische, gesellschaftliche und politische Faktoren hinzu — wie tragfähige Geschäftsmodelle, einheitliche Standards, Amortisation der Infrastruktur, Stückkosten, Preise, gesellschaftliche Akzeptanz neuer mobiler Dienste sowie politische und rechtliche Rahmenbedingungen.

Das BSI arbeitet aktiv an der Lösung von Sicherheitsproblemen im Bereich der mobile security, damit dem Bedürfnis nach Mobilität und Sicherheit in Zukunft gleichermaßen Rechnung getragen werden kann.

Ob am Strand, im Wohnzimmer oder unterwegs im Zug — die kabellose Datenkommunikation zwischen IT-Geräten ist auf dem Vormarsch.

3. Verschlüsselungstechnik

Der steigende Austausch sensitiver Informationen im Bereich der Bundesverwaltung, der geheimschutzbetreuten Industrie, aber auch der Sicherheitsbehörden wie Polizei, Nachrichtendienste und des Militärs erfordert leistungsfähige Verschlüsselungssysteme.

Sie müssen höchste Sicherheitsansprüche erfüllen und trotzdem genügend Bandbreite für moderne Anwendungen bereitstellen. Die leistungsfähigen kryptographischen Systeme des BSI genügen beiden Anforderungen.

Bei ihrem Einsatz können Unbefugte weder Kenntnis der Rohdaten erhalten noch sie unbemerkt manipulieren. Grundlage der Aktivitäten ist das Kryptoinnovationsprogramm des BSI vom Frühjahr 2003.

Zentrales Thema ist die langfristige Versorgung der Kunden mit innovativen Kryptosystemen für die wichtigsten IT-Anwendungen im Bereich der Hochsicherheit.
Strategische Ziele des Kryptoinnovationsprogrammes sind:

- Zeitnahe Berücksichtigung technologischer Trends,
- Verkürzung der Entwicklungs- und Planungszeiten,
- Umsetzung der Entwicklungskonzepte,
- Reduktion der Anschaffungs-, Betriebs- und Folgekosten für den Anwender,
- Nachhaltige Förderung des kryptographischen Know-hows in Deutschland.

Das Kryptoinnovationsprogramm schafft einen Handlungsrahmen für eine nachhaltige Versorgung sicherheitskritischer Bereiche in Deutschland mit wirksamen und vertrauenswürdigen Systemen.

Die Verschlüsselungssysteme des BSI kommen weltweit zum Einsatz. Auch in den deutschen Botschaften in Prag (Tschechien), Maskat (Oman) oder Tiflis (Georgien) sichert Elcrodat 6-2 den Datenverkehr auf ISDN-Basis für den weltweiten Austausch von sensitiven Informationen auf dem höchsten Sicherheitsniveau (v.l.n.r.).

Die wichtigsten Produkte und Aktivitäten des BSI sind:

Elcrodat 6-2

Gemeinsam mit dem Partner Rohde & Schwarz hat das BSI dieses Kryptosystem für den Telefon- und Datenverkehr auf ISDN-Basis entwickelt. Durch Elcrodat 6-2 können die Verschlüsselungsfunktionen sehr kostengünstig für viele Telekommunikationsanlagen in einfacher Weise genutzt werden. Eine zur Verfügung stehende Public Key Infrastruktur (PKI) entlastet den Kunden vollständig bei der Versorgung des Systems mit Schlüsselmitteln.

Zwischenzeitlich kommt das Kryptosystem bei deutschen Sicherheitsbehörden weltweit zum Einsatz. Darüber hinaus wird der Telefon- und Datenverkehr der am IVBB (Informationsverbund Berlin–Bonn) beteiligten Behörden durch das Kryptosystem Elcrodat 6-2 erstmals bei Bedarf verschlüsselt.
Weitere Organisationen im In- und Ausland, so zum Beispiel NATO und Europäische Union, haben bereits starkes Interesse bekundet und wollen zukünftig ihre Kommunikation durch das Elcrodat 6-2 schützen.

Sichere Inter-Netzwerk Architektur (SINA)

Die SINA-Architektur hat das BSI in Kooperation mit Secunet realisiert. SINA bildet die Grundlage für die Übertragung und Verarbeitung von Verschlusssachen in lokalen Netzen (LAN) über ein durch Verschlüsselung gebildetes virtuelles Netz. Dieses VPN-Verfahren (Virtual Private Network) kann auch für die Nutzung des Internets eingesetzt werden. Damit können mit SINA erstmalig Verschlusssachen kryptographisch gesichert über das Internet übertragen werden. Zusätzlich können kostspielige materielle Absicherungen an den Leitungswegen und bei den Arbeitsplätzen weitgehend entfallen. Schließlich verkürzen und beschleunigen sich die Verteilwege für Verschlusssachen erheblich.
Durch den Einsatz im Internet werden außerdem hohe Kosten für Miet- und Wählleitungen eingespart bei gleichzeitig deutlich höherer Übertragungsbandbreite. Ein weiteres Novum für derartige Systeme ist der Einsatz des Open Source Betriebssystems LINUX in einer speziell gehärteten Variante. Damit werden nicht nur Abhängigkeiten von Herstellern reduziert, sondern gleichzeitig Kosten eingespart.

Kryptosystem für digitale BOS-Funknetze

Für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) soll der flächendeckende Einsatz eines BSI-Verschlüsselungssystems im künftigen digitalen BOS-Funknetz als national einheitliche Lösung erfolgen. Mit der Bereitstellung dieses Verschlüsselungssystems wird

Fortsetzung auf S. 62

Blick auf das Frankfurter Bankenviertel — auch Kreditinstitute brauchen eine sichere Verschlüsselungstechnik.

Sichere Netzwerk-Architektur

Das SINA-Kryptosystem bildet ein geschlossenes und sicher verschlüsseltes Netzwerk (VPN) innerhalb einer Organisation oder über Ländergrenzen hinweg. Damit können als geheim eingestufte Informationen auch über das ansonsten unsichere Internet gesendet werden.

Die vom BSI entwickelte IT-Architektur zur Verarbeitung von hoch schützenswerten Informationen in unsicheren Netzen arbeitet mit der Kombination von Thin-Client/Server Verarbeitung und Virtual Private Network (VPN)-Technologie. Mit SINA können flexible, hochsichere Systemlösungen realisiert werden. So sind sämtliche Auslandsbotschaften über SINA vernetzt. Die Hardware-Variante der SINA-Box erhielt die Klassifizierung „streng geheim“.

Auf der Messe „Moderner Staat“ im November 2003 in Berlin wurde auf dem gemeinsamen Stand der Firma Secunet und des BSI dem Fachpublikum demonstriert, wie SINA arbeitet.

der Schutz der Funkkommunikation gegen Mit- bzw. Abhören national und grenzüberschreitend erfüllt. Eine flexible und kostengünstige Adaption an moderne Endgeräte ist mit dem Einsatz der Verschlüsselung auf Smartcard-Basis gewährleistet. Die Karte übernimmt alle kryptographischen Funktionen und kann einfach an existierende Endgeräte angepasst werden. Über eine PKI erfolgt die Schlüsselversorgung. Mit der Sicherheitskarte – adaptiert an Endgeräte der Firmen Motorola und Nokia – wurde im TETRA-Versuchsnetz Aachen die Ende-zu-Ende-Verschlüsselung erfolgreich nachgewiesen.

Bis Ende 2004 soll die Sicherheitskarte an TETRA, TETRAPOL- und GSM-BOS Endgeräte und Systeme angepasst werden. TETRA, TETRAPOL und GSM-BOS sind diejenigen digitalen Funksysteme, die als Kandidaten für das künftige digitale BOS-Funknetz von den BOS ermittelt wurden.

Realisierung kundenfreundlicher Kryptosysteme

Zur Unterstützung der Ziele des Kryptoerneuerungsprogramms werden moderne kryptographische Mechanismen benötigt, wie zum Beispiel effiziente Public-Key-Protokolle oder hochperformante Verschlüsselungsalgorithmen. Sie werden für den Einsatz speziell im staatlichen Hochsicherheitsbereich benötigt. Das Design und die Analyse dieser Algorithmen werden deshalb vom BSI anwendungsorientiert für diverse Projekte fortgeführt. Hierzu gehören spezielle schmalbandige Protokolle für Satellitensysteme wie Terra SAR und SAR Lupe oder das Design eines kryptographischen Verfahrens. Da Anwendungen zur digitalen Signatur zudem auch im nicht-staatlichen Bereich zunehmend an Bedeutung gewinnen, untersucht das BSI regelmäßig die Sicherheit der verschiedenen Verfahren. Bei Bedarf schlägt das BSI entsprechende Änderungsempfehlungen für die Parametergrößen und Rahmenbedingungen vor.

Um die Eignung von Signaturverfahren zu beurteilen, kooperiert das BSI auch mit Forschern der Universität Bonn. Das Ergebnis der diesjährigen Prüfung ist ein neuer Faktorisierungsweltrekord, der im April veröffentlicht wurde. Es wurde eine 160 Dezimalstellen große ganze Zahl, von der man wusste, dass sie das Produkt von zwei Primzahlen ist, in ihre Primfaktoren zerlegt. Zahlen dieses Typs sind die Basis z.B. für das RSA-Verschlüsselungsverfahren.

Zur Unterstützung der strategischen Ziele des Kryptoerneuerungsprogramms ist eine flexible aber dennoch sichere Plattform als kryptographisches Hardwaremodul notwendig. Die notwendigen konzeptionellen Arbeiten wurden vorangetrieben. Parallel wurden für weniger sicherheitskritische Anwendungsumgebungen schon Beispielimplementierungen von Kryptomechanismen auf den Chips vorgenommen. Um die effiziente Realisierung von sehr komplexen Public Key Kryptoalgorithmen auf den Modulen zu demonstrieren, wurde ein neuer Elliptic-Curve-Kryptokoprozessor in rekonfigurierbarer Hardware entwickelt.

Sichere PC-Nutzung

In Zusammenarbeit mit der INFINEON AG hat das BSI den Verschlüsselungschip PLUTO entwickelt. Dieser Kryptobaustein setzt hinsichtlich Sicherheit und Leistungsumfang neue Maßstäbe: auf einem Chip sind alle benötigten Grundfunktionen wie Ver-/Entschlüsselung, Authentisierung und Schlüsselerzeugung und -management vereinigt. PLUTO enthält Funktionsmodule für sowohl symmetrische als auch asymmetrische kryptografische Verfahren und Protokolle. Auf Grund der hohen Performance von bis zu 2 GBit/s Verschlüsselungsleistung existieren vielfältige Einsatzmöglichkeiten für PLUTO. Derzeit konzentriert sich der Einsatz des PLUTO-Chips auf die Hochsicherheitsvarianten der SINA Lösungsfamilie in Verbindung mit einer von der Firma Rohde & Schwarz entwickelten Kryptokarte mit der Bezeichnung PEPP-1.

4. Der Mensch in Bits & Bytes: Biometrie

Elektronische Verfahren zur Identitätssicherung und -überprüfung – oder kurz biometrische Systeme – erfassen einzigartige Merkmale des Menschen. Sie machen diese für Maschinen erkenn- und unterscheidbar. Diese zukunftsweisende Technologie bietet neue Ansatzpunkte für die Steigerung der Inneren Sicherheit.

Ob es sich nun um lasergestützte Irisscanner oder temperaturüberwachte Fingerprintsysteme handelt: Die Liste der heute schon entwickelten Technologien ist vielfältig und lang. Einige der biometrischen Verfahren bieten spezifische Vorteile, manche bringen aber auch grundsätzliche Einschränkungen mit sich.

Zu prüfen sind beispielsweise Fragen wie: Welches Verfahren eignet sich für welchen Zweck? Wie müssen die rechtlichen und organisatorischen Rahmenbedingungen gestaltet sein?

Für das BSI besteht die Kernaufgabe darin, biometrische Verfahren unter IT-sicherheitstechnischen Aspekten zu analysieren und an internationalen Standardisierungsverfahren mitzuwirken. In umfangreichen Erprobungstests sollen die konkreten Lösungsansätze möglichst praxisnah umgesetzt werden. Dies geschieht in Kooperation mit anderen Sicherheitsbehörden wie z.B. dem BKA und in enger Abstimmung mit dem Bundesministerium des Inneren.

Vor dem Hintergrund der dringend notwendigen internationalen Abstimmung müssen außerdem die Grundlagen für harmonisierte und interoperable Lösungen erarbeitet werden. Die aktive Mitwirkung bei nationalen, europäischen und internationalen Standardisierungsprozessen ist daher unerlässlich.

Die wichtigsten geplanten Einsatzzwecke von biometrischen Verfahren sind:

- Pässe und Personalausweise,
- Ausländerdokumente,
- Grenzkontrollen,
- Zutrittskontrollen in Sicherheitsbereichen.

Aus strategischer Sicht liegt zum gegenwärtigen Zeitpunkt der Schwerpunkt der Projekttätigkeiten des BSI auf den Verfahren der Gesichts-, Iris- und Fingerabdruckerkennung.

Untersucht werden die biometrischen Systeme beim BSI erstens nach Erkennungsleistung und Überwindungssicherheit unter Laborbedingungen. Damit sind grundsätzliche Aussagen zur Leistungsfähigkeit möglich. Zweitens erfolgt in Feldtests die Erprobung der biometrischen Verfahren anhand von definierten Zielpopulationen in realistischen Anwendungen. Das gibt Aufschluss über ihre Alltagstauglichkeit.

Fortsetzung auf S. 66

PC-Tastatur mit Sensorfeld für den Fingerabdruck.

Kombinationssysteme mit Smart Card und Fingerprint kommen bei Zugangskontrollanlagen zum Einsatz.

Menschen lassen sich täuschen, aber Computer auch? Diese Form der Zugangskontrolle durch automatische Gesichtserkennung funktioniert über hochkomplexe mathematische Berechnungen, die sich auf ein elastisches Gitternetz beziehen.

Eine andere Technik, das gleiche Ziel. Ein Gesicht wird mit Hilfe von Streifenrastern vermessen. Vier Digitalkameras und ein normaler PC genügen, um die Daten zu verarbeiten.

Zukunft Biometrie

Beides dient der zuverlässigen Beurteilung der Leistungsfähigkeit auf dem Markt verfügbarer biometrischer Systeme. Kernpunkt der Analyse ist die Identifizierung von Schwachstellen und die Entwicklung von technischen – und organisatorischen – Rahmenbedingungen für einen verlässlichen Betrieb.

Das BSI hat bereits 2002 eine Reihe von Aktivitäten zur Untersuchung der Biometrie gestartet. Die wichtigsten Arbeitsschwerpunkte und konkreten Ergebnisse aus dem Jahre 2003 sind:

BioFace (Gesichtserkennung)

Die Algorithmen- bzw. Feldtests sind erfolgreich abgeschlossen und veröffentlicht worden. Das nächste Projektelement – Einfluss von Störungen auf die Erkennungsleistung – befindet sich in der Fertigstellung.

BioFinger (Fingerabdruckerkennung)

Die Analyse zu den Tests über ihre Leistungsfähigkeit ist mit System- und Algorithmenprüfungen verfügbar.

Bio-P (allgemeine, praxisorientierte Projektreihe)

Die (Massen-)Erprobung der Gesichts-, Finger- und Iriserkennung ist mit der Prüfung der Gesichtserkennung auf Ausweisdokumenten abgeschlossen. Die zweite Phase zur Analyse der Erkennungsleistung und Überwindungssicherheit mit rund 2000 Nutzern ist gestartet.

Informationsdatenbank

Eine weltweite Marktübersicht über Anwendungsprojekte und zugehörige Systemübersichten ist in einer Informationsdatenbank zusammengefasst.

Sicherheitstests

Im Rahmen eines durch das BSI initiierten Projektes wurden Normungsanforderungen an die Biometrie erarbeitet. Erste Sicherheitstests wurden im 2003 neu errichteten BSI-internen Testlabor durchgeführt.

5. Schutz Kritischer Infrastrukturen

Der Einsatz moderner Informationstechnologien schafft neue Verwundbarkeiten und Abhängigkeiten: Computer steuern Energiesysteme, sie lenken Verkehrs- und Informationsströme, sie machen den modernen Zahlungsverkehr erst möglich.

Staat, Wirtschaft und Gesellschaft verlassen sich bei der Erfüllung ihrer Aufgaben immer mehr auf eine funktionierende IT. Dadurch sind viele Bereiche nur noch dann arbeitsfähig, wenn die Informations- und Kommunikationstechnik (IuK) zuverlässig ihren Dienst verrichtet. Ist dies nicht gewährleistet, kann es zu unabsehbaren Folgen für Staat und Gesellschaft kommen. Der „Schutz Kritischer Infrastrukturen – KRITIS“ ist angesichts einer Vielzahl möglicher und denkbarer Bedrohungen und Verwundbarkeiten eine Aufgabe, der sich Staat und Wirtschaft gemeinsam stellen müssen.

Das Konzept „Schutz Kritischer Infrastrukturen“ unterscheidet sich in einem wichtigen Punkt von der rein technischen IT-Sicherheit. Es berücksichtigt auch gesamtstaatliche bzw. gesamtgesellschaftliche Risiken und bindet sie staatenübergreifend in ein allgemeines Sicherheitsverständnis ein. Ein wesentliches Element bildet der Schutz der kritischen IT-Bereiche oder „Critical Information Infrastructure Protection – CIIP“.
„Kritische Infrastrukturen“ sind Organisationen oder Einrichtungen mit (lebens-)wichtiger Bedeutung für das staatliche Gemeinwesen. Bei Störung oder Ausfall dieser Systeme drohen für größere Bevölkerungsgruppen nachhaltig wirkende Versorgungsengpässe oder andere schwerwiegende Folgen. Staat und Wirtschaft funktionieren nur, wenn die folgenden Kritischen Infrastrukturen ohne wesentliche Beeinträchtigungen jederzeit verfügbar sind:

1. Telekommunikation und Informationstechnik
2. Energie
3. Finanz- und Versicherungswesen
4. Transport- und Verkehrswesen
5. Gesundheitswesen
6. Notfall- und Rettungswesen
7. Behörden und Verwaltung

IT-Sicherheit leistet für das Funktionieren dieser Bereiche einen wichtigen Beitrag. Doch sie allein kann noch keinen hinreichenden Schutz bieten. Vielmehr wird ein umfassendes Schutzkonzept benötigt, das über rein technische Maßnahmen hinaus auch folgende Komponenten umfasst:

- Prävention zur Minimierung der Vorfälle,
- Frühzeitiges Erkennen von Gefahren und Bedrohungslagen,
- Einschränken und Begrenzen der Auswirkung von Störungen auf Staat und Gesellschaft,
- Beheben der technischen Ursachen der Störungen.

Neue Formen der Kooperation sind erforderlich

Ein breitgefächertes und über technische Maßnahmen hinausgehendes, ganzheitliches Schutzkonzept für Kritische Infrastrukturen erfordert neue Formen der Kooperation von Staat, Wirtschaft und Gesellschaft.

Schon seit gut zehn Jahren gibt es in Deutschland eine Vielzahl von Initiativen und Projekten, die nach heutigem Verständnis direkt oder indirekt zum Bereich „Schutz Kritischer Infrastrukturen“ gezählt werden können. So wurden z.B. im Auftrag des BSI Analysen von sieben Kritischen Infrastrukturbereichen in Deutschland erstellt, eine „Kooperation-KRITIS“ zwischen Vertretern der Wirtschaft und dem BSI eingeleitet und die Zusammenarbeit mit den Bereichen Wissenschaft und Forschung intensiviert.

Weiterhin erstellt das BSI erstmals einen „Nationalen Plan zum Schutz IT-abhängiger Kritischer Infrastrukturen“. Kernstück dieses Plans ist die Darstellung einer Konzeption, wie der Schutz der Kritischen Infrastrukturen Deutschlands in den nächsten Jahren gestaltet sein soll. Diese Vision hat vier strategische Ziele: Prävention, Reaktion, Sensibilisierung und Nachhaltigkeit. Für jedes dieser Ziele werden Details für die drei Bereiche Politik, Privatwirtschaft und Bevölkerung mit Angaben zu Verantwortlichkeiten, Zielgruppen und ersten Maßnahmen erarbeitet.

Das Bundeskanzleramt, eine Bahnstrecke, der Flughafen Berlin-Tegel, — IT-abhängige Kritische Infrastrukturen brauchen umfassenden Schutz.

Kritische Infrastrukturen betreffen nicht nur staatliche Strukturen, sondern auch privatwirtschaftliche Einrichtungen in ganz Deutschland. Um ein verlässliches Funktionieren aller Bereiche sicherzustellen, ist das gemeinsame Handeln aller verantwortlichen Stellen notwendig. Koordination und Informationsaustausch sind unerlässlich. Nur durch eine intensive Zusammenarbeit zwischen Wirtschaft und Staat kann dieses Ziel effektiv erreicht werden. Aus diesem Grund spielen Initiativen und „Public Private Partnerships“ als Bindeglied zwischen Staat und Wirtschaft in Deutschland eine wichtige Rolle.

Zu nennen ist hier z.B. die Initiative D21. 300 Unternehmen haben sich zu einem gemeinnützigen, branchenübergreifenden Verein zusammengeschlossen. Sein Ziel ist es, in Zusammenarbeit mit Politik und Verwaltung den Wandel von der Industrie- zur Informationsgesellschaft zu fördern.

Im Arbeitskreis Schutz von Infrastrukturen (AKSIS) tauschen Unternehmen und Behörden ihre Erfahrungen aus. Sie analysieren die Abhängigkeiten der kritischen Sektoren von der IT und ihre Wechselbeziehungen untereinander. Die partnerschaftlich gewonnenen Ergebnisse kommen letztlich allen zugute: den direkt Beteiligten durch robustere Systeme und schließlich der gesamten Bevölkerung Deutschlands durch eine noch höhere Sicherheit.

Der Schutz Kritischer Infrastrukturen kann von einzelnen Nationen im Alleingang nicht erreicht werden. Um angesichts der internationalen Vernetzung einen umfassenden Schutz Kritischer Infrastrukturen zu erreichen, werden vom BSI auf Kongressen und Konferenzen, Gremien der G8 und Nato Ziele und Ergebnisse auch international diskutiert.

Der Schutz Kritischer Infrastrukturen gewinnt national wie international immer mehr an Bedeutung. Am Beispiel von 18 Ländern und drei internationalen bzw. supranationalen Organisationen stellt diese 2003 veröffentlichte Studie in einem bislang einzigartigen Umfang und Ansatz den gegenwärtigen Stand der Aktivitäten zum Schutz kritischer Infrastrukturen dar. Dabei geht es weniger um einen detaillierten Ergebnisbericht, sondern um die Beleuchtung des Schutzes Kritischer Infrastrukturen aus programmatischer, planerischer und konzeptioneller Sicht.

1. CD-ROM

Die vom BSI im Internet veröffentlichten Informationsangebote stehen allen Interessierten in Form einer kostenlosen CD-ROM zur Verfügung.

Bezug der BSI-CD-ROM
Gegen Einsendung eines an sich selbst adressierten Rückumschlags (DIN C5 frankiert mit Euro 1,44) beim BSI CD-Versand
Postfach 20 10 10, D - 53140 Bonn

Das Informationsangebot für Bürger findet sich ständig aktualisiert unter *www.bsi-fuer-buerger.de*. Das Webportal wird darüber hinaus als CD auf Messen verteilt und als Heftbeilage verbreitet. Außerdem sind die Inhalte der CD auf bestimmten PCs vorinstalliert.

2. BSI-Newsletter

Möchten Sie den fünfmal jährlich erscheinenden Online-Newsletter des BSI abonnieren? Dann senden Sie bitte eine E-Mail an: newsletter@bsi.bund.de

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,
55435 Gau-Algesheim oder
Postfach 1234,
D - 55205 Ingelheim
Tel: 06725-93 04-0
E-Mail: info@secumedia.de

4. Fachinformationen

Tagungsband: – Deutscher IT-Sicherheitskongress — IT-Sicherheit im verteilten Chaos
Herausgeber: BSI, Stand: 2003
ISBN 3-922746-49-7, Preis: 49,10 Euro
Bezugsquelle: SecuMedia Verlags GmbH
Postfach 1234, D - 55205 Ingelheim
Tel: 06725-93 04-0, Fax: 06725-59 94
Internet: www.secumedia.de

IT-Grundschutzhandbuch
Das IT-Grundschutzhandbuch wird als Loseblatt-Sammlung vom Bundesanzeiger Verlag vertrieben.
ISBN 3-88784-915-9
Grundwerk, A4, rund 2000 Seiten in drei Ordnern, Loseblattsammlung mit CD-ROM, Preis: 148,- Euro
Bestellungen richten Sie bitte an:
Bundesanzeiger Verlag, Postfach 10 05 34,
D - 50445 Köln, Fax: 0221-97 66 82 78
E-Mail: vertrieb@bundesanzeiger.de

Leitfaden IT-Sicherheit
Stand: 2003, ca. 42 Seiten
Download als PDF-Datei unter
www.bsi.bund.de/gshb/Leitfaden/index.htm

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

Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte
Stand: 2003, ca. 62 Seiten
Download als PDF-Datei unter www.bsi.bund.de/literat/doc/drahtloskom/index.htm

Internationale Aktivitäten zum Schutz Kritischer Infrastrukturen, ISBN 3-922746-54-3
Bezugsquelle: SecuMedia Verlags GmbH
Postfach 1234,
D - 55205 Ingelheim
Tel: 06725-93 04-0, Fax: 06725-59 94
Internet: www.secumedia.de

5. Studien

Kommunikations- und Informationstechnik 2010+3
Neue Trends und Entwicklungen in Technologie, Anwendungen und Sicherheit
Herausgeber: BSI, Stand: 2003
ISBN 3-922746-48-9
Preis: 78,- Euro
Bezugsquelle: SecuMedia Verlags GmbH
Postfach 1234, D - 55205 Ingelheim
Tel: 06725-93 04-0
Fax: 06725-59 94
Internet: www.secumedia.de

Apache Webserver – Sicherheitsstudie
Herausgeber: BSI, Stand: 2003
ISBN 3-922746-46-2
Preis: 19,80 Euro
Bezugsquelle: SecuMedia Verlags GmbH
Postfach 1234,
D - 55205 Ingelheim
Tel: 06725-93 04-0
Fax: 06725-59 94
Internet: www.secumedia.de
Auch downloadbar als PDF-Version unter
www.bsi.bund.de/literat/secumed.htm

Microsoft Internet Information Server – Sicherheitsstudie
Herausgeber: BSI, Stand: 2003
ISBN 3-922746-47-0
Preis: 19,80 Euro
Bezugsquelle: SecuMedia Verlags GmbH
Postfach 1234,
D - 55205 Ingelheim
Tel: 06725-93 04-0, Fax: 06725-59 94
Internet: www.secumedia.de
Auch downloadbar als PDF-Version unter
www.bsi.bund.de/literat/secumed.htm

Leitfaden zur Einführung von Intrusion-Detection-Systemen
Download als PDF unter www.bsi.bund.de/literat/studien/ids02/dokumente/ Leitfadenv10.pdf

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

Anhang Ansprechpartner und Kontakte

Jahrgang 1955, studierter Physiker und Mathematiker, bis 1983 wissenschaftlicher Angestellter am Institut für theoretische Physik der Ruhr-Universität Bochum. Abteilungsleiter an der Bergischen Universität in Wuppertal bis 1985. Wechsel zu Messerschmitt-Bölkow-Blohm (heute EADS). Bis 1995 dort in verschiedenen Führungspositionen tätig. Vor Amtsantritt beim BSI 2003 Direktor und Bereichsleiter bei der Bayerischen Versorgungskammer, München.

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

Jahrgang 1950, Studium der Mathematik in Bonn. Seit 1977 in der Bundesverwaltung als Referent und ab 1985 als Referatsleiter im Bereich IT-Sicherheit tätig. Mit Gründung des BSI Abteilungsleiter und maßgeblich am Auf- und Ausbau beteiligt. Seit 1994 Vizepräsident und in dieser Funktion als nationaler Direktor für Kommunikationssicherheit deutscher Repräsentant in IT-Sicherheitsgremien der NATO und EU.

Michael Hange, Vizepräsident

Jahrgang 1963, Studium der Verwaltungswissenschaft in Konstanz, Diplom 1988. Wissenschaftliche Mitarbeiterin an den Universitäten Konstanz und Bonn sowie am Kernforschungszentrum Karlsruhe, seit 1993 Mitarbeiterin im BSI mit den Schwerpunkten Sicherheitskultur, Aufklärung und Sensibilisierung zu Fragen der IT-Sicherheit.

E-Mail: anja.hartmann@bsi.bund.de

Anja Hartmann, Referatsleiterin Öffentlichkeitsarbeit, Marketing

Jahrgang 1955, Studium der Rechtswissenschaften in Bonn, Rechtsanwalt. Wechsel zum Technischen Hilfswerk als Personalleiter. Mit Gründung des BSI im Jahr 1991 Referatsleiter Organisation und zugleich Pressesprecher.

Fragen und Anregungen zu Pressemitteilungen senden Sie bitte an michael.dickopf@bsi.bund.de

Michael Dickopf, Pressesprecher

Das BSI im Internet

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, z.B. mit

- Verschlüsselungs-Tool
- Virenscanner
- PC-Firewall-Programm und
- Bildschirmschoner

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

Fachleute und Experten finden hier Informationen u.a. zu den Themen

- Zertifizierung
- E-Government
- CERT-Bund
- Elektronische Signatur
- IT-Grundschutz
- Kritische Infrastrukturen
- Schadprogramme

sowie Hinweise auf Veranstaltungen, Schulungen und Publikationen.

Anschrift
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189,
53175 Bonn
Tel: +49-228-9582-0
Fax: +49-228-9582-400
E-Mail: bsi@bsi.bund.de

Internetadressen des BSI
www.bsi.bund.de
www.bsi-fuer-buerger.de

Bildnachweis
Pierre Boom, Bremen Online Services, BSI Referat Öffentlichkeitsarbeit, Caro Fotoagentur, Das Fotoarchiv, Deutsche Bahn, Deutsche Telekom, Andreas Ernst, European Commission Audiovisual Library, Fujitsu Siemens Computers, Hans Georg Gaul, Geschäftsstelle Bundesprogramm Ökologischer Landbau, Paul Glaser, Institut für Mikrotechnik Mainz, Nokia, Jan Pauls, Photodisc, Presse- und Informationsamt der Bundesregierung – Bundesbildstelle, Presse- und Informationsamt der Bundesstadt Bonn, Siemens Presse-bild, Vodafone D2, Frank Weihs

Herausgeber
Bundesamt für Sicherheit in der
Informationstechnik – BSI
53175 Bonn

Bezugsstelle
Bundesamt für Sicherheit in der
Informationstechnik – BSI
Referat III.21
Godesberger Allee 185-189, 53175 Bonn
Tel: +49-228-95 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
Internet: www.thomas-ppr.de

Druck
Druckhaus Dierichs Akzidenz GmbH, Kassel

Stand
März 2004