Bundesamt
für Sicherheit in der
Informationstechnik

Jahresbericht 2006
2007

# Sichere Informations-technik für unsere Gesellschaft

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

# Moderne Staaten brauchen sichere Informationstechnik

*Liebe Mitbürgerinnen und Mitbürger,*

beinahe alle gesellschaftlichen Bereiche sind heute durch Informations- und Kommunikationssysteme in einem Maße miteinander vernetzt, das noch vor 20 Jahren undenkbar gewesen wäre. Handel, Verkehr und auch die öffentliche Verwaltung setzen heute mehr und mehr auf IT bei ihren Geschäftsprozessen.

Dabei ist die immer größer werdende Vernetzung der Informations- und Kommunikationssysteme eine besondere Herausforderung. Denn durch wechselseitige Abhängigkeiten entstehen auch neue Gefährdungen. IT-Systeme sind, unabhängig davon, ob es sich um die Computer privater Anwenderinnen und Anwender oder ganze Unternehmensnetze handelt, Hackerangriffen und Bedrohungen durch Schadprogramme ausgesetzt. Die Gefährdungssituation hat sich in letzter Zeit deutlich verschärft.

Moderne Industriestaaten sind auf sichere Informationstechnik angewiesen. Im Rahmen der Daseinsvorsorge muss der Staat auch Ausfälle kritischer Infrastrukturen verhindern. Wir brauchen Lösungen, die die Nutzung dieser Technologien dauerhaft gewährleisten. Wir brauchen auch ein Bewusstsein für die Gefahren bei den Bürgerinnen und Bürgern, bei Wirtschaft und Wissenschaft und auch beim Staat. Die Bundesregierung ist sich bewusst, dass die innere Sicherheit unseres Staates heute untrennbar mit sicheren Informationsinfrastrukturen verbunden ist. Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) kommt daher bei der Gestaltung der IT-Systeme in Gegenwart und Zukunft eine wichtige Rolle zu.

Das BSI leistet einen maßgeblichen Beitrag für unsere IT-Sicherheit. Damit das BSI seine Aufgaben weiterhin kompetent, verantwortungsvoll und den aktuellen Bedrohungen angemessen wahrnehmen kann, muss das IT-Sicherheitsrecht angepasst werden. Dazu gehört auch die laufende grundlegende Überarbeitung des BSI-Gesetzes. Nur so kann das BSI den veränderten Rahmenbedingungen gerecht werden und auch in Zukunft als einzige staatliche IT-Sicherheitsbehörde die Sicherheit unserer Regierungskommunikation verantworten und IT-Sicherheit in Deutschland gewährleisten.

Berlin, im Mai 2008

Dr. Wolfgang Schäuble MdB
Bundesminister des Innern

# Das BSI: modern, leistungsfähig, serviceorientiert

*Liebe Leserinnen und Leser,*

Deutschland braucht sichere Informationstechnik. Herausforderungen wie die verstärkte Abhängigkeit von moderner Informationstechnik unterstreichen das. Wie der Bericht zur Lage der IT-Sicherheit in Deutschland 2007 zeigt, nehmen seit Jahren die Gefahren weiter zu. Inzwischen sind 40 Millionen Menschen in Deutschland online. Beim Surfen im Internet oder beim Empfangen von E-Mails hatten ein Drittel schon einmal Kontakt mit Schadprogrammen wie Trojanischen Pferden, und bereits 60 Prozent waren von Computerviren und -würmern betroffen. Auch in der Wirtschaft wachsen die Gefahren. Es gibt kaum ein sicherheitsrelevantes Unternehmen, das nicht schon einmal den Versuch erlebt hat, über das Internet ausgespäht zu werden. Weil die Angriffe immer raffinierter werden, steigen die Herausforderungen an eine sichere Informationstechnik ständig weiter. Besonders im Mittelstand besteht hier erheblicher Nachholbedarf.

Der nun vorliegende Jahresbericht 2006/2007 dokumentiert eindrucksvoll die Arbeit des BSI bei der Abwehr dieser Gefahren und das Eintreten für eine sichere Informationstechnik. Das BSI ist der zentrale IT-Sicherheitsdienstleister in Deutschland. Wir sind eine moderne und leistungsfähige Behörde, die service- und kundenorientiert handelt. Das Jahr 2006 war in der Geschichte unseres Amtes ein besonderes Jahr: Das BSI konnte sein 15-jähriges Jubiläum feiern. 1991 gegründet, legte das BSI in den 90er Jahren die Grundlagen für den Aufbau eines IT-Grundschutzes und die Zertifizierungs- und Akkreditierungsverfahren. In den vergangenen Jahren konnte das BSI seine herausragende Position auf dem Gebiet der IT-Sicherheit festigen und weiter ausbauen. Inzwischen leisten fast 500 Mitarbeiterinnen und Mitarbeiter im BSI ihren Beitrag zur Inneren Sicherheit Deutschlands. Diese Konzentration von Expertenwissen ist europaweit einmalig. Dauerhaft lässt sich allerdings das IT-Sicherheitsniveau in Deutschland nur verbessern, wenn alle gesellschaftlichen Gruppen zusammenarbeiten. Ich gehe davon aus, dass dieser Jahresbericht einen Beitrag zur Information und Aufklärung leisten wird.

Im Jahr 2008 wird sich das BSI besonders auf die Themen Netzsicherheit, Trojanerabwehr, Sicherheit Hoheitlicher Dokumente, Bürgerportale, Mobilfunksicherheit und den Ausbau der technischen Evaluierungskapazität konzentrieren. Damit setzt das BSI unter anderem die Ziele des Nationalen Plans zum Schutz der Informationsstrukturen (NPSI) weiter konsequent um und reagiert auch auf Veränderungen der IT-Sicherheitslage.

Bonn, im Mai 2008

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

# 1.1 Zahlen und Fakten

*Informationstechnik (IT) durchdringt alle Lebensbereiche: Telekommunikation, Börsen, Versicherungen, Behörden, Produktionsprozesse, Unterhaltungsindustrie. Wo Millionen Informationen und Daten verarbeitet werden, müssen Schutzmechanismen vorhanden sein, damit für das Funktionieren der Gesellschaft wichtige Systeme nicht versagen oder durch Angriffe von außen gestört werden.*

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) leistet als die zentrale deutsche IT-Sicherheitsbehörde dazu seit mehr als 15 Jahren einen bedeutenden Beitrag. Als obere Bundesbehörde im Geschäftsbereich des Bundesministerium des Innern (BMI) ist das BSI operativ für den Bund, kooperativ mit der Wirtschaft und informativ für den Bürger tätig.

Grundlage seiner Arbeit ist das vom damaligen und heutigen Innenminister Dr. Wolfgang Schäuble vorgelegte BSI-Errichtungsgesetz. Am 1. Januar 1991 nahm das BSI unter dem Gründungspräsidenten Dr. Otto Leiberich seine Arbeit auf. Im Jahr 2006 konnte die Behörde somit auf eine 15-jährige Geschichte zurückblicken.

### Ziele des BSI

Oberste Prämisse für das BSI ist der Schutz von Information und Kommunikation. Wie im „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ der Bundesregierung festgelegt, stehen drei strategische Ziele im Vordergrund:

- **Prävention:**
  Informationsinfrastrukturen angemessen schützen!
- **Reaktion:**
  Wirkungsvoll bei IT-Sicherheitsvorfällen handeln!
- **Nachhaltigkeit:**
  Deutsche IT-Sicherheitstechnologie und -kompetenz fördern – international Standards setzen!

### Aufgaben und Selbstverständnis

Das Bundesamt für Sicherheit in der Informationstechnik wendet sich mit seinem komplexen Aufgaben- und Dienstleistungsangebot an die öffentliche Verwaltung in Bund, Ländern und Kommunen sowie an Unternehmen und Privatanwender.

Für die unterschiedlichen Bezugsgruppen bietet es zielgruppengerechte Dienstleistungen an:

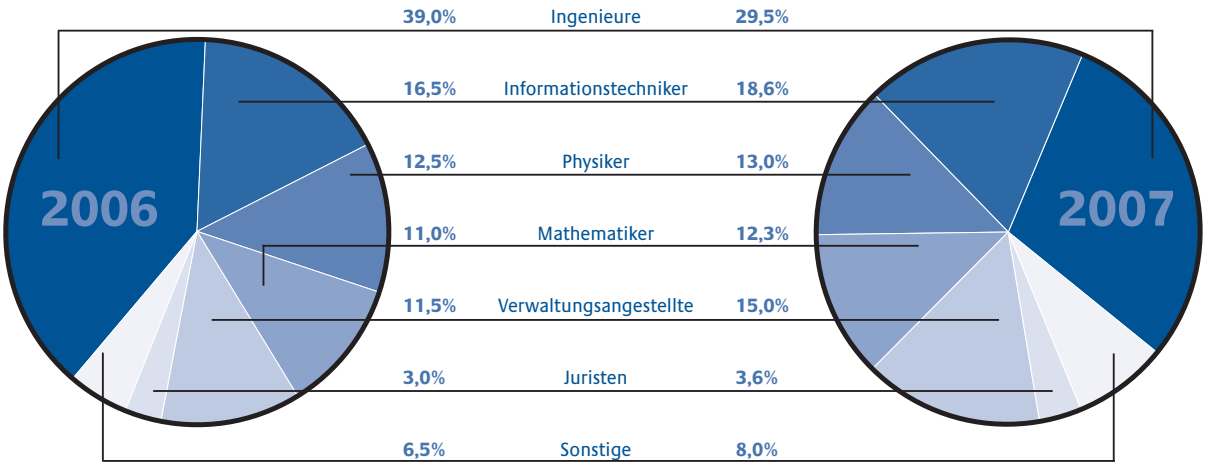
- **Information:**
  Das BSI informiert zu allen wichtigen Themen der IT-Sicherheit.
- **Beratung:**
  Das BSI berät und unterstützt seine Kunden bei der Umsetzung geeigneter Maßnahmen.
- **Entwicklung:**
  Das BSI konzipiert und entwickelt IT-Sicherheitsanwendungen und IT-Sicherheitsprodukte.

Eine weitere wichtige Aufgabe ist das Prüfen, Bewerten und Zertifizieren von IT-Produkten und IT-Systemen im Hinblick auf ihre Sicherheitseigenschaften. Auch die Zulassung von IT-Systemen für die Verarbeitung geheimer Informationen gehört zu den Aufgaben des BSI.

Das BSI arbeitet an allen wichtigen Themen der IT-Sicherheit und ist auf diesem Gebiet führend in Deutschland. Ziel ist es, die Ergebnisse neben den staatlichen Einrichtungen auch der Industrie und den Bürgern zu gute kommen zu lassen. International versteht sich das BSI als Vertreter deutscher Sicherheitsinteressen. Seine Mitarbeiterinnen und Mitarbeiter wissen bei ihren Dienstleistungen durch Kompetenz zu überzeugen. Viele Bestandteile ihrer Arbeit sind als Best-Practice-Modelle anerkannt.

**Fachrichtungen im BSI – 2006 und 2007 im Vergleich**

*nur höherer und gehobener Dienst, in Prozent*



Bei der Umsetzung ihrer Aufgaben arbeitet die Behörde service- und kundenorientiert. Dabei ist das BSI bestrebt, das Verhältnis von Aufwand und Ergebnis kontinuierlich zu optimieren.

Hierfür werden moderne Managementwerkzeuge wie die Ausrichtung aller operativen Aufgaben des BSI nach Programmen, die Kosten-Leistungs-Rechnung und eine Balanced Scorecard eingesetzt.


*Eine breite Palette von Dienstleistungen: die Auswahl der Angebote des BSI reicht von A wie Akkreditierung bis Z wie Zertifizierung.*

## Mitarbeiter- und Haushaltszahlen

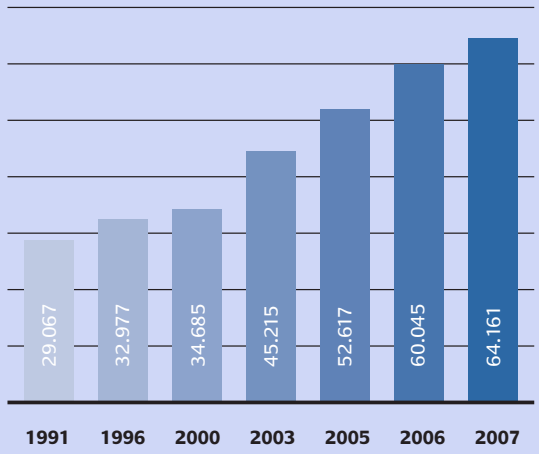
Im BSI arbeiten fast 500 Generalisten und Spezialisten gemeinsam an der komplexen Aufgabe, das IT-Sicherheitsniveau in Deutschland zu erhöhen. Dies sind 50 Mitarbeiterinnen und Mitarbeiter mehr als im Jahr 2005. So vielfältig die Aufgaben im BSI sind, so vielfältig sind auch die Fachrichtungen der Mitarbeiter. Von den rund 500 Mitarbeitern stellen Ingenieure mit 29,5 Prozent die größte Gruppe, gefolgt vom Fachgebiet Informationstechnologie mit 18,6 Prozent. Aber auch andere Fachrichtungen wie Rechtswissenschaft, Politik- und Kommunikationswissenschaft sind vertreten. Somit kann das BSI auf die unterschiedlichen Anforderungen der sich schnell wandelnden Informationstechnik fachlich kompetent und differenziert reagieren. Denn zur IT-Sicherheit stellen sich neben informationstechnischen auch wirtschaftliche, rechtliche und gesellschaftliche Fragen.

Ein Indiz für die steigende Bedeutung des BSI ist auch die kontinuierliche Aufstockung des Etats. Waren es im Jahr 1997 noch zirka 33,5 Millionen Euro, so lag der Gesamthaushalt im Jahr 2007 bei zirka 64 Millionen Euro. Das ist gegenüber dem Jahr 2006 ein Anstieg von vier Millionen Euro. Davon entfielen 24 Millionen Euro auf Personalkosten und 33 Millionen auf Sachkosten. Die Ausgaben für Investitionen betrugen 6,8 Millionen Euro.

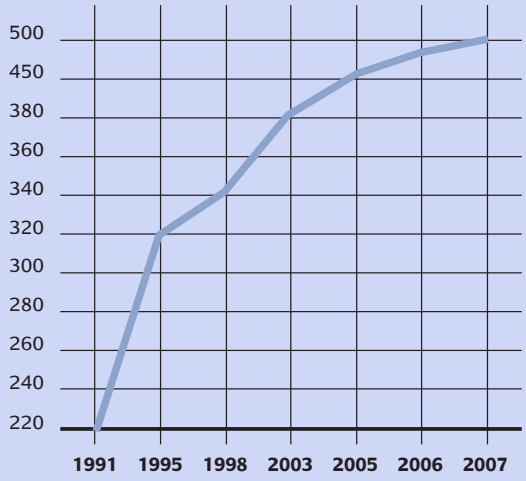
In der IT-Branche gilt das BSI seit Jahren als einer der beliebtesten Arbeitgeber. Das spricht für seinen Stellenwert in der Fachwelt. Auf der von dem Unternehmen trendence Institut GmbH erstellten Rangliste „Das Deutsche Absolventenbarometer – IT-Edition“ nimmt das BSI im Jahr 2007 unter 98 Unternehmen den 13. Platz ein. Befragt wurden 4.893 Studierende. Damit steht das BSI auf einer Stufe mit Weltkonzernen wie Microsoft, Google oder Siemens.

**Haushaltszahlen 1991 bis 2007**

*in Tausend Euro*

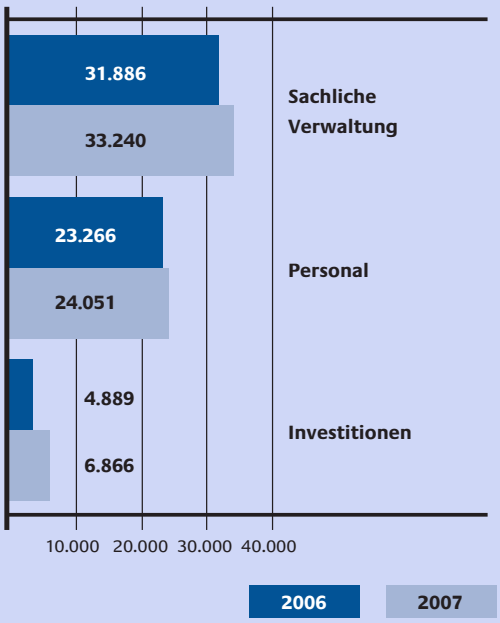



**Mitarbeiterzahlen 1991 bis 2007**




**Ausgaben nach Sachgebieten**

*in Tausend Euro*



# 1.2 Information und Kommunikation – das BSI in der Öffentlichkeit

*Aufklärung und Sensibilisierung bedeutet aktive Information, Kommunikation und Interaktion. Nur so lässt sich das Thema IT-Sicherheit als permanente Aufgabe nachhaltig in das Bewusstsein der Öffentlichkeit bringen.*

Für aktuelle Fragen der IT-Sicherheit zu sensibilisieren und IT-Sicherheitskompetenz aufzubauen bedeutet konkret:

- Bewusstsein schaffen bei den verschiedenen Zielgruppen;
- Fachwissen aufbauen, um aktuelle Gefährdungen zu erkennen;
- geeignete Sicherheitsmaßnahmen treffen.

Zielgruppen sind Bürger, Verwaltung (Bund, Länder, Gemeinden), Wirtschaft, Multiplikatoren (insbesondere Medien) sowie Organisationen wie Verbände und Vereine. Von besonderer Wichtigkeit ist dabei die neutrale und produktunabhängige Präsentation der Zusammenhänge. Dafür hält das BSI eine Vielzahl von Angeboten und Leistungen bereit.

### Der Internetauftritt des BSI

Die BSI-Website www.bsi.bund.de richtet sich in erster Linie an IT-Experten. Dort wird ein umfangreiches Angebot zu Themen wie IT-Grundschutz, CERT-Bund oder Zertifizierung und Akkreditierung bereitgestellt. Studien, Veröffentlichungen, Beiträge und Fachpublikationen stehen zum Download zur Verfügung. Es besteht auch die Möglichkeit, den BSI-Newsletter zu abonnieren. Er erscheint fünfmal im Jahr und enthält aktuelle Informationen zu Veröffentlichungen und Veranstaltungen des BSI.

### Die Website für Einsteiger

Auf der Internetseite www.bsi-fuer-buerger.de bietet das BSI kompakt und in verständlicher Sprache für Privatanwender Informationen zu allen Themen rund um die IT-Sicherheit. Verschiedene Kapitel erläutern grundsätzlich, wie man sich vor Viren

und Würmern schützt, wie die Datensicherung funktioniert oder wie man mit vertraulichen Daten umgeht. Eine Toolbox mit Programmen, ein Glossar und viele nützliche Links bieten das Gerüst für ein breites Basiswissen. Ein „Brennpunkt des Monats“ greift aktuelle IT-Sicherheitsthemen wie das Web 2.0, Patch-Management oder den Umgang mit Tauschbörsen auf.


Die Bürger-Website hat im September 2007 eine neue Form bekommen. Die Seite wurde optisch ansprechender gestaltet. Vertraute Strukturen wie zum Beispiel die Menüführung blieben erhalten, auch behält das Maskottchen „Argus“ die Benutzerführung.

Alle Inhalte der Bürger-Website sind auch auf der CD „Ins Internet – mit Sicherheit“ enthalten. Die CD wurde im Jahr 2007 in hoher Auflage verteilt, da es gelang, gezielt Multiplikatoren in Volkshochschulen, Verbraucherberatungsstellen und bei der Polizeilichen Kriminalprävention der Länder und des Bundes anzusprechen. In Zusammenarbeit mit dem Deutschen Sparkassen Verlag erschien die Informationsbroschüre „Einfach Online – Mit Sicherheit durchs Internet“.


*Ein „Longseller“ des BSI: Diese CD-ROM bietet nicht nur Informationen, sondern auch kostenlose Schutzprogramme.*

## Das Bürger-CERT

Bundesinnenminister Dr. Wolfgang Schäuble hat im März 2006 den Informationsdienst Bürger-CERT feierlich online geschaltet www.buerger-cert.de. Ergänzend zu „BSI für Bürger“ geht es hier um tagesaktuelle Warnungen vor Viren, Würmern und anderen Computerschädlingen. Hinter dem Bürger-CERT steht ein Team aus Spezialisten, die sich intensiv mit IT-Sicherheit beschäftigen. Sie beobachten in Netzwerken die IT-Infrastrukturen, geben Warnmeldungen und Sicherheitsinformationen heraus und bieten Unterstützung bei der Lösung von IT-Sicherheitsvorfällen. Die Abkürzung „CERT“ steht für „Computer Emergency Response Team“ (deutsch: Computer-Notfallteam).

Mit dem Bürger-CERT steht in Deutschland erstmals ein neutraler und kostenloser Warn- und Informationsdienst zur IT-Sicherheit zur Verfügung. Internetnutzer haben so die Möglichkeit, sich bei besonderen Risiken und Gefahren aufgrund von aktuellen Sicherheitslücken im Internet schnell, kompetent und umfassend informieren und warnen zu lassen.

Das Bürger-CERT bietet parallel drei verschiedene Informationsdienste an:

- Der **Online-Newsletter „Sicher Informiert“** liefert vierzehntäglich einen Überblick über die wichtigsten Sicherheitsnachrichten.
- Bei extrem zeitkritischen Sicherheitslecks mit umgehendem Handlungsbedarf warnen **„Extraausgaben“** des Online-Newsletters.
- **„Technische Warnungen“** mit detaillierten Hintergrundinformationen für technisch interessierte und versierte Anwender runden das Angebot ab.

Der Internetauftritt des Bürger-CERT enthält darüber hinaus ein Archiv zur Recherche in früheren Meldungen sowie ein Glossar, in dem IT-Fachbegriffe verständlich erklärt werden.

Im Mai 2006 erhielt das Bürger-CERT den Preis „Sicherheit im Internet“ der Initiative „klicksafe“ www.klicksafe.de. Diese Initiative ist Bestandteil des europaweiten „Safer Internet“-Programms der Europäischen Union. Klicksafe zeichnet Projekte und Initiativen aus, die sich in herausragender Art und Weise für mehr Medienkompetenz und Sicherheit im Internet stark machen.

Die hochrangig besetzte Experten-Jury begründete die Auszeichnung wie folgt: „Bürger-CERT ist ein inhaltlich und fachlich hochwertiges Angebot, das sehr geeignet ist, die breite Bevölkerung zu erreichen und mit Sicherheitsthemen vertraut zu machen. Der Ansatz, dass eine Behörde sich öffnet und ihre Informationen auf einem passenden Weg für die Öffentlichkeit bereitstellt, ist besonders hervorzuheben. Damit ist garantiert, dass unabhängig und für die Nutzer kostenfrei fachlich fundierte Informationen bereitgestellt werden. Überzeugt hat die Jury auch die große Reichweite des Angebots: Bereits im ersten Monat haben 60.000 Bürgerinnen und Bürger den Warn- und Sicherheitsdienst abonniert.“

### Kooperationspartner des BSI

Das BSI kooperiert mit verschiedenen Unternehmen aus der Wirtschaft, um den IT-Sicherheitsgedanken noch mehr in der Gesellschaft zu verankern. Dabei arbeitet das Haus im Bereich Öffentlichkeitsarbeit mit verschiedenen Partnern zusammen:

**heise security**
Unter www.heise.de/security/ werden ausgewählte Informationen aus dem BSI präsentiert.


**Freenet.de**
Im Themenbereich Computer & Technik –> Viren & Sicherheit werden Meldungen sowie für die Zielgruppe Privatanwender Artikel zur IT-Sicherheit präsentiert.

**Fujitsu-Siemens**
Durch vom Hardwarehersteller vorinstallierte Inhalte des BSI wird der Anwender gleich nach dem Kauf eines neuen PC auf den hohen Stellenwert der IT-Sicherheit aufmerksam gemacht.

**Netzcheckers**
Das BSI ist mit zielgruppengerechten Inhalten wie „Computerspiele – aber sicher!“ oder „Handy-Payment kann teuer werden“ auf der Internetseite www.netzcheckers.de präsent. Das BSI versucht so, besonders Jugendliche für Themen der IT-Sicherheit zu sensibilisieren.

Bei der Aufklärung und Sensibilisierung der Bürgerinnen und Bürger geht es immer darum, den hohen Stellenwert der IT-Sicherheit bewusst zu machen.


## Auftritte auf Fachmessen und Kongressen

Das BSI präsentierte sich 2006 und 2007 mit Themen wie IT-Grundschutz und IT-Sicherheitszertifizierung, aber auch mit neuen Entwicklungen zum Thema „Hoheitliche Dokumente“ auf verschiedenen Fachmessen und Kongressen. Dort bot sich die Möglichkeit, direkten Kontakt mit IT-Experten aufzunehmen und dem Privatanwender das Angebot des BSI vorzustellen.

**10. Deutscher IT-Sicherheitskongress**
Vom 22. bis 24. Mai 2007 tagte der 10. Deutsche IT-Sicherheitskongress des BSI in der Stadthalle von Bonn-Bad Godesberg. Der Jubiläumskongress, der unter dem Motto „Innovationsmotor IT-Sicherheit“ stand, beleuchtete an den drei Veranstaltungstagen die vielfältigen Aspekte der IT-Sicherheit.

### CeBIT Hannover

Auf den CeBIT-Messen im März 2006 und März 2007 war das BSI in Halle 7 vertreten. Themen wie Internetsicherheit, Sicheres E-Government oder IT-Sicherheitszertifizierung nach Common Criteria stießen am BSI-Stand auf besonderes Interesse. Zudem wurde die CD, auf der Informationen der Internetseite des BSI enthalten sind, stark nachgefragt. Weiterhin präsentierte sich das BSI auf der Gemeinschaftsfläche des Bundes, dem Public-Sector-Parc. Vortragsreihen im Convention Center rundeten das umfangreiche Angebot auf der CeBIT ab.

### Systems München

Auf den Messen Systems 2006 und Systems 2007 übernahm das BSI in beiden Jahren wieder die Schirmherrschaft über die IT-Security-Area. Die Schwerpunkte der technischen Präsentationen am BSI-Stand waren Sichere Inter-Netzwerk Architektur (SINA), Mobile Security sowie Informationen rund um das Thema IT-Sicherheitszertifizierung. Am Dienstag, den 23. Oktober 2007, eröffnete BSI-Präsident Dr. Udo Helmbrecht die IT-Security-Area auf dem Forum Blau. Hier fanden auch die Vorträge der BSI-Experten zu den Themen IT-Grundschutz, Hoheitliche Dokumente, IT-Sicherheitszertifizierung und eCard-API statt.

### Security Essen

In Essen präsentierte das BSI 2006 seine Sicherheitslösungen und Beratungsservices. Themenschwerpunkte des BSI-Standes auf der Gemeinschaftsfläche „Themenpark IT-Sicherheit“ bildeten die Beratungsdienstleistungen zur materiellen Sicherheit und zum IT-Grundschutz. Lösungsansätze zu Problemen bei der organisatorischen Zusammenführung der materiellen Sicherheit und der IT-Sicherheit zeigte das BSI auch beim messebegleitenden Kongress, unter anderem mit dem Vortrag des BSI-Präsidenten Dr. Udo Helmbrecht zum Thema „Informationsschutz – warum zu viele Unternehmen hilflos sind“.

### Moderner Staat Berlin

IT-Sicherheit war in beiden Jahren einer der Themenschwerpunkte auf der Messe „Moderner Staat“. Der Themenpark IT-Sicherheit mit seinen rund 20 Ausstellern bildete den zentralen Treffpunkt für die IT-Sicherheitsbranche. Das BSI als Partner IT-Sicherheit des Messeveranstalters informierte dort über aktuelle Themen. Zusätzlich richtete das BSI eine Vortragsreihe zu SINA-Architektur, Kommunikationssicherheit im E-Government und Risikomanagement aus.

### LinuxTage Wiesbaden und Berlin

Auf den LinuxTagen 2006 in Wiesbaden und 2007 in Berlin stellte das BSI aktuelle IT-Sicherheitslösungen auf Basis von Open Source Software vor. Ein zentraler Aspekt innerhalb der IT-Strategie des Bundes ist die Förderung der Vielfalt von Software. Nur so können Monokulturen vermieden und dadurch IT-Sicherheit besser gewährleistet werden.


*LinuxTag 2007 unter dem Berliner Funkturm – der Messeplatz Berlin ist bei IT-Sicherheitsexperten mehrmals im Jahr ein gefragter Treffpunkt.*

## Weitere Veranstaltungen

### Tag der offenen Tür in Berlin

Unter dem Motto „Einladung zum Staatsbesuch“ öffnet die Bundesregierung und damit auch das Bundesministerium des Innern (BMI) in Berlin jedes Jahr die Türen für interessierte Bürgerinnen und Bürger. In den Jahren 2006 und 2007 war das BSI dort präsent und zeigte sein Service- und Informationsangebot für die privaten PC-Anwender. Die Schwerpunkte bildeten dabei die Website www.bsi-fuerbuerger.de sowie der Warn- und Informationsdienst www.buerger-cert.de mit dem kostenlosen Newsletter „Sicher • Informiert“.

### Girls’ Day

Beim Mädchen-Zukunftstag Girls’ Day, der bundesweit stattfand, beteiligte sich das BSI 2006 und 2007 mit Vorträgen und Präsentationen zum Thema „Mit Sicherheit auch Frauensache!“. BSI-Experten aus unterschiedlichen Abteilungen zeigten den Mädchen, welche Aufgaben IT-Spezialisten beim BSI übernehmen.

### BSI im Gespräch

Das BSI bietet mit der Veranstaltungsreihe „BSI im Gespräch“ regelmäßig ein Forum zur Kommunikation zwischen Wirtschaft, Wissenschaft und Verwaltung. Im kleinen Kreis diskutieren dort hochrangige Teilnehmer über Themen wie „IT-Sicherheit als Geschäftsmodell“ und „IT-Sicherheit und Recht“. Ziel der Veranstaltungsreihe ist es, einen nachhaltigen Dialog über zukunftsweisende Themen anzustoßen.

## Gefragte Experten

Die Informationstechnik ist seit Jahren auch ein Dauerthema in Presse, Rundfunk und Fernsehen. Dabei wird vor allem die IT-Sicherheit immer stärker thematisiert. Zeitungen und Zeitschriften, Online-Medien sowie Radio- und Fernsehsendungen berichten immer häufiger darüber, wie Privatanwender ihren PC und ihre persönlichen Informationen vor Online-Angriffen schützen können. Dabei sind die Experten des BSI gefragte Gesprächs- und Interviewpartner. Sie erläutern die Bedrohungen und Angriffsszenarien und geben verständliche Tipps für eine sichere IT der Bürgerinnen und Bürger. Häufig verweisen die Medien dabei auch auf die Informations- und Serviceangebote des BSI („BSI für Bürger“ und „Bürger-CERT“).

### <kes> – Die Zeitschrift für Informations-Sicherheit


Das offizielle Verlautbarungsorgan des BSI ist das BSI-Forum in der Zeitschrift <kes>. Sechsmal jährlich informiert das Forum mit Fachbeiträgen von BSI-Autoren oder Gastautoren über aktuelle IT-Sicherheitsthemen. Zielgruppe sind vorrangig IT-Sicherheitsexperten. Zu den Lesern der <kes> zählen die wichtigen IT-Entscheider der großen Wirtschaftsunternehmen, Banken und Behörden. Das BSI-Forum ist neben der Printausgabe in der <kes> auch elektronisch unter www.bsi.bund.de/literat/forumkes.htm verfügbar.

## 1.3 Internationale Zusammenarbeit

*Der grenzüberschreitende Personen- und Warenverkehr, die vernetzten Finanzmärkte, der blitzschnelle weltweite Datenaustausch zeigen es: IT-Sicherheit ist keine nationale Angelegenheit.*

Globalen Herausforderungen stellt sich das BSI durch internationale Kooperation. Nur wenn Informationen und Erfahrungen ausgetauscht und gemeinsam genutzt werden, können wichtige Entwicklungen im Bereich der IT-Sicherheit erkannt und sicherheitsrelevante Lücken frühzeitig entdeckt werden.

**Die internationale Zusammenarbeit umfasst zum Beispiel:**

- die **Entwicklung** geeigneter Maßnahmen zur IT-Krisen-Bewältigung durch Computer-Notfallteams oder im Bereich Kritische Infrastrukturen;
- die **Sicherung** der internationalen Interoperabilität bei biometrischen Anwendungen;
- die **Standardisierung** und Normierung von Sicherheitsprodukten (Common Criteria);
- die **Mitwirkung** an technischen Großprojekten der Luft- und Raumfahrt wie beim Airbus A400M oder dem Satelliten-Projekt Galileo;
- die **Unterstützung** internationaler Einrichtungen durch zugelassene BSI-Produkte wie SINA und dem Verschlüsselungsgerät Elcrodat.

Das BSI vertritt die deutschen Interessen sowohl in internationalen Gremien – etwa bei NATO, EU, ENISA und ISO – als auch in der bi- und multilateralen Zusammenarbeit mit anderen Staaten. Neben dem traditionell starken Engagement des BSI in der NATO wurde in den Jahren 2006 und 2007 die Zusammenarbeit mit der EU intensiviert. Für die Europäische Agentur für Netz- und Informationssicherheit (ENISA) ist das BSI der zentrale nationale Ansprechpartner. Die Behörde ist seit Mitte 2007 im internationalen Verwaltungsrat der ENISA vertreten. Seit 2006 koordiniert der „Stab Internationale Beziehungen“ die entsprechenden Aktivitäten des BSI. Nach außen ist der Stab zentraler Ansprechpartner für alle internationalen Angelegenheiten.

# IT-Sicherheit mit europäischer Dimension


Von der EU-Ratspräsidentschaft, die Deutschland im ersten Halbjahr 2007 innehatte, wurde erwartet, dass sie politische Prozesse anstößt. Im entsprechenden Arbeitsprogramm des Bundesministerium des Innern (BMI) „Europa sicher leben“ kam der IT-Sicherheit große Bedeutung zu.

Zwei Schwerpunktveranstaltungen, die BMI und BSI gemeinsam organisierten, richteten sich an ein internationales Fachpublikum. Der Workshop „Trusted Computing from a European Perspective – The Impact on the Public Sector“ im Februar 2007 führte 70 Trusted-Computing-Experten und IT-Verantwortliche aus 19 EU-Mitgliedstaaten sowie den USA, Japan und Neuseeland zusammen.

Unter dem Motto „Innovation und Verantwortung“ lenkte die internationale IT-Sicherheitskonferenz im Juni 2007 mit 250 Teilnehmern die Aufmerksamkeit auf den Aspekt, wie die Verantwortung für IT-Sicherheit zwischen Staat, Wirtschaft und Bürger zu verteilen ist. Die Ergebnisse beider Veranstaltungen sind auf der Webseite www.itsecurity2007.de dargestellt.

# 2.1 Am Puls der Zeit – Das Lagezentrum des BSI

*Hersteller informieren über Sicherheitsupdates. IT-Sicherheitsspezialisten warnen vor neu entdeckten Schwachstellen. Die Medien berichten über „kritische“ Vorfälle und Bedrohungen. Unzählige Meldungen zur IT-Sicherheit erschweren es den Betroffenen, die Spreu vom Weizen zu trennen.*

Die wahre Bedeutung dieser Nachrichten, die Zusammenhänge und die Folgen erfassen oft nur Teams von Spezialisten mit einem entsprechend umfangreichen Hintergrundwissen. Ein Einzelner ist damit leicht überfordert. Dass der Schutz der Informationstechnik angesichts stetig steigender Risiken und Abhängigkeiten eine besondere Bedeutung besitzt, ist unstrittig.

Erhebungen des BSI (siehe Bericht „Die Lage der IT-Sicherheit in Deutschland 2007“) zeigen, dass vier von fünf Befragten bereits negative persönliche Erfahrungen mit Online-Bedrohungen sammeln mussten. Begriffe wie Viren, Würmer, Trojaner, Spam oder Phishing sind in den allgemeinen Sprachgebrauch übergegangen. Umso mehr stellt sich die Frage, wie die Gesamtsituation der IT-Sicherheit angesichts der Informationsflut ständig korrekt und aktuell erfasst werden kann und welche Reaktion auf eine Einzelinformation angemessen ist. Insbesondere eine unternehmens- und branchenübergreifende Einschätzung auf nationaler Ebene stellt eine besondere Herausforderung dar.

*Bei der Vorstellung des neuen Lageberichts sagte BSI-Präsident Dr. Helmbrecht: „Die Technisierung nimmt zu und immer mehr geschäftliche und private Aktivitäten werden in die virtuelle Welt verlagert. Damit geht weiterhin die Professionalisierung und Kommerzialisierung der IT-Bedrohungen einher.“*


## Die Grundidee

Eine Lösung ist die strukturierte Herangehensweise mit dedizierten, also nur einem bestimmten Zweck gewidmeten Ressourcen. Speziell ausgebildete IT-Experten bearbeiten kontinuierlich die einzelnen Schritte des Arbeitszyklus „Lagebeobachtung – Lagebeurteilung – Entscheidung – Maßnahmen“. Dabei sind nicht nur rein technische Aspekte, sondern auch psychologische Wirkungen, betriebswirtschaftliche Erwägungen

oder auch politische Implikationen zu berücksichtigen. Die folgenden Fragen zeigen die Bandbreite an Problemen auf, die sich bei einem IT-Sicherheitsvorfall stellen können:

- Ist das Vertrauen in eine Institution oder ein Verfahren gefährdet?
- Ist der potenzielle Schaden im Rahmen einer Risikoabwägung tolerabel?
- Welche Folgen hat der Sachverhalt auf die angebotenen Dienstleistungen und Produkte?
- Bekommt das Ereignis eine politische Bedeutung?
- Muss beruhigt oder eskaliert werden?
- Besteht die Gefahr einer Überreaktion?
- Wird das Problem ignoriert oder gar nicht wahrgenommen?

Im Idealfall gehört zur Bewertung von IT-Sicherheit eine interdisziplinäre Betrachtungsweise. Der Sachverhalt ist zu identifizieren und vor allem zu bewerten. Danach geht es um Maßnahmen zur Bewältigung der Situation und zur Eindämmung der Auswirkungen. Arbeitsprozess und Entscheidungskriterien sind klar zu definieren, die Kommunikationsbeziehungen zu regeln sowie Notfallpläne auszuarbeiten. Starre Verhaltensmuster wären hier fehl am Platz: Ein Lagezentrum muss flexibel handeln können, um unvorhergesehene Situationen bewältigen zu können. Vor allem die Bewertung der politischen oder auch unternehmenspolitischen Zusammenhänge hängt sehr stark ab von den Erfahrungen und dem Wissen der eingesetzten Mitarbeiterinnen und Mitarbeiter.

**Politischer Auftrag**

Im „Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI)“ hat die Bundesregierung unter anderem den Aufbau und Betrieb eines Lage- und Analysezentrums beschlossen. Im Koalitionsvertrag wurde vereinbart, den NPSI in dieser Wahlperiode umzusetzen. Neben den weiteren wichtigen Zielsetzungen wird im NPSI insbesondere mit den Zielen 8 und 10 die Absicht verfolgt, jederzeit über ein verlässliches Bild der aktuellen IT-Gefährdungslage in Deutschland zu verfügen. Somit ist die Voraussetzung dafür geschaffen, den Handlungsbedarf und die Handlungsoptionen bei IT-Sicherheitsvorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft schnell und kompetent einschätzen zu können.

Die operative Ausgestaltung wurde mittels spezifischer Umsetzungspläne für die Bundesverwaltung (Umsetzungsplan Bund) und für den Bereich der Wirtschaft, der den so genannten „Kritischen Infrastrukturen“ (Umsetzungsplan Kritis) zuzuordnen ist, erarbeitet. Diese Umsetzungspläne bilden die Basis für den Informationsaustausch. Ziel ist es, die von einem schwerwiegenden IT-Sicherheitsvorfall betroffenen oder gefährdeten Nutzergruppen je nach Eskalationsbedarf zielgruppengerecht zu informieren, zu warnen oder zu alarmieren. Die Reaktionsfähigkeit insgesamt soll verbessert werden, um Gegenmaßnahmen rechtzeitig zu ermöglichen und Schäden in größerem Ausmaß zu vermeiden.

*Der NPSI wurde unter Federführung des Bundesministeriums des Innern (BMI) erstellt. Seine Umsetzung führt zu einer Stärkung des Schutzes der Informationstechnik in Deutschland gegen weltweite Bedrohungen.*


**Operativer Betrieb**

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat als die nationale und kompetente Fachbehörde zum Thema IT-Sicherheit die notwendigen Voraussetzungen geschaffen und betreibt seit Anfang des Jahres 2006 ein Lage- und Analysezentrum. Die Keimzelle bildete hierfür das Computer-Notfallteam für die Bundesverwaltung, das CERT-Bund (Computer Emergency Response Team des Bundes).

Das Lagezentrum hat sich im täglichen Routinebetrieb und bei den herausragenden Großereignissen Fußball-WM 2006 und G8-Gipfeltreffen im Juni 2007 bereits bewährt. Aufmerksam werden Einzelinformationen zusammengetragen und zu Lageberichten verdichtet, welche die jeweils aktuelle IT-Sicherheitslage widerspiegeln. IT-Vorfallsmeldungen können so vor diesem Hintergrund und nach weiterer Aufbereitung interpretiert und bewertet werden. Dabei stellt sich immer wieder heraus, dass zum Zeitpunkt der Erstsichtung und Ersteinschätzung eines Sachverhalts nicht alle Informationen verfügbar sind. Die im Laufe der Zeit nachträglich gewonnenen Informationen können die Ersteinschätzung erheblich verändern.

Eine weitere Erfahrung zeigt, dass jede fundierte Bewertung von der Kenntnis lokaler Rahmenbedingungen abhängt. Erst im Kontext dieser Details sind aussagekräftige Bewertungen möglich. Voneinander abweichende Einschätzungen durch verschiedene Stellen zu ein und demselben Sachverhalt lassen sich häufig darauf zurückführen, dass die lokalen Rahmenbedingungen unterschiedlich eingeschätzt werden oder nicht bekannt sind. Dies verdeutlicht die Herausforderung, der sich ein Analyst stellen muss, um zu bereichsübergreifenden Gesamtaussagen zu gelangen. Indem sich das Fachpersonal des BSI vorrangig auf diese Informationsaufbereitung konzentriert, gelingt es ihm trotz der zuvor genannten Einschränkungen, die IT-Sicherheitslage in einem Gesamtüberblick zu verfolgen. Die einzelnen Meldungen werden im jeweiligen Kontext eingeordnet und unter dem Gesichtspunkt eines nationalen Lagezentrums bewertet. Die Spezialisten stellen sich dieser Herausforderung im wahrsten Sinne des Wortes jeden Tag. Auch Wochenenden und Feiertage bilden keine Ausnahme. Die Mitarbeiter am Lagezentrum analysieren systematisch und regelmäßig verschiedene frei verfügbare, kommerziell betriebene oder auch nicht-öffentliche Informationsquellen.

Diese Erkenntnisse werden durch die Auswertung technischer Sensordaten ergänzt, die ein zentrales Element eines zukünftigen IT-Frühwarnsystems bilden.

*Vom 6. bis zum 8. Juni 2007 fand der G8-Gipfel in Heiligendamm statt. Im Bild: Das „Kempinski Grand Hotel", wo sich die Regierungschefs zu ihren Gesprächen trafen. Das Gebäude war sicherheitstechnisch optimal abgeschirmt.*

**IT-Frühwarnung**

Neue technische Möglichkeiten haben gelegentlich eine Achillesferse! Die Komplexität der heutigen Vernetzung, die verfügbaren hohen Übertragungsbandbreiten sowie die leistungsfähigen angeschlossenen Endgeräte begünstigen teilweise Störungen. Ein Beispiel ist die Massenverbreitung von Schadprogrammen. Das Ausbreitungspotenzial und die theoretisch denkbare Ausbreitungsgeschwindigkeit solcher Schadprogramme erreichen eine Dimension, die scheinbar kaum noch Handlungsspielräume zulässt. Berühmt berüchtigte Schadprogramme wie CodeRed (2001), Slammer (2003) oder Blaster (2003) haben dies in erschreckender Art und Weise eindrucksvoll vor Augen geführt.

Obwohl sich im Zeitalter der Hochgeschwindigkeits-Datenautobahnen die Früherkennung angesichts des ständig kleiner werdenden Zeitfensters schwierig gestaltet, gilt umso mehr für das BSI der Grundsatz: „Früh erkennen, früh warnen, Reaktionszeit verschaffen!". Zwar wird es nur in seltenen Fällen möglich sein, bereits vor Eintritt einer Schadwirkung zu warnen. Doch meist ist davon auszugehen, dass zum Zeitpunkt der Warnung immer noch nicht betroffene oder nur gering betroffene Gruppen existieren. Darüber hinaus werden auch Gegenmaßnahmen empfohlen, die je nach Situation nicht nur präventiv schützen, sondern auch Auswirkungen mindern oder eine zügige Wiederaufnahme des IT-Betriebs ermöglichen.

**Sensoren**

Das Lagezentrum des BSI greift auf unterschiedliche Informationsquellen und Überwachungsnetzwerke für das Internet – so genannte Sensoren – zurück, um frühzeitig Abweichungen vom Normalzustand erkennen zu können. Auch die internen Monitoringsysteme des Regierungsnetzwerkes Informationsverbund Berlin Bonn (IVBB) lassen erste Erkenntnisse zu. Trotz der Bedeutung des IVBB sind dennoch nur bedingt repräsentative Aussagen möglich.

Das BSI hat deswegen ein eigenes datenschutzkonformes Internet-Analyse-System zur Erfassung statistisch relevanter Protokollinformationen entwickelt und betreibt bereits einige Sensoren dieses Systems. Zusätzlich ist ein Framework für ein klassisches,

ereignisorientiertes Sensornetzwerk mit zentraler Auswertungsplattform in der Entstehung. Beiden Entwicklungen ist gemeinsam, dass vor allem Anomalien, die auf Störungen oder Angriffe hinweisen, frühzeitig erkannt und analysiert werden können. Daraus werden zusätzlich Erkenntnisse über die aktuelle Bedrohungslage abgeleitet. Die Qualität der gewonnenen Aussagen ist davon abhängig, wie repräsentativ die gemessenen Stichproben sind. Das BSI sucht daher ständig nach weiteren Kooperationspartnern, die einen Beitrag zu einem nationalen Frühwarnsystem leisten können und weitere Sensoren betreiben. Nur so ist es möglich, die lokal vorliegenden Erkenntnisse den branchenspezifischen oder gesamtübergreifenden Auswertungen gegenüber zu stellen. Dadurch kann festgestellt werden, ob der beobachtete Vorfall vereinzelt, regional oder großflächig auftritt. Notwendige Gegenmaßnahmen können so gezielter in Angriff genommen werden.

### Kooperation und Kommunikation

Gute Organisation und Spitzentechnik sind das eine, das gebündelte Expertenwissen von Spezialisten das andere. Sicherheitsfachleute müssen die Möglichkeit haben, reibungslos national und international kooperieren zu können. Eine wichtige Aufgabe des BSI ist es, solche Kommunikationskanäle nicht nur verfügbar zu halten, sondern auch ihre Vertraulichkeit und Integrität zu garantieren.

### Nationales Lagebild

Die Erkenntnisse aus diesen technischen und nicht-technischen Quellen münden schließlich in einem regelmäßigen Lagebericht. Er hält den aktuellen Sachstand fest und liefert eine Folgeabschätzung aufgetretener Störungen. Basierend auf diesem Wissen können fundierte Entscheidungen getroffen werden. Das Lagezentrum des BSI bildet also einen zentralen Knotenpunkt zur Informationsaufnahme, Informationsverdichtung und Informationsverteilung. Zu Recht gilt dafür das Motto: „Wissen, was geschieht und entsprechend reagieren!“

### Ausblick

Ausgehend vom Nationalen Plan zum Schutz der Informationsinfrastrukturen wird in einem weiteren Entwicklungsschritt das Krisenreaktionszentrum weiter ausgebaut sowie die Reaktionsfähigkeit und -schnelligkeit gestärkt. Wesentlicher Bestandteil der Fortentwicklung ist die Formalisierung der Kommunikationsbeziehungen zu weiteren lokalen und brancheninternen Krisenmanagementorganisationen. Den Schwerpunkt bildet die Verknüpfung des BSI mit weiteren Lagezentren einzelner Behörden der Bundesverwaltung wie dem Lagezentrum des Bundesministeriums des Innern oder des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe. Einerseits können so die Melde- und Alarmierungswege optimiert werden, andererseits wird die Kapazität der Informationsaufnahme und -verarbeitung erhöht.

**Das Lagezentrum des BSI passt sich weiter den wandelnden Anforderungen an. Hier fühlt man sich am Puls der Zeit!**

## 2.2 Der Umsetzungsplan KRITIS

*Im Rahmen des „Nationalen Plans zum Schutz der Informationsinfrastrukturen“ (NPSI) haben BMI und BSI im Jahr 2005 den Auftrag erhalten, einen Plan für den Bereich „Kritische Infrastrukturen“ auszuarbeiten. Der so genannte Umsetzungsplan KRITIS (UP KRITIS) liegt nun vor – als Kooperationsergebnis von Staat und Wirtschaft: An seiner Erstellung haben sich 30 führende Betreiber Kritischer Infrastrukturen beteiligt.*

- **Kritische Infrastrukturen** sind Lebensadern unserer Gesellschaft. Ein Großteil dieser Infrastrukturen wird von der privaten Wirtschaft betrieben. Keine dieser Organisationen und Einrichtungen kann ohne angemessen geschützte Informationsinfrastrukturen ihre Dienstleistungen erbringen.

- **Kritische Infrastrukturen** sind Organisationen und Einrichtungen mit enormer Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten. Dazu gehören unter anderem Krankenhäuser, Flughäfen, Banken, Verkehrsleitzentralen oder Polizeidienststellen.

Dies ist den Betreibern bewusst. Sie haben von sich aus deshalb bereits ein hohes Maß an IT-Sicherheit etabliert. Ein angemessener Schutz der Informationsinfrastrukturen ist aber nicht allein durch Maßnahmen in den einzelnen Unternehmen und Organisationen zu erreichen. Begleitende branchenweite und branchenübergreifende Maßnahmen auf nationaler und internationaler Ebene sind erforderlich.

Deshalb haben sich 30 Betreiber mit dem Bundesministerium des Innern und dem Bundesamt für Sicherheit in der Informationstechnik zusammengefunden, um notwendige Maßnahmen zum Schutz der Informationsinfrastrukturen zu ermitteln und im „Umsetzungsplan KRITIS“ zusammenzufassen. Grundlage sind die im Nationalen Plan zum Schutz der Informationsinfrastrukturen definierten strategischen Ziele: Prävention, Reaktion, Nachhaltigkeit.

Die Zusammenarbeit ist Ausdruck der gemeinsamen Verantwortung von Staat und Wirtschaft. Das Know-how der Betreiber wird gebündelt und die IT-Sicherheit in Deutschland auch in Zukunft nachhaltig gestärkt.

Im gemeinsamen Leitbild heißt es: „Wir arbeiten zusammen, um die Kompetenz und das Know-how der deutschen Wirtschaft und der Bundesregierung in der gemeinsamen Verantwortung für die IT-Sicherheit in den Prozessen Kritischer Infra-

strukturen zu beschreiben. Durch Empfehlungen und Maßnahmen soll dazu beigetragen werden, dass alle Betreiber Kritischer Infrastrukturen ein angemessen hohes Sicherheitsniveau der Informationsinfrastrukturen im Allgemeinen und der in den Unternehmen eingesetzten IT bewahren und weiter ausbauen können. Die langfristige Zusammenarbeit zur Erkennung und Bewältigung von IT-Krisen soll branchenübergreifend gemeinsam mit der Bundesregierung gefördert werden. Unser Ziel ist es, dass sich die Betreiber Kritischer Infrastrukturen aktiv zu den gemeinsamen Grundsätzen bekennen und auf Basis der (im UP KRITIS zusammengestellten) Empfehlungen das IT-Sicherheitsniveau in den Kritischen Infrastrukturen noch weiter erhöhen."

*Auch der Berliner Flughafen Tegel gehört zu den Kritischen Infrastrukturen in Deutschland. Ohne sichere IT würde der Flugbetrieb nicht funktionieren.*


*Polizei, Feuerwehr, Katastrophenschutz, Züge und Flughäfen sind auf sichere Internetverbindungen angewiesen. Ohne sie würde vieles in der Gesellschaft nicht mehr funktionieren.*


## Übungen und Planspiele

Am 5. September 2007 hat das Bundeskabinett den UP KRITIS zur Kenntnis genommen. Der im Umsetzungsplan dargestellte Status Quo des Sicherheitsniveaus zeigt, dass die Betreiber Kritischer Infrastrukturen bereits sehr gut aufgestellt sind. Handlungsbedarf besteht im Bereich der unternehmensübergreifenden Maßnahmen, insbesondere in Bezug auf ein branchenübergreifendes IT-Krisenmanagement. Auf Grundlage einer gemeinsam erarbeiteten Roadmap sollen die im UP KRITIS identifizierten Aufgaben unter fachlicher und organisatorischer Begleitung des BSI in den nächsten Jahren in Angriff genommen werden. Dazu wurden vier Arbeitsgruppen gegründet, die sich mit

- Notfall- und Krisenübungen,
- Krisenreaktion und -bewältigung,
- Aufrechterhaltung kritischer Infrastrukturdienstleistungen und der
- nationalen und internationalen Zusammenarbeit beschäftigen.

Die Arbeitsgruppen sollen durch Übungen und Planspiele Notfall- und Krisenpläne in regelmäßigen Abständen testen und Verbesserungsmöglichkeiten erkunden. Auch eine bessere Kommunikation zwischen den Betreibern Kritischer Infrastrukturen ist eine vorrangige Aufgabe. Das BSI wird mit seinem IT-Lage- und -Analysezentrum Informationen sammeln, bewerten und den Partnern aufbereitet zur Verfügung stellen.

Darüber hinaus wird der Informationsaustausch zwischen den Betreibern Kritischer Infrastrukturen und der Bundesregierung intensiviert, um eine Verbesserung der IT-Sicherheit in Kritischen Infrastrukturen auch auf internationaler Ebene gemeinsam vorantreiben zu können. Auf diese Weise soll in einem gemeinschaftlichen Prozess das Risiko minimiert werden, das durch die immer größer werdende Abhängigkeit von Informationstechnik auch im Bereich Kritischer Infrastrukturen entsteht.

Der Umsetzungsplan KRITIS kann unter publikationen@bundesregierung.de angefordert oder aus dem Web herunter geladen werden unter www.bsi.bund.de/fachthem/kritis/veroeff_upkritis.htm.

Kommentierungen und Anregungen zum Umsetzungsplan KRITIS sind jederzeit erwünscht. Nutzen Sie bitte dazu folgende Adresse:

Bundesministerium des Innern, Referat IT 3
Alt-Moabit 101 D, 10559 Berlin
Telefon: 030-186 81-0
E-Mail: it3@bmi.bund.de

*Beim Umsetzungsplan KRITIS (UP KRITIS) kommt der Wirtschaft eine besondere Bedeutung zu. Rund 85 Prozent der Kritischen Infrastrukturen in Deutschland befinden sich heute in privatem Besitz. Derartige Kooperationen zwischen Staat und der Wirtschaft, aber auch andere Public Private Partnerships tragen zur Verbesserung des Schutzes Kritischer Infrastrukturen bei.*

## 2.3 Das Kompetenzzentrum Datensicherheit

*Das Kompetenzzentrum Datensicherheit ist ein Beratungsangebot des BSI, das im Jahr 2002 eingerichtet wurde. Die Beratungsdienstleistungen standen eng mit der Initiative BundOnline im Zusammenhang. Anfangs erfolgte die Finanzierung aus zentralen Haushaltsmitteln; seit Anfang 2006 müssen entsprechende Dienstleistungen durch die abrufenden Behörden selbst finanziert werden.*

Das Kompetenzzentrum des BSI unterstützt seine Kunden durch Analyse, Beratung, Konzeption, Coaching und Abnahmen in allen Fragen zur IT-Sicherheit. Diese Beratungsdienstleistungen können durch alle Institutionen, Behörden und Zuwendungsempfänger des Bundes abgerufen werden.

Die Fokussierung auf Dienstleistungen im Zusammenhang mit BundOnline 2005 ist entfallen. Anfragen können sich sowohl auf laufende als auch auf zukünftige Projekte beziehen. Die Beratung soll nicht nur die Belange der einzelnen Behörden berücksichtigen, sondern auch die Vorstellungen und Interessen von Bürgern, Verbänden und der Wirtschaft einbeziehen.

### Einsatzgebiete des Kompetenzzentrum Datensicherheit

Auf den folgenden Gebieten ist das Kompetenzzentrum Datensicherheit hauptsächlich tätig:

- Im Bereich **IT-Sicherheitskonzepte** geht es um alle technischen und organisatorischen Fragen rund um die Absicherung der Geschäftsprozesse der Behörden. Dabei wird nicht nur die Neukonzeption entsprechender Vorhaben angeboten, sondern auch die Weiterentwicklung bestehender Lösungen.

  Beispiele sind Schutzbedarfsfeststellungen, Risikoanalysen und umfassende IT-Sicherheitskonzepte im Rahmen der ISO 27001 auf der Basis von IT-Grundschutz.

  Besondere Relevanz bekommt dieser Beratungsbereich im Rahmen der Aktivitäten, die sich durch den Nationalen Plan zum Schutz der Informationsinfrastrukturen in Deutschland – Umsetzungsplan Bund – ergeben.

- Im Fokus des Bereichs **Kommunikationssicherheit** stehen Fragen des Datenschutzes und der Datensicherheit bei der Übermittlung und Bearbeitung vertraulicher (personenbezogener) Daten und die Revisionssicherheit elektronischen Verwaltungshandelns.

  Dabei geht es insbesondere um den Einsatz von Technologien zur elektronischen Signatur, Authentisierung und Verschlüsselung. Besonders wird auf die angemessene technische Umsetzung gesetzlicher Vorgaben sowie die Interoperabilität der verschiedenen Lösungen geachtet.

  Eine wichtige Aufgabe im Rahmen dieses Bereichs ist die Integration der Basiskomponente Datensicherheit in die jeweils bestehende IT-Infrastruktur.

- Das Kompetenzzentrum **Datensicherheit** wird innovative Großprojekte der Bundesregierung in Fragen der IT-Sicherheit begleiten, etwa auf dem Gebiet der Bürgerportale. (Siehe Kapitel 5.1)

  Weiterhin steht das Kompetenzzentrum bereit, die Verantwortlichen für die Projekte „Hoheitliche Dokumente“ einschließlich der E-Card-API und das Bundesmelderegister zu unterstützen.

  Die projektbezogene Arbeit wird um Analysen des Marktangebotes für IT-Sicherheit, Bereitstellung von Grundlagenwissen, Erarbeitung von „Best Practices“ und ein Schulungsangebot ergänzt. Dies stellt den notwendigen Know-How-Transfer zwischen dem Kompetenzzentrum und den Nutzern sicher.

### Spezialisten gewährleisten Kontinuität

Im Kompetenzzentrum arbeiten besonders erfahrene Berater mit Spezialistenwissen in den wesentlichen Bereichen der IT-Sicherheit. Einige Mitarbeiter waren bereits im Rahmen des Projektes Bund Online im Einsatz, so dass die notwendige Kontinuität sichergestellt werden kann.

Weitergehende Informationen zum Kompetenzzentrum sowie zum Abruf von Leistungen können per E-Mail bsi@bsi.bund.de oder telefonisch unter 0228 99 9582-0 erfragt werden.

## 2.4 Recht und Gesetz – Zur Rechtsentwicklung in der IT-Sicherheit

*IT-Sicherheit ist nicht nur ein technisches, sondern auch ein juristisches Problem. Sicherheitslücken in Softwareprogrammen werfen die Frage auf, wer im Schadensfall zur Verantwortung gezogen werden kann. Wer muss welche Maßnahmen ergreifen? Wer haftet in welchem Umfang für die Risiken? Wer muss im Streitfall welche Tatsachen wie beweisen?*

Jeder, der an der Herstellung und dem Einsatz von IT-Produkten beteiligt ist – Hersteller, Dienstleister, Anwender – hat ein Interesse daran, darauf verlässliche Antworten zu erhalten. Nur so kann Rechtssicherheit geschaffen werden.

Aus juristischer Sicht stellt sich zudem die Frage, inwieweit das Recht mit seinen Steuerungsinstrumenten in der Lage ist, den neuen Risiken ausreichend Rechnung zu tragen. In welchem Maße können Hersteller, Nutzer und Dienstleister rechtlich eingebunden werden, um IT-Risiken wirksam zu begegnen? Kann das Recht angesichts der rasend schnellen Entwicklung des IT-Sektors überhaupt noch eine bestimmende Rolle spielen oder hinkt es den ständigen technischen Neuerungen zwangsläufig hinterher? Auch aus staatlicher Sicht stellen sich diese Fragen, wenn es darum geht, Infrastrukturverantwortung im Bereich der IT-Sicherheit zu übernehmen.

### Interdisziplinärer Ansatz

Als für die IT-Sicherheit verantwort-liche Bundesbehörde ist es auch Aufgabe des BSI, sich mit den rechtlichen Aspekten der IT-Sicherheit stärker auseinander zu setzen. Das BSI verfolgt dabei einen interdisziplinären Ansatz, bei dem IT-Experten Hand in Hand mit Juristen arbeiten.

Das erste Projekt trug den Titel „Rechtsentwicklung in der IT-Sicherheit“. Im Jahr 2006 wurde der Auftrag für eine Studie vergeben, in der zunächst die Sicherheitsanforderungen herausgearbeitet wurden, die die Rechtsordnung gegenwärtig an die Herstellung und den Einsatz von Informationstechnik stellt. Das geschieht teilweise in Gestalt von Spezialgesetzen, in erster Linie jedoch durch die Auslegung bestehender allgemeiner Rechtsvorschriften.

Die Studie „Verantwortlichkeiten von Herstellern, Nutzern und Intermediären im Recht der IT-Sicherheit“ ist auf der Homepage des BSI abrufbar:
www.bsi.bund.de/literat/studien/recht/IT-Recht.pdf

## Sensibilisierung für rechtliche Aspekte der IT-Sicherheit

Ausgehend von der Analyse der aktuellen Rechtslage will das BSI verstärkt die Öffentlichkeit für die rechtlichen Aspekte der IT-Sicherheit sensibilisieren und die Diskussion mit allen betroffenen Kreisen suchen. Studien und Veranstaltungen sollen dazu dienen, die Entwicklungen auf dem Gebiet des IT-Sicherheitsrechts zu begleiten. Das BSI hat deshalb im Rahmen seiner Veranstaltungsreihe „BSI im Gespräch“ am 13.06.2007 Vertreter aus Wirtschaft, Verbraucherschutzverbänden, Wissenschaft und Verwaltung in das Besucherzentrum des Bundesministerium des Innern eingeladen, um das Thema „IT-Sicherheit durch Regulierung?“ zu diskutieren. Die dort gehaltenen Vorträge beleuchteten aus verschiedenen Blickwinkeln Erfordernisse gesetzlicher Regelungen von IT-Sicherheit. Die Vorträge der Referenten stehen auf der BSI-Homepage zum Herunterladen bereit.

Die Ausarbeitung eines eigenständigen IT-Sicherheitsrechts hat gerade erst begonnen. Das BSI wird sein Engagement in diesem Bereich kontinuierlich ausbauen. Dazu wird es sowohl europäische wie internationale Trends beobachten, als auch auf Verbände zugehen und nicht zuletzt das Gespräch mit IT-Sicherheitsexperten und Juristen suchen, um eigene Vorschläge auf einer breiten Basis entwickeln zu können. Schließlich setzt das BSI darauf, dass auch in der rechtswissenschaftlichen Literatur das Thema aufgegriffen wird und durch die Zusammenarbeit von Wissenschaft und Praxis eine fruchtbare Diskussion entsteht.

**IT-Sicherheit:**
**bürgerliches und öffentliches Recht**


*„Einheitliche Regelungen oder ein übergreifender Ansatz zur Gewährleistung einer grundlegenden IT-Sicherheit – unabhängig von vertraglichen Regelungen – fehlen; die Strukturen stellen sich als inhomogen dar. Lediglich die Regelungen im Datenschutzrecht bezüglich einer datenschutzsichernden Organisation, die Elemente eines IT-Riskmanagements umfassen, erstrecken sich als spezifisch IT-bezogene Normen breitflächig auf zahlreiche Nutzer und IT-Anbieter. Im geltenden Recht muss daher im wesentlichen auf die allgemeinen Regelungen im bürgerlichen sowie im öffentlichen Recht rekurriert werden.“*

Aus dem Endergebnis des Gutachtens

# 2.5 Der Bericht zur Lage der IT-Sicherheit in Deutschland 2007

*Das BSI veröffentlicht mit dem „Bericht zur Lage der IT-Sicherheit in Deutschland“ alle zwei Jahre einen Überblick über gegenwärtige und künftige Risiken, Herausforderungen und Trends. Ziel ist es, die Öffentlichkeit zu informieren und für IT-Sicherheit zu sensibilisieren. Nur so ist auch weiterhin eine verlässliche Nutzung der Informationstechnik zum Vorteil aller gesellschaftlichen Gruppen Deutschlands gewährleistet.*

Im Bericht werden Bedrohungen untersucht und bewertet, die durch technische Sicherheitslücken und ihre Nutzung entstehen, Chancen und Risiken beim Einsatz innovativer Technologien aufgezeigt und Trends aus den Bereichen Wirtschaft, Gesellschaft, Technik und Recht präsentiert. Er vermittelt zudem einen Überblick über den Umgang verschiedener gesellschaftlicher Gruppen mit der Informationstechnik und stellt dar, welche Hilfen das BSI den unterschiedlichen Zielgruppen in die Hand gibt. Dr. Udo Helmbrecht, Präsident des BSI, stellte den zweiten Bericht „Die Lage der IT-Sicherheit in Deutschland 2007“ auf einer Pressekonferenz im Rahmen des 10. Deutschen IT-Sicherheitskongresses vor.

## Gefährdungspotential erhöht

Der Bericht macht deutlich, dass sich das Gefährdungspotential im Vergleich zum Jahr 2005 erhöht hat. Mit der zunehmenden Verlagerung von geschäftlichen und privaten Aktivitäten in die virtuelle Welt geht auch eine Professionalisierung und Kommerzialisierung der IT-Bedrohungen einher. Es besteht eine anhaltend hohe Bedrohungslage der IT-Sicherheit bei Privatanwendern sowie bei Unternehmen und in Verwaltungen.

Im Jahr 2006 wurden 7.247 neue Sicherheitslücken in Programmen und Betriebssystemen entdeckt – dies ist ein Anstieg um 40 Prozent im Vergleich zum Vorjahr.

Computerschadprogramme stellen die häufigste Angriffsform gegen IT-Systeme und PCs dar; davon wiederum sind Trojanische Pferde und Würmer die größten Gruppen.

Angriffe gegen die Verfügbarkeit eines IT-Systems oder IT-Dienstes stiegen im Jahr 2006 ebenfalls dramatisch an. Eine Ursache dafür ist auch die verstärkte Zunahme von Bot-Netzen, die unter anderem für solche Angriffe aufgebaut oder zur Versendung von SPAM genutzt werden.

## Trend zum modularen Schadprogramm

Neben der Quantität hat sich auch die Qualität der Angriffe auf IT-Systeme von Unternehmen und Privatnutzern gesteigert. Ein Trend bei den Schadprogrammen geht zum Beispiel dahin, diese modular aufzubauen. Kleine Programme, so genannte Downloader, haben zum Ziel, möglichst lange und unbemerkt auf dem Computer aktiv zu sein. Sie können zu bestimmten Zeitpunkten oder auf Anweisung des Angreifers weitere Schadfunktionen aus dem Internet nachladen. Dadurch kann der Angreifer die Schadprogramme auf den infizierten Systemen durch optimierte Versionen ersetzen. Die regelmäßige Veränderung der Dateien erschwert zudem die Erkennung durch Virenschutzprogramme.

Den Anstrengungen zur Erhöhung der IT-Sicherheit auf Seiten der Hersteller, Administratoren und Behörden stehen also kontinuierlich veränderte und angepasste Methoden der Angreifer gegenüber.

Die Autoren der Schadprogramme zielen heute bevorzugt auf Sicherheitslücken in Standardsoftware wie Office-Anwendungen oder Webbrowser ab. Besonders häufig sind die Computer argloser Nutzer im privaten und beruflichen Umfeld Opfer von Infektionen. Die Schadprogramme werden meistens über E-Mail-Anhänge oder präparierte Webseiten verbreitet. Gefährlich sind dabei nicht nur ausführbare Dateien; auch unverdächtige Bilddateien oder Dokumente lassen sich zum Angriff missbrauchen.


*BSI-Präsident Dr. Udo Helmbrecht zusammen mit Referatsleiter Günther Ennen (rechts) und BSI-Pressesprecher Matthias Gärtner (links).*

## Problembewusstsein wächst

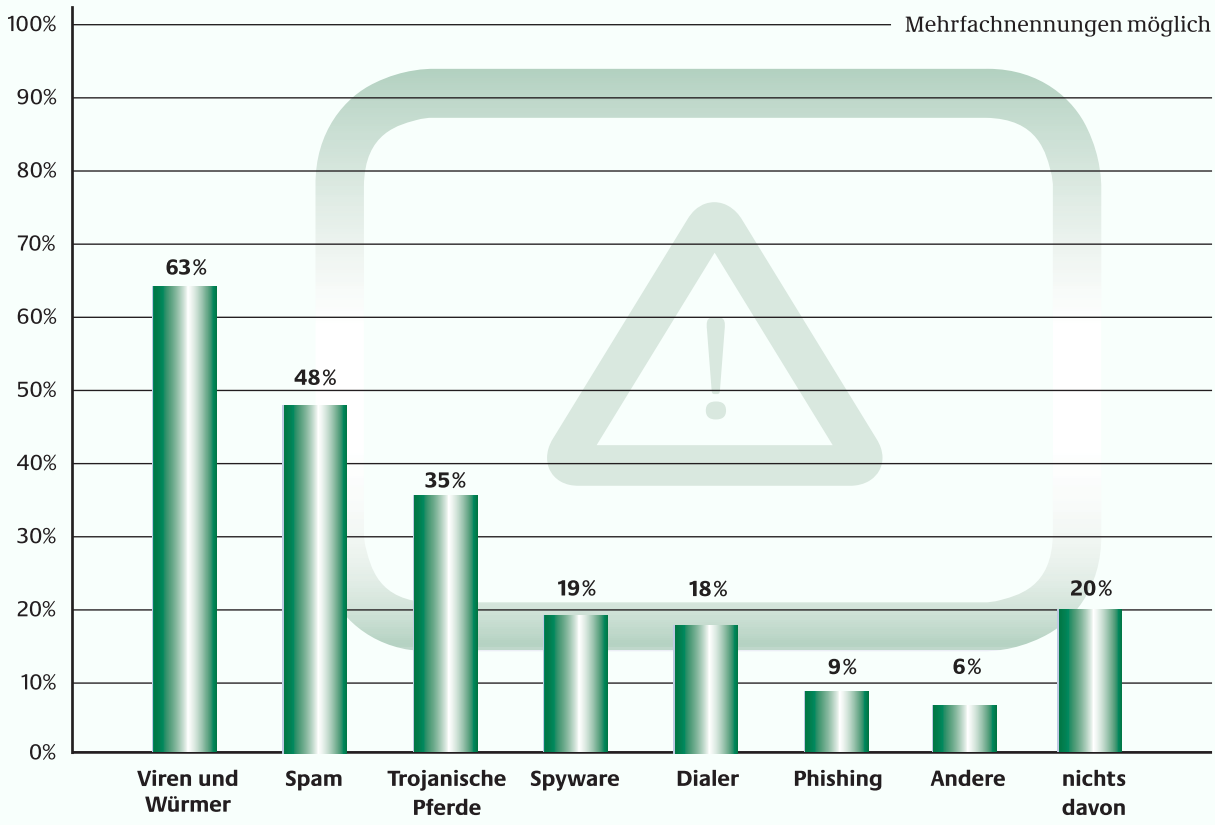
Außerdem enthält der Bericht „Die Lage der IT-Sicherheit in Deutschland 2007“ des BSI Hinweise darauf, wie hoch das Problembewusstsein gegenüber IT-Gefahren beim Bürger, der Wirtschaft und in der Verwaltung ausgeprägt ist. Das Bewusstsein für die Risiken beim Einsatz von Informationstechnik ist in einigen gesellschaftlichen Gruppen im Vergleich zum Bericht aus dem Jahre 2005 stärker geworden. Hier sind, nicht zuletzt durch die Aufklärungsarbeit des BSI, positive Trends festzustellen.

Nach einer Umfrage des BSI im Jahre 2006 haben 90 Prozent der Bürgerinnen und Bürger einen Virenscanner auf dem Computer installiert. Das ist ein Anstieg um 14 Prozentpunkte im Vergleich zum Vorjahr. Auch setzen bereits 52 Prozent eine Personal Firewall ein, immerhin sechs Prozentpunkte mehr als noch im Jahr 2004. In der Wirtschaft herrscht dagegen ein eher heterogenes Bild. Obwohl IT-Sicherheit hier immer wieder als äußerst wichtig erkannt und herausgestellt wird, investieren die Unternehmen insgesamt immer noch zu wenig Geldmittel in die IT-Sicherheit.

## Sicherheitskompetenz weiter verbessern

Trotz dieser positiven Trends: Die aktuelle Lage macht es dringend erforderlich, die Sicherheitskompetenz aller gesellschaftlichen Gruppen weiter zu verbessern. Dazu zwingen vor allem die steigende Qualität der Angriffe, einhergehend mit der Professionalisierung der IT-Kriminalität. Das BSI ergreift seit Jahren umfassende Maßnahmen zur Aufklärung und Sensibilisierung und gibt konkrete Hilfestellungen.

**Persönliche Erfahrung mit Online-Bedrohungen**

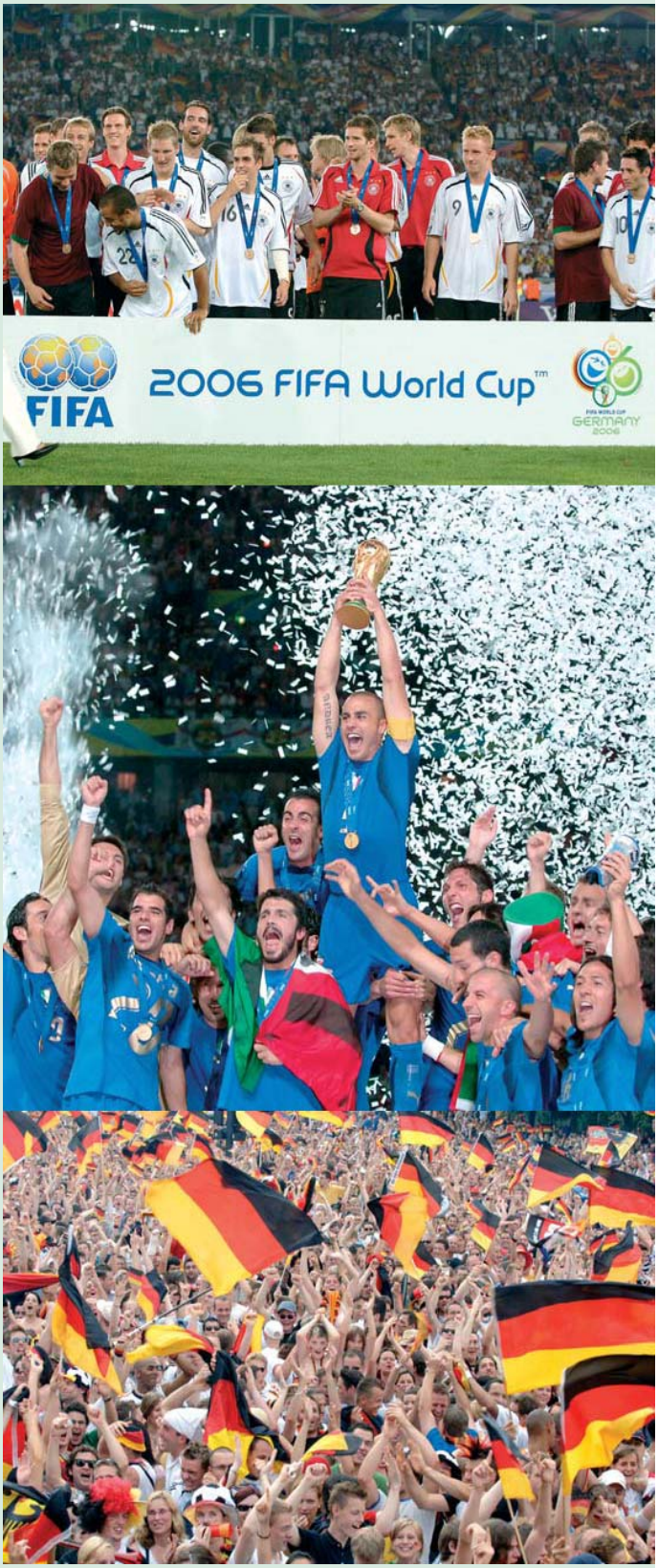



Quelle: BSI

*Mehr als die Hälfte der befragten Nutzer melden sich nicht, wie von Sicherheitsexperten empfohlen, mit beschränkten Benutzerrechten an ihrem Rechner an. Eine Konsequenz daraus: Infektionen mit Computerschädlingen können weit schwerwiegendere Folgen haben. Die Tabelle zeigt: Nur jeder fünfte glaubt, bisher verschont geblieben zu sein.*

# Ein Lederball und die IT-Sicherheit

„Die Welt zu Gast bei Freunden“ – so lautete das offizielle Motto der FIFA Fußball-Weltmeisterschaft Deutschland 2006. Zu einem Besuch bei Freunden gehört auch, dass man sich sicher fühlt. Der Dienst im BSI-Lagezentrum wurde während der WM 2006 verstärkt, damit Gefahren und akute Sicherheitsbedrohungen rechtzeitig erkannt und auf sie reagiert werden konnte. Bis auf die erwarteten Phishing-Angriffe, die zum Ziel hatten, vertrauliche Daten von Fußballfans auszuspionieren, wurden während der WM keine weiteren wesentlichen Störungen registriert.




Zudem engagierte sich das BSI auch im von der Bundesregierung vor und während der FIFA Fußball-Weltmeisterschaft Deutschland 2006 im BMI eingerichteten „Nationalen Informations- und Kooperationszentrum (NICC)“. Aufgabe der Mitarbeiter aus allen Sicherheitsbehörden des Bundes war es, Informationen zu sammeln, zu bündeln und im Verantwortungsbereich des Bundes zu steuern. Das NICC erstellte zudem täglich das „Nationale Lagebild WM 2006“. IT-Experten des BSI koordinierten als so genannte Verbindungsreferenten von Mitte Mai bis Mitte Juli 2006 die Kommunikation zwischen BSI-Lagezentrum und NICC. —› www.itsecurity2007.de

# 3.1 Aktuelle Entwicklungen in der Sicherheitstechnik

*Lösungen für Computerarbeitsplätze, bei denen es auf den Geheimschutz ankommt, die Weiterentwicklung von Verschlüsselungsgeräten und die Ende-zu-Ende-Sicherheit auch bei der drahtlosen Telekommunikation – das sind Beispiele für Sicherheitstechnik in Behörden und Ministerien, die immer wieder an den aktuellen Stand der Leistungsfähigkeit angepasst werden muss. Das BSI berät und entwickelt dabei immer auf dem neuesten Stand.*

Für IT-Arbeitsplätze mit Internetanbindung sind erhöhte Absicherungsmaßnahmen gegen einen Zugriff von außen erforderlich. Bei der Verarbeitung von Verschlusssachen (VS) ist durch die Vorschriftenlage zwingend eine physische Trennung von offenen und als sicher eingestuften Netzen notwendig. Grundsätzlich verboten ist es, an einem IT-Arbeitsplatz gleichzeitig im Internet zu recherchieren und an Verschlusssachen zu arbeiten, wenn keine zugelassenen Sicherungsmaßnahmen vorhanden sind.

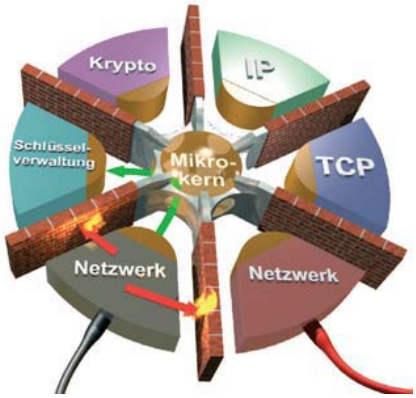
### Sichere Plattformen

Eine Lösung für diese Probleme ist die Einführung eines Multisession-IT-Arbeitsplatzes. Eine Session ist hier durch die Benutzeroberfläche eines Betriebssystems definiert. Der Wechsel der Arbeitsplatzumgebung zwischen den Sessions kann durch eine so genannte Virtualisierung der Hardware erreicht werden. Für diese Virtualisierung ist eine spezielle Software (Virtualisierungsmonitor) notwendig. Sie stellt in enger Kooperation mit einer zentralen vertrauenswürdigen Betriebssysteminstanz (zum Beispiel Mikrokern, Hypervisor) und einem Hardwaresicherheitsmodul (zum Beispiel Smartcard, TPM) die wichtigsten Komponenten einer hochsicheren Plattform dar. Eine Virtualisierung der Hardware ermöglicht unterschiedlichen Betriebssystemen die gleichzeitige Koexistenz auf einem einzigen physischen IT-System und die kontrollierte Verteilung der Hardwareressourcen, wie zum Beispiel den gemeinsamen Zugriff auf das Netzwerk. Der Mikrokern ermöglicht die Überwachung der Systemschnittstellen und realisiert die Kapselung der unterschiedlichen Anwendungen innerhalb des Systems durch geschützte Speicherbereiche.

Das Prinzip der Virtualisierung zur Kapselung eines im Allgemeinen nicht vertrauenswürdigen Gastbetriebssystems sorgt umgekehrt auch für einen zusätzlichen Schutz des Hostbetriebssystems. Zugriffe des Gastbetriebssystems auf Systemressourcen

werden vom so genannten VM-Monitor ausschließlich über die vom Mikrokern bereitgestellte Kommunikationsinfrastruktur erlaubt. Mit der Virtualisierungstechnologie L4-VM stehen die Basiskomponenten einer innovativen und hochgradig modularen mikrokernbasierten Sicherheitsarchitektur zur Verfügung. Der Aufbau der Architektur ist in der Abbildung (siehe unten) dargestellt und liegt als Prototyp vor. Multisession-IT-Arbeitsplätze bieten den Anwendern Flexibilität und erweiterten Komfort. Internet-Recherchen und Online-Buchungen sind beliebte Anwendungen, deren Gebrauch durch netzinterne Richtlinien zwar erlaubt, aber durch Filterung aktiver Inhalte oder Java-Skript meist nicht nutzbar ist. Durch Isolation nicht vertrauenswürdiger Betriebssysteme können diese Beschränkungen aufgehoben werden. Virtualisierung macht es für den Hochsicherheitsbereich auch möglich, Sessions mit unterschiedlichen Einstufungen oder kryptographischen Parametern parallel zu betreiben. Voraussetzung für den sicheren Einsatz aller Lösungen ist die Verwendung vertrauenswürdiger minimalisierter Subsysteme (Trusted Computing Base) in einer modularen Sicherheitsarchitekur.

*Mikrokernbasierte Sicherheitsarchitektur für den Multisessionbetrieb mit „Compartments“. Durch geeignete Virtualisierungstechniken kann der direkte Zugriff der Gastbetriebssysteme auf die gemeinsamen Systemressourcen und den Mikrokern kontrolliert werden.*




## Konfigurierbare Kryptomodule

Bisher gebräuchliche Kryptogeräte für die Verarbeitung von Verschlusssachen mit einer Einstufung von „Geheim“ oder höher machen nach nationaler und nach NATOSicherheitsphilosophie die Hardware-basierte Realisierung von Kryptofunktionen erforderlich. Zu diesem Zweck enthalten beispielsweise SINA-Komponenten für die Verschlüsselung von Daten der Einstufung „Geheim“ einen speziell für diesen Zweck entwickelten Kryptobaustein (Pluto-ASIC). Maskenprogrammierte ASICs mit weitgehend fixierter Funktionalität waren zur Realisierung der hohen Anforderungen im Geheimschutz bisher aufgrund ihrer inhärenten Sicherheitseigenschaften am geeignetsten. Sie erschwerten Manipulationen am vertrauenswürdig gefertigten Baustein ebenso wie die Kenntnisnahme der enthaltenen Kryptofunktionalität. Allerdings ist die statische Funktionalität solcher ASICs auch von Nachteil, da schnelle Anpassungen an spezielle und/oder neue Anforderungen, Spezifikationen oder Einsatzszenarien kaum möglich sind. Daher hat das BSI in einer internen Studie grundlegende Konzepte zu Sicherheitsmodulen erarbeitet, die den hohen Sicherheitserfordernissen im staatlichen Geheimschutzbereich gerecht werden und zugleich ein hohes Maß an Flexibilität ermöglichen – auch für die Kryptofunktionalität. Ausgehend von und basierend auf diesen Konzepten lässt das BSI derzeit eine neue Kryptokomponentengeneration entwickeln.

Durch die Verwendung reprogrammierbarer Logikbausteine, so genannter FPGAs, wird das BSI in die Lage versetzt, schneller auf sich ändernde Anforderungen reagieren zu können. Dabei ist der ladbare Anteil der Sicherheitsfunktionalität durch starke kryptographische Verfahren und die technische Schutzhülle des Sicherheitsmoduls derart abgesichert, dass nur vom BSI geprüfte und autorisierte Gerätekonfigurationen in das Gerät geladen werden können.

Durch die Möglichkeit, mehrere gesicherte Gerätekonfigurationen gleichzeitig im Gerät vorzuhalten, entsteht die für den Hochsicherheitsbereich neue Fähigkeit, die vorhandene Hardware nacheinander mit der jeweils ausgewählten Konfiguration exklusiv verwenden zu können. Jede so vorbereitete Gerätekonfiguration wird im Rahmen des Projektes als Geräteklasse bezeichnet. Der Nutzer legt beim Booten durch das Stecken einer entsprechenden Chipkarte fest, welche der sich möglicherweise sicherheitspolitisch gegenseitig ausschließenden Sicherheitsfunktionalitäten er benötigt und welche Geräteklasse er hierzu laden möchte. Derzeit ist eine nationale Geräteklasse in der Entwicklung. Erste Entwicklungsergebnisse liegen dem BSI zur Analyse vor.

*So genannter Wafer mit der neuen Virtex-5-Plattform für die ultraschnelle Messdatenerfassung.*


## Sicherheitsmanagement moderner Kryptosysteme

### ElcroDat 6-2

Gemeinsam mit dem Unternehmen Rohde & Schwarz hat das BSI dieses Kryptosystem für den Telefon- und Datenverkehr auf Euro-ISDN-Basis entwickelt. Dies ist das erste zugelassene Kryptogerät in der Bundesrepublik, das zur Übertragung bis zu STRENG GEHEIM eingestufter Informationen eine Schlüsselverteilung mit Hilfe eines Public-Key-Verfahrens durchführt. Die in dem Sicherheitsmanagement des Systems eingesetzte Public-Key-Infrastruktur entlastet den Benutzer fast vollständig von der Versorgung der Geräte mit Schlüsselmitteln. Sie beruht auf dem Einsatz von Kryptoverfahren, die auf der Gruppenarithmetik von elliptischen Kurven basieren. Die für den Einsatz des Systems benötigten Kurvenparameter werden vom BSI erzeugt, getestet und den Anwendern zur Verfügung gestellt. Im Rahmen des Sicherheitsmanagements werden die ElcroDat 6-2 Schlüsselgeräte an der Managementstation über Smartcards mit den nötigen Parametern versorgt. Der in den Schlüsselgeräten realisierte Rauschgenerator ermöglicht zusammen mit dem Public-Key-Verfahren die gegenseitige Authentisierung und Schlüsseleinigung.

**SINA**

Mit der „Sicheren Inter-Netzwerk Architektur“ – abgekürzt SINA – stellt das BSI eine Technologie zur Verfügung, mit der sich hochsichere Verbindungen über das Internet aufbauen lassen. Die kryptographischen Mechanismen umfassen den Einsatz von asymmetrischen Kryptoverfahren, zum Beispiel beim Zertifikatsmanagement und beim Verbindungsaufbau. Diese Kryptoverfahren basieren ebenfalls auf der Gruppenarithmetik von elliptischen Kurven. Die dafür benötigten Kurvenparameter werden im BSI unter Einsatz von Großrechnern erzeugt, qualitätsgesichert und SINA-konform aufbereitet, getestet und den Anwendern zur Verfügung gestellt. Die nationalen Zulassungsregeln sehen vor, dass diese Kurvenparameter, dem jeweiligen Einsatzfall entsprechend, turnusmäßig ersetzt werden. Die für den Verbindungsaufbau benötigten Kurvenparameter können beim Vorliegen eines SINA-Online-Kryptomanagements im laufenden Betrieb gewechselt werden. Dies erfolgt auf Basis eines Generationenmodells mittels gesicherter Zugriffe auf die neuen Parameter über einen vom Kryptomanagement eingerichteten LDAP-Server. Im Offline-Fall werden diese Parameter entweder mittels Update-CDs manuell oder durch den Austausch der SINA-Smartcards ersetzt. Bei den im Zertifikatsmanagement eingesetzten Kurvenparametern erfolgt der Austausch über eine entsprechende Wechselprozedur im Rahmen eines Generationenmodells.


*Links: Eine Chipkarte schützt diesen Rechner vor jedem Angriff von Computerschädlingen. Das ElcroDat 6-2 (unten) ist einsetzbar für alle ISDN-Basisdienste, selbst über Satellitenstrecken, für Telefon-, Fax-, Daten- und Video-Kommunikation. Das Gerät ist für die Übertragung von Verschlusssachen aller nationalen Geheimhaltungsgrade der Bundesrepublik Deutschland zugelassen.*

## Absicherung der Regierungskommunikation

Bei der rasanten Fortentwicklung der Telekommunikationsnetze stellt sich die Frage nach geeigneten Sicherheitslösungen immer wieder neu. Schon heute kommen bei einem einfachen Telefongespräch so unterschiedliche Netze und Übertragungstechniken zum Einsatz, dass sie nicht mehr überschaubar sind. Die „sichere Leitung“ gehört damit endgültig der Vergangenheit an. Der Einsatz von Kryptographie an den beiden Enden der Übertragungskette, zum Beispiel in den Telekommunikationsendgeräten oder unmittelbar davor, bietet den stärksten Schutz. Man spricht dabei auch von einer Ende-zu-Ende-Verschlüsselung. Zahlreiche der vom BSI entwickelten Sicherheitslösungen stützen sich auf diesen konzeptionell überlegenen Ansatz. So stellt das ISDN-Verschlüsselungssystem ElcroDat 6-2 die zentrale Ende-zu-Ende-Sicherheitslösung für die sprachgebundene Regierungskommunikation dar. Das System wurde in den vergangenen beiden Jahren technisch weiterentwickelt und an die Erfordernisse moderner Netze angepasst. Die von der Bundeswehr beauftragte Entwicklung des Krypto-Telefons ElcroDat 5-4 wurde vom BSI begleitet und wesentlich mitgestaltet. Für dieses in analogen und digitalen Netzen einsetzbare Telefon liegt bereits eine erste Zulassung vor. Auch in der drahtlosen Telekommunikation gewinnt die Ende-zu-Ende-Verschlüsselung zunehmend an Bedeutung. Für das neue digitale BOS-Netz der Bundesrepublik wurde vom BSI eine solche Verschlüsselung auf Basis einer Chipkarte konzipiert. In den vergangenen beiden Jahren konnten die wesentlichen Teile dieser Neuentwicklung zur Einsatzreife gebracht werden. Sie stehen pünktlich zur Einführung des neuen Netzes zur Verfügung.

Der GSM/UMTS-basierte Mobilfunk ist mittlerweile ein wichtiger Faktor in der Regierungskommunikation. Die Ende-zu-Ende-Verschlüsselung ist für den sicheren Betrieb in öffentlichen Funknetzen besonders wichtig. Das BSI hat in Kooperation mit dem Unternehmen Rhode & Schwarz SIT die Entwicklung einer geräteunabhängigen, externen Lösung gestartet. Eine feste Integration in die Endgeräte wird damit vermieden. Die schnell wechselnden Handy-Generationen würden ständige Neuentwicklungen und einen entsprechend hohen finanziellen Aufwand erforderlich machen.

*Blick auf den Stuttgarter Fernsehturm. Der Mast dient auch zur drahtlosen Übertragung von Telefongesprächen und Internetdaten.*

## 3.2 Geprüfte Sicherheit für den Hochsicherheitsbereich

*In Kooperation mit Industrie und Verwaltung ist das BSI aktiv an verschiedenen zukunftsorientierten Großprojekten beteiligt. Neue technische Herausforderungen stellen unter anderem das Projekt Software Defined Radio (SDR) und das Bundeswehrsatellitensystem SAR-Lupe dar.*

SDR soll eine große Anzahl unterschiedlicher Funksysteme, die im militärischen Umfeld genutzt werden, durch eine einheitliche Technologie ersetzen. Bislang wurden Funksysteme (so genannte Radios) für das militärisch-taktische Umfeld dediziert auf die jeweilige Einsatzanforderung und -plattform abgebildet und mit einem festgelegten Funkverhalten und fester Kryptographie ausgestattet. Das Ergebnis sind viele unterstützte Funkstandards und Geräteplattformen mit einer Vielzahl unterschiedlichster Sicherheitsfunktionen. Daher liegt es nahe, nach einer Lösung zu suchen, die eine Konvergenz hin zu einer Plattform bedeutet, welche in der Lage ist, die unterschiedlichen Anforderungen an Funkstandard, Einsatzplattform und Sicherheitsverfahren im nationalen und Bündnisumfeld zu vereinen.

### SDR – das sichere, militärische Funksystem

Kern der avisierten Lösung ist der Wechsel von der „harten“ dedizierten zur „weichen“ veränderbaren Technologie, also der Wechsel von Hardware definierten Radios hin zu Software definierten Radios (SDR). Und dies gilt für nahezu alle Anteile des Funksystems (Radios). Ähnlich einem leistungsfähigen Rechner kann mit einer Software, der Wellenformsoftware, jeder Funkstandard und jedes Sicherheitsverfahren „geladen“ und auf die jeweilige Anforderung hin konfiguriert werden. Diese Technik sollte es dann für die unterschiedlichen Plattformen geben, so dass die Wellenformsoftware gleichermaßen auf allen Einsatzplattformen betrieben werden kann.

Dass solche Systeme technologisch möglich sind, zeigt das Joint Tactical Radio System (JTRS) Programm der US-Armee. Hier ist für den Bereich der taktischen Datenlinks das MIDS/JTRS als Vier-Linien-System entwickelt worden und soll in mindestens drei der Linien vollständig software-programmierbar sein. Die Anforderungen an die Prüfbarkeit zur Feststellung der Vertrauenswürdigkeit im Rahmen einer NATO-Zulassung wachsen jedoch enorm und stellen eine große Herausforderung dar.

*Vernetzte Operationsführung basiert auf Informationsüberlegenheit. Softwaregestützte Funkgeräte sind dabei unverzichtbar.*

Neben dem Wechsel einer hardware-fixierten zu einer software-definierten Kryptographie für die Datenverschlüsselung und eventuell für Frequenzsprungverfahren (Hopping) sind neue Sicherheitsanforderungen zu bewältigen. Ein SDR-Mehrliniengerät soll linienunabhängig unterschiedliche Wellenformsoftware betreiben können. Es gilt somit, die Linien derart voneinander zu separieren, dass es nicht zur kompromittierenden Beeinflussung zwischen ihnen kommt. Dies ist besonders dann erforderlich, wenn auf den Linien Daten unterschiedlicher Geheimhaltungsgrade übertragen werden und wenn diese Daten unterschiedlicher Hoheit unterliegen (national, NATO, EU). Solch eine Separierung muss somit dem höchsten geplanten Geheimhaltungsgrad genügen. Dem gegenüber steht die Notwendigkeit, Software und Daten (Schlüssel, Konfigurationen) zentral im System zu verwalten und auf die Linien zu verteilen. Innerhalb einer Linie soll der Wechsel von Wellenformsoftware möglich sein, somit auch ein Wechsel der kryptographischen Anteile.

Alle diese neuen Anforderungen müssen unterschiedlichen internationalen Vorgaben standhalten. Zurzeit gibt es kein System, das diese Anforderung berücksichtigt und international anerkannt ist. Es ist keine Lösung in Sicht, die international harmonisierten Ansprüchen gerecht würde. Das BSI ist somit im SDR-Projekt in die Plattformentwicklung wie auch in die Prozesse zur internationalen Anerkennung von Lösungsansätzen einbezogen.

## Die Evaluierung von SAR-Lupe

Informationssichernde Systeme, welche Daten und Informationen verarbeiten, die als Verschlusssachen (VS-Anweisung – VSA) eingestuft sind, bedürfen einer Zulassung durch das BSI. Im Rahmen eines solchen Verfahrens ist die Evaluierung der entsprechenden Produkte notwendig. Dieser Evaluierungsprozess ist immer sehr produktspezifisch und muss entsprechend individuell gestaltet werden. Das Verfahren wird im nachfolgenden am Beispiel des deutschen Aufklärungssatelliten SAR (Synthetic Aperture Radar)-Lupe beschrieben. Im Dezember 2006 wurde der erste deutsche Aufklärungssatellit – SAR-Lupe – gestartet. Er hat mittlerweile alle Tests im Weltraum bestanden. Der zweite Satellit der Baureihe wurde am 2. Juli 2007 erfolgreich gestartet. Im nächsten Jahr folgen noch drei weitere Satelliten des gleichen Typs. Sie werden im Weltraum ein Gesamtsystem bilden.

*Ein Techniker testet die Leistungsfähigkeit der Solarzellen des SAR-Lupe Satelliten.*

Das BSI hat über mehrere Jahre und durch alle Projektphasen hindurch maßgeblich an der IT-Sicherheit dieser Satelliten und des Gesamtsystems mitgearbeitet. Zuerst wurde ein kryptographisches Konzept entwickelt und der Systemhersteller bei der Umsetzung beraten. Später folgte dann seitens des BSI die Evaluierung. Das Besondere an diesem Projekt war und ist: Es gibt in Deutschland bisher keine vergleichbaren Systeme. Für die besonderen Anforderungen der Raumfahrt mussten außerdem immer wieder neue Problemlösungen gefunden werden. Das galt besonders für die Evaluierung: Es gab kein eigenes Exemplar des Prüfobjektes. Aus diesem Grund wurden in den vergangenen drei Jahren Tests beim Hersteller in Bremen vorgenommen.

Auch wenn jetzt der erste Satellit im Orbit seinen Betrieb aufgenommen hat, ist die Arbeit des BSI noch längst nicht abgeschlossen, denn auch für die drei im Abstand von jeweils rund vier Monaten noch folgenden Satelliten müssen Systemprüfungen durchgeführt werden. Inzwischen hat das BSI die Zulassung für die Verarbeitung von Daten und Informationen bis einschließlich der VS-Einstufung Geheim erteilt. Doch das Projekt ist noch nicht beendet. Der nächste Schritt ist die Erweiterung des Systems im Sinne einer Kooperation mit anderen Nationen. Und hier ist wieder das BSI gefragt, wenn es darum geht, die IT-Sicherheit und den nationalen Geheimschutz sicherzustellen.

*SAR-Lupe ist das erste satellitengestützte Aufklärungssystem Deutschlands. Es besteht aus fünf baugleichen Kleinsatelliten und einem Bodensegment. Das Computermodell zeigte einen der Satelliten beim Umrunden der Erde.*

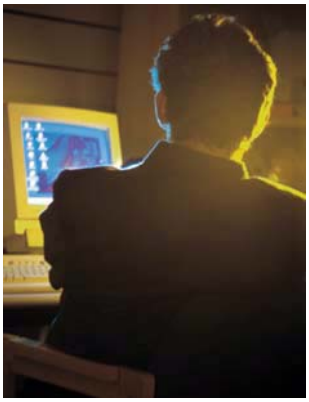
## 3.3 Abstrahlsicherheit

*Kompromittierende Strahlung ist heute zu einem Sicherheitsproblem auch ziviler Computernutzung geworden, besonders für Unternehmen. Eine gute Abschirmung dieser elektromagnetischen Strahlung durch die umgebende Bausubstanz erschwert das unbefugte Aufnehmen und Entschlüsseln. Eine Studie des BSI in Zusammenarbeit mit der Universität Hannover untersucht, wie eine wirksame Abschirmung kostengünstig realisiert werden kann.*

Jedes elektronische Gerät erzeugt im Betrieb mehr oder weniger starke Störemissionen. Bei IT-Geräten können diese Emissionen auch die gerade verarbeiteten Informationen transportieren. Wer die Strahlung empfängt, kann die verarbeiteten Daten aus einiger Entfernung mitlesen. Die Vertraulichkeit der Daten ist nicht mehr gegeben. So lässt sich zum Beispiel aus der Störstrahlung von Computerbildschirmen der gerade dargestellte Bildschirminhalt rekonstruieren. Diese Emissionen werden als „kompromittierende Abstrahlung“ bezeichnet.

Ein probates Mittel, die Abhörgefahr durch kompromittierende Abstrahlung vor Ort messtechnisch zu bewerten, ist das vom BSI entwickelte Zonenmodell (siehe Jahresbericht BSI 2005).

*Gerade, wenn ein Computernetz jedem Angriff widersteht oder Daten verschlüsselt sind, ist das Belauschen der Abstrahlung eine Alternative. Man geht davon aus, dass es allein in Deutschland jedes Jahr mehrere hundert Versuche gibt, die Abstrahlung von Monitoren, Computern, Tastaturen oder Druckern zur Informationssammlung zu nutzen.*



### Spätere bauliche Veränderungen sind teuer

Ergibt die Überprüfung vor Ort, dass die Abschirmwirkung eines Gebäudes nicht ausreicht, um das vorgegebene Schutzziel zu erreichen, können nachträglich bauliche Maßnahmen erforderlich werden, die mit hohen Kosten verbunden sind. Günstiger wäre es, bereits in der Planungsphase die erforderliche Abschirmwirkung zu ermitteln. Bisher konnten sich Voraussagen zum Dämpfungsverhalten von Baukörpern in der Planungsphase nur auf empirisch ermittelte Erkenntnisse stützen.

## Von Beton bis Kupfer

Um die aus vielen Messreihen an Gebäuden gewonnenen Erfahrungswerte durch Laborexperimente abzusichern und der Öffentlichkeit in systematischer Form zugänglich zu machen, hat das BSI die Studie „Untersuchung der elektromagnetischen Dämpfung von Baukörpern“ beauftragt. Im Rahmen dieser Studie wurde eine Technische Leitlinie (TL) erstellt. Sie bewertet vierzig verschiedene Baumaterialien: von der Betonmauer bis zur Kupfertapete. Damit werden bei der Planung von Gebäuden mit Sicherheitscharakter Entscheidungshilfen bei der Auswahl der richtigen Baumaterialien gegeben. Gleichwohl ist die TL auch ein hilfreicher Ratgeber, wenn ein Gebäude gegen das Eindringen von äußeren Störemissionen (Stichwort Elektrosmog) geschützt werden soll. Die technische Leitlinie wird 2008 auf der Website des BSI veröffentlicht.

*Blick in eine Messkabine: Solche Magnetfeldmessungen geben Aufschluss über den Grad der Abschirmung.*

## 3.4 Das Programm zur Stärkung der Inneren Sicherheit (PSIS)

*In den Mittelpunkt seines Handelns stellt das BSI die Aufgabe der Prävention. Schwachstellen bei Hardware, Software und in Netzen werden analysiert und in Kooperation mit den Herstellern, Anbietern und Anwendern bereinigt. Die aktuelle Gefährdungslage hat einen maßgeblichen Einfluss auf die Wahrnehmung dieser Aufgabe.*

Die im Jahre 2006 aufgedeckten und vereitelten Terroranschläge machten sehr deutlich, dass Deutschland sich mitten in einem Gefahrenraum befindet, der unmittelbar von weltweit wirkenden Einflüssen bestimmt ist. Eine Entspannung der Sicherheitslage ist auf absehbare Zeit nicht zu erwarten. Der potentielle Täterkreis und ihre vermutlichen Anschlagsziele sind nur mit großen logistischen und personellen Anstrengungen zu ermitteln. Dies führt zu neuen und komplexen Anforderungen, denen sich die Sicherheitsbehörden stellen müssen. Das BSI unterstützt im Rahmen seines gesetzlichen Auftrages nach § 3 BSIG die Sicherheitsbehörden mit Konzepten und Methoden bei der IT-Sicherheit der einzusetzenden Informationstechnik.

Seit mehreren Jahren ist das BSI als zentraler IT-Sicherheitskompetenzträger in Deutschland mit den Grundlagen und den Einsatzmöglichkeiten der Biometrie befasst. Bisherige Einsatzfelder der Biometrie sind ePass (elektronischer Reisepass) und der geplante elektronische Personalausweis. Biometrische Verfahren sind darüber hinaus geeignet, bei besonderen Bedrohungslagen notwendige Personenidentifikationen und Personenkontrollen effektiv und sicher zu unterstützen.

Regierungsnetze und kritische Infrastrukturen in der Wirtschaft sind lohnende Ziele für terroristische Angriffe. Die Innen- und Justizminister der EU haben die Bedrohung durch Cyberangriffe in 2005 als eine der neuen Bedrohungsformen identifiziert und sich der Bekämpfung angenommen. Die Entwicklung technischer Lösungen zur Detektion und Abwehr von terroristischer Infiltration in kritischen Kommunikationsnetzen durch das BSI bilden die technischen Voraussetzungen für Maßnahmen der Sicherheitsbehörden.

Zu einer erfolgreichen Detektion und Abwehr wird zwingend eine unverzügliche, verlässliche und vertrauliche Verteilung von Früherkenntnissen an alle relevanten Stellen notwendig. Die Bereitstellung einer vertrauenswürdigen und hochverfügbaren Kommunikationsinfrastruktur für den schnellen, mobilen und grenzüber-

schreitenden Austausch von Informationen muss sich auf verlässliche IT-Sicherheitskomponenten des BSI abstützen.

Das BSI erhielt aus dem Programm PSIS kein zusätzliches Personal, sondern Haushaltsmittel in Höhe von insgesamt vier Millionen Euro. Diese zusätzlichen Mittel wurden für die Erarbeitung und Bewertung neuartiger konzeptioneller Ansätze und Verfahren eingesetzt. Das BSI hat Projekte in drei Bereichen initiiert, die sich wiederum in mehrere Einzelmaßnahmen untergliedern:

## 1. Biometrie-gestützte Früherkennung von terrorverdächtigen Personen bei bildverarbeitenden Überwachungen

- **Auto-Erkennung**
  Konzeption eines Verfahrens zur automatisierten Erfassung und Erkennung von biometrischen Merkmalen unter Echtzeitbedingungen;

- **MitarbeiterIdent**
  Konzeption eines Verfahrens, um mittels elektronischer Mitarbeiterausweise mit Biometrie-Merkmalen Kontrollen für Mitarbeiter in kritischen Bereichen, wie Flughäfen, zu optimieren;

- **Trackingsystem**
  Konzeption kombinierter RFID- und Biometrie-gestützter Verfahren zur Verfolgung des Personen- und Gepäck-/Gütertransports in besonders gefährdeten öffentlichen Verkehrsbereichen.

*IT-Sicherheit ist heute zu einem entscheidend wichtigen Bestandteil der Inneren Sicherheit geworden. Im Blick: Regierungsgebäude*

## 2. Detektion und Abwehr terroristischer Infiltration in kritischen Kommunikationsnetzen

- Schaffung der technischen Infrastruktur zur Beobachtung der Steuerkanäle von Bot-Netzen;
- Erarbeitung von Maßnahmen zur Behinderung von Bot-Netzen durch Abschaltung, Übernahme oder Überlastung;
- Erarbeitung von Maßnahmen zum Schutz von kritischen Kommunikationsnetzen gegen Angriffe auf die Verfügbarkeit (Denial of Service Angriffe).

### 3. Sichere Kommunikationsinfrastrukturen zur Früherkennung terroristischer Aktivitäten

- Konzeption von sicheren und verfügbaren Kommunikationsarchitekturen und -infrastrukturen, ausgerichtet auf die speziellen Anforderungen der Verteilung und Auswertung von Früherkenntnissen aus dem terroristischen Umfeld;
- Intensivierte Beratung und Unterstützung der Sicherheitsbehörden beim Aufbau sicherer Netze;
- Entwicklung von innovativen sicheren Kommunikationskomponenten.

Insgesamt hat das BSI 22 Projekte initiiert, die geeignete Lösungen zur Erreichung der Ziele erbringen werden. Sie reichen von Projekten zur Sensibilisierung der Bürger und Mitarbeiter in Behörden über Rechtsgutachten und die Beobachtung von Bot-Netzen bis hin zur Entwicklung von Hardwaresystemen, die geeignet sind, hochvertrauliche Verschlusssachen sicher zu transportieren.

**PSIS-Projekte (Auswahl)**

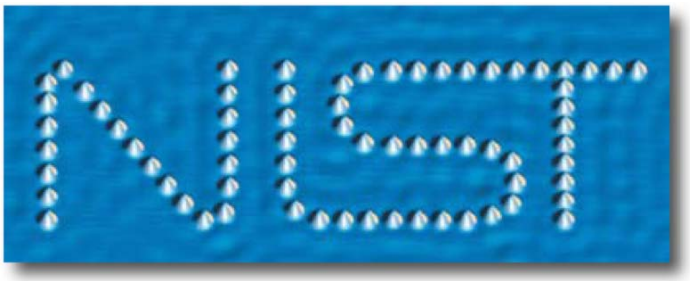
- Untersuchung von Schwachstellen, Designschwächen, typischen Konfigurationsfehlern von Windows Vista, die zur Verbreitung und Installation von Bots genutzt werden können.
- Rechtsgutachten über Maßnahmen zur Beobachtung und Bekämpfung von Bot-Netzen.
- Entwicklung eines sicheren Boot Tokens inklusive eines Antitampermechanismus für mobile SINA Clients.
- Absicherung des EU-Visumaufklebers durch die Entwicklung von drucktechnisch integrierbaren elektronischen Sicherheitsmerkmalen zum Schutz von maschinenlesbaren Daten und Lichtbildern gegen Fälschung und Verfälschung.
- Erweiterung von Gpg4win und S/MIME-Funktionalität, sowie Verbesserung der Integration in Outlook und der Handbücher/Dokumentationen, so dass Behörden, Bürger, Unternehmen E-Mails mit automatischer Authentizitäts-, Integritäts- und Vertraulichkeits- Sicherung senden und empfangen können.
- Untersuchung der Machbarkeit eines signaturunabhängigen Schutzprogramms zur Abwehr von Bot-Netzen.
- Synchronisation eines niederländischen Lehrfilms über Schadprogramme, um Internetnutzer prägnant und verständlich über die Gefahren durch Schadprogramme bei der Nutzung des Internets aufzuklären.
- Prototypische Implementierung von biometrischen Mitarbeiterausweisen unter Verwendung von BioMiddle und EA EAC-Chipkarten.

# 3.5 Aktuelle Entwicklungen in der Kryptographie

*Signieren, chiffrieren, verschlüsseln – ein großer Teil der Forschung im Bereich Verschlüsselungstechniken basiert auf internationaler Zusammenarbeit. Ein Einblick in den „Kompetenzbereich Kryptographie" – ein Feld, auf dem das BSI sich ganz vorne in der Spitzengruppe der einschlägigen Forschungen bewegt.*

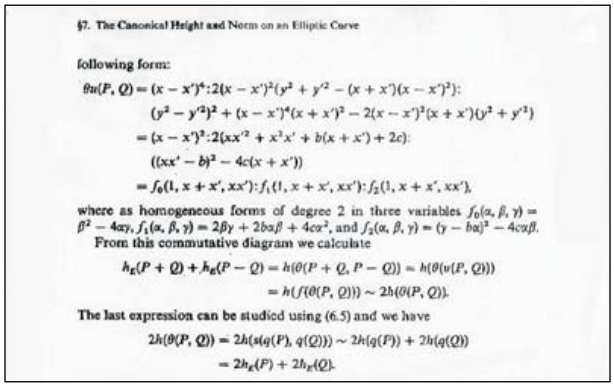
Kryptographische Hashfunktionen spielen unter anderem bei der Erstellung digitaler Signaturen eine zentrale Rolle. Unverzichtbar ist in diesem Kontext die so genannte Kollisionsresistenz: das heißt, es soll praktisch nicht möglich sein, zwei unterschiedliche Urbilder anzugeben, die denselben Hashwert besitzen. Weltweit verbreitet ist der von der US-Behörde National Institute of Standards and Technology (NIST) standardisierte SHA-1-Algorithmus. Anders als zum Beispiel beim MD5-Hashalgorithmus sind zwar bislang keine SHA-1-Kollisionen bekannt, aber 2005 gelang es einem chinesischen Forscherteam, erstmals Schwächen aufzudecken.

Seitdem ist offenkundig, dass das Sicherheitsniveau des SHA-1 deutlich geringer ist als dies Experten zuvor angenommen hatten. Inzwischen hat eine Forschergruppe aus Graz Kollisionen für eine reduzierte SHA-1-Variante gefunden. Gegenwärtig ist diese Gruppe dabei, eine Kollision für den vollständigen SHA-1-Algorithmus zu suchen. Hierfür werben sie um Mitstreiter, die für dieses Projekt kostenlos Rechenzeit zur Verfügung stellen.



Die US-Behörde NIST hat daher beschlossen, einen Wettbewerb auszurufen, um einen neuen Hash-Standard zu ermitteln. Im Oktober 2005 und August 2006 fanden in den USA zwei vorbereitende internationale Workshops statt, an denen jeweils mehr als 170 Vertreter von Hochschulen, Behörden und Industrie teilnahmen. Der Kompetenzbereich Kryptographie des BSI war auf beiden Workshops mit Vorträgen präsent. Nach einem weiteren Workshop im Mai 2007 in Spanien plant NIST, den avisierten Wettbewerb in Kürze auszurufen. Der neue Standard soll dann bis Ende 2012 in Kraft treten.

*Sitz der Bundesnetzagentur im ehemaligen Bonner Regierungsviertel (rechts). Sie veröffentlicht jährlich den maßgeblichen „Algorithmenkatalog.“ Mathematik ist heute mehr denn je gefragt, wenn es um neue kryptographische Verfahren geht (unten).*



§7. The Canonical Height and Norm on an Elliptic Curve

following form:

$$\theta u(P,Q) = (x-x')^4 : 2(x-x')^2(y^2+y'^2-(x+x')(x-x')^2):$$
$$(y^2-y'^2)^2+(x-x')^4(x+x')^2-2(x-x')^2(x+x')(y^2+y'^2)$$
$$= (x-x')^2 : 2(xx'^2+x^2x'+b(x+x')+2c):$$
$$((xx'-b)^2-4c(x+x'))$$
$$= f_0(1, x+x', xx') : f_1(1, x+x', xx') : f_2(1, x+x', xx'),$$

where as homogeneous forms of degree 2 in three variables $f_0(\alpha,\beta,\gamma) = \beta^2 - 4\alpha\gamma$, $f_1(\alpha,\beta,\gamma) = 2\beta\gamma + 2b\alpha\beta + 4c\alpha^2$, and $f_2(\alpha,\beta,\gamma) = (\gamma - b\alpha)^2 - 4c\alpha\beta$.

From this commutative diagram we calculate

$$h_E(P+Q)+h_E(P-Q) = h(\theta(P+Q, P-Q)) = h(\theta(u(P,Q)))$$
$$= h(f(\theta(P,Q))) \sim 2h(\theta(P,Q)).$$

The last expression can be studied using (6.5) and we have

$$2h(\theta(P,Q)) = 2h(s(q(P), q(Q))) \sim 2h(q(P)) + 2h(q(Q))$$
$$= 2h_E(P) + 2h_E(Q).$$

## Hashfunktionen und der Einfluss auf das Signaturgesetz

Berücksichtigt man Vorlaufzeiten und die Lebenszyklen von Chipkarten, kann man davon ausgehen, dass andere Hashfunktionen als der zukünftige Standard mindestens noch bis 2018 im Feld sein werden. Bei sicherheitskritischen Signaturanwendungen ist es unbedingt erforderlich, den SHA-1-Algorithmus möglichst rasch zu ersetzen. Als „Zwischenlösung“ bis zum Inkrafttreten des neuen Standards kommen insbesondere Vertreter der SHA-2-Familie in Frage. Die (Un-)Sicherheit von Hashfunktionen wie SHA-1 ist unter anderem auch relevant für qualifizierte elektronische Signaturen (q.e.S.) nach dem deutschen Signaturgesetz (SigG). Rechtlich maßgeblich für die Zulässigkeit von Algorithmen und Parametern (u.a. Schlüssellängen) für q.e.S. ist ein von der Bundesnetzagentur (BNetzA) alljährlich im Bundesanzeiger veröffentlichtes Papier, kurz „Algorithmenkatalog“ genannt.

Der für Signaturanwendungen gegenwärtig überwiegend eingesetzte SHA-1-Algorithmus ist zurzeit noch für q.e.S. zugelassen. Auf Grund der oben skizzierten Entwicklung vertritt das BSI seit zwei Jahren die Auffassung, dass der Gültigkeitszeitraum für den SHA-1 Algorithmus verkürzt werden sollte.

## Neue Stromchiffren gesucht

Vor einigen Jahren wurde der Blockchiffrieralgorithmus AES von NIST standardisiert. Obwohl Stromchiffren in vielen Anwendungen eine wichtige Rolle spielen, existiert keine standardisierte Stromchiffre. Im November 2004 wurde der erste Call for Primitives im Algorithmenwettbewerb „eSTREAM – ECRYPT Stream Cipher Project“ veröffentlicht. Das erklärte Ziel ist es, neue Stromchiffren zu identifizieren, die als geeignet angesehen werden können. Der Wettbewerb wird voraussichtlich im Mai 2008 zu Ende gehen.

## Asymmetrische kryptographische Algorithmen

Aufgrund internationaler Vereinbarungen (EU/NATO) werden zumindest im Hochsicherheitsbereich die Schlüssellängen ansteigen. Schlüssellängen für symmetrische Verfahren werden in Zukunft typischerweise 256 Bit, für auf elliptischen Kurven basierende asymmetrische Verfahren mindestens 384 Bit betragen. Die Grundsatzentscheidung fiel zugunsten elliptischer Kurven aus, die endgültige Algorithmenentscheidung wird durch Patentfragen erschwert. Moderne Kryptogeräte werden zukünftig nicht mehr auf Spezial-ASICs basieren. Vielmehr lassen sie den gesicherten Download von Algorithmen zu, die auf rekonfigurierbarer Hardware ausgeführt werden. Es gilt innovative Methoden zur Sicherung dieser Downloads zu entwickeln, die Quantencomputer-resistent und auch dann noch sicher sind, falls die gegenwärtig genutzten Hashfunktionen gebrochen werden sollten.

Fortschritte in der Krypto-Analyse bedingen auch eine Erhöhung der Schlüssellängen bei q.e.S. nach SigG. Bei den derzeit verwendeten Signaturkarten spielt das RSAVerfahren eine zentrale Rolle. Bis Ende 2007 wird im Algorithmenkatalog (siehe „Hashfunktionen“) eine Schlüssellänge von 1024 Bit für RSA als ausreichend betrachtet, während zum Beispiel ab Anfang 2011 eine Mindestschlüssellänge von 1976 Bit gefordert wird. Langfristig könnten auch q.e.S.-Verfahren eine größere Bedeutung erlangen, die auf elliptischen Kurven basieren.

## ECC für hoheitliche Dokumente

Wie bereits erwähnt, setzen sich auf elliptischen Kurven basierende Public-Key-Verfahren immer weiter durch. Konsequenterweise hat sich das BSI maßgeblich an der Entwicklung von Standardkurven und der Festlegung von Sicherheitskriterien für Kurven beteiligt, die im Rahmen des ECC-Brainpools erfolgte. Mitglieder des Brainpools sind neben dem BSI zahlreiche weitere Unternehmen und Universitäten, die sich im Bereich der ECC-Technologie engagieren; insgesamt umfasst die Arbeitsgruppe heute zirka 25 Mitgliedsunternehmen und -institute. Weitere Informationen finden sich unter www.ecc-brainpool.org.

Dort sind zudem die standardisierten Parameter verfügbar. Die Brainpool-Kurven werden auch als Internet-Draft der IETF diskutiert; ein entsprechender Draft findet sich unter https://datatracker.ietf.org/drafts/draft-lochter-pkix-brainpool-ecc/.

Bereits jetzt werden zwei dieser Kurven als Grundlage zur Berechnung von Signaturen eingesetzt, die zur Authentizitätssicherung der in den RF-Chips der deutschen Reisedokumente gespeicherten Daten dienen. So benutzt die deutsche Country Signing Certification Authority, die vom BSI betrieben wird, die Brainpoolkurve brainpoolP256r1, der deutsche Document Signer, betrieben von der Bundesdruckerei GmbH, die Brainpoolkurve brainpoolP224r1. Ähnliche Mechanismen werden im zukünftigen elektronischen Personalausweis eingesetzt. Geplant ist weiterhin, auch im Umfeld der elektronischen Gesundheitskarte standardisierte Brainpoolkurven ab dem Jahr 2010 zu benutzen.

## Quantenkryptographie und quantencomputerresistente Kryptoverfahren

Falls es gelingt, Quantencomputer in entsprechender Größenordnung zu realisieren, sind derzeit weit verbreitete kryptographische Algorithmen (zum Beispiel RSA) de facto gebrochen. Obwohl sich Quantencomputer derzeit noch in der Phase der Grundlagenforschung befinden, befasst sich die Forschung im Hinblick auf Daten, deren Vertraulichkeit, Integrität und Authentizität über einen sehr großen Zeitraum gewährleistet werden sollen, bereits heute mit dieser Thematik. Dazu versucht man einerseits, „klassische“ Algorithmen zu entwickeln, die resistent gegen Angriffe mit Quantencomputern sind. Umgekehrt nutzt die Quantenkryptographie quantenmechanische Eigenschaften (von Photonen) zur Verschlüsselung. Im Rahmen des Zukunftsfonds leitet das BSI auch das Cluster „Quantencomputerresistente Kryptoverfahren und Sicherheitstechnologien“.

## Seitenkanalangriffe gegen Hardware- und Softwareimplementierungen

Die Sicherheit kryptographischer Systeme hängt zunächst von der Sicherheit der verwendeten kryptographischen Algorithmen und Protokolle gegen kryptanalytische Angriffe ab. Von größter Wichtigkeit ist aber auch die Resistenz der Implementierung gegen Seitenkanalangriffe. Seitenkanalangriffe werden seit etwa zehn Jahren sowohl im universitären wie im industriellen Umfeld intensiv studiert. Seitenkanalangriffe versuchen, beispielsweise aus der Laufzeit einer kryptographischen Operation, dem Stromverbrauch oder der elektromagnetischen Abstrahlung einen geheimen Schlüssel zu bestimmen. Konzentrierte man sich in den Anfangsjahren auf Chipkarten, so sind inzwischen auch Softwareimplementierungen ins Visier geraten (zum Beispiel cachebasierte Angriffe). Man darf davon ausgehen, dass Seitenkanalangriffe auch in den kommenden Jahren eine wichtige Rolle spielen werden.

## Fault Attacks

Ebenso wie Seitenkanalangriffe versuchen auch Fault Attacks, etwaig vorhandene Implementierungsschwachstellen auszunutzen. Anders als bei den Seitenkanalangriffen verhält sich der Angreifer jedoch nicht passiv (d.h. nur beobachtend). Stattdessen versucht der Angreifer, durch gezielte Einflüsse eine Chipkarte oder eine Softwareimplementierung zu fehlerhaften Berechnungen zu bewegen, um daraus den gesuchten Schlüssel zu bestimmen. Fault Attacks dürften auch in den kommenden Jahren von Bedeutung sein.

## Zufallszahlengeneratoren für kryptographische Anwendungen

Viele kryptographische Mechanismen benötigen Zufallszahlen (zum Beispiel als Sessionkeys). Schwache Zufallszahlengeneratoren können ansonsten starke kryptographische Mechanismen entscheidend schwächen. Im deutschen Zertfizierungsschema sind seit mehreren Jahren die AIS 20 und die AIS 31 verbindlich, die die Evaluierung von deterministischen bzw. physikalischen Zufallszahlengeneratoren festlegen. Die beiden Evaluierungsvorschriften haben sich in der praktischen Anwendung bewährt. Zentrale Ideen der AIS 31 sind in die ISO-Norm 18031 „Random Bit Generation“ eingeflossen. Forschungsgruppen aus dem Hochschulbereich und Halbleiterunternehmen präsentieren regelmäßig neue Design-Vorschläge für physikalische Zufallszahlengeneratoren.


*Fälschungssichere Chipkarten sind ein Gegenstand der sicherheitstechnischen Forschungsarbeit im BSI.*

# IT-Grundschutztage
# Jahrestagung – IT-Sicherheitsbeauftragte


## Rekordbesuch beim Treffen in Berlin

Auch wenn IT-Grundschutz den meisten Unternehmen und Behörden schon lange vertraut ist, gibt es doch immer etwas Neues zu berichten. Das BSI präsentiert Weiterentwicklungen und Projekte auf Tagungen und Messen oder richtet eigene Veranstaltungen aus. 2006 und 2007 führte das Haus acht IT-Grundschutz-Tage mit mehr als 1.500 Teilnehmern durch. Der 1. IT-Grundschutztag 2007 am 2. Juli 2007 setzte mit 400 Teilnehmern eine neue Rekordmarke. Die Themen waren u.a. Notfall-Management, Sicherheit in einer verteilten IT-Landschaft und Infrastruktursicherheit. Nachlesbar sind Inhalt und Ergebnisse auf der Website www.bsi.bund.de/gshb/.

## Jahrestagung der IT-Sicherheitsbeauftragten

Zu ihrer Jahrestagung 2007 versammelten sich rund 100 IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung am 4. und 5. September 2007 in Bonn. Die gemeinsam von der Bundesakademie für öffentliche Verwaltung (BAköV) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) durchgeführte Tagung ist eine Basis für den aktuellen Wissenstransfer und den Erfahrungsaustausch. Fachvorträge behandeln unter anderem Sicherheitsprodukte, organisatorische Aspekte der IT-Sicherheit, Computerkriminalität und Virenschutzprogramme für Bundesbehörden (VSP-Bund). Die Jahrestagung wurde von Michael Hange, dem Vizepräsidenten des BSI, eröffnet (siehe Foto rechts oben).


# 4.1 IT-Grundschutz und Hochverfügbarkeitskompendium

*Nicht allein technische Fragen definieren die IT-Sicherheit. In erheblichem Maße hängt sie auch von den organisatorischen und personellen Rahmenbedingungen ab. Die Arbeiten des BSI auf dem Gebiet des IT-Grundschutzes tragen dieser Erkenntnis seit langem Rechnung. Außerdem entwickelt das BSI zurzeit ein Hochverfügbarkeitskompendium, das konkrete Maßnahmen beschreibt, wie IT-Ressourcen auch im Fehlerfall verfügbar gehalten werden können. Das Kompendium ist vor allem für IT-Verantwortliche gedacht.*

Zu den Aufgaben von IT-Sicherheitsverantwortlichen gehört es, den Überblick über die abzusichernden Geschäftsprozesse und die zugehörige IT zu bewahren und angemessene Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Mit dem IT-Grundschutz hat das BSI dafür eine einfache Methode entwickelt. Mit der Kombination aus der IT-Grundschutz-Vorgehensweise im BSI-Standard 100-2 und den IT-Grundschutz-Katalogen stellt das BSI sowohl eine Sammlung von IT-Sicherheitsmaßnahmen als auch eine entsprechende Methodik zur Auswahl und Anpassung geeigneter Maßnahmen zur Verfügung.

## Neues vom IT-Grundschutz

Um möglichst nah am Stand der Technik und der Managementmethoden zu bleiben, werden die IT-Grundschutz-Kataloge und die BSI-Standardempfehlungen zum IT-Sicherheitsmanagement ständig fortgeschrieben und auf Basis regelmäßiger Bedarfsanalysen und Diskussionen mit den Anwendern weiterentwickelt.

Derzeit werden die BSI-Standards stärker auf Informationssicherheit ausgerichtet sowie an die Entwicklungen im Bereich Risikomanagement und Datenschutz angepasst. Die IT-Grundschutz-Kataloge enthalten zu den verschiedensten Themenbereichen Sammlungen von konkreten Gefährdungs- und Maßnahmenbeschreibungen, jeweils in Bausteinen zusammengefasst. Sie werden kontinuierlich aktualisiert und ergänzt. Im Dezember 2006 ist die 8. Ergänzungslieferung der IT-Grundschutz-Kataloge erschienen. In dieser Ausgabe wurden die Bausteine Windows 2003 Server, Speichersysteme und Speichernetze, WLAN, VoIP und SAP-System neu aufgenommen. Der Baustein Datenbanken erfuhr eine grundlegende Überarbeitung, um technische Entwicklungen aus den vergangenen Jahren aufzunehmen. Er enthält jetzt beispielsweise eine

dedizierte Maßnahme, um Risiken durch SQL-Injections zu reduzieren. Im ersten Quartal 2008 erscheint die 9. Ergänzungslieferung. Die erweiterten IT-Grundschutz-Kataloge enthalten dann die Bereiche elektrotechnische Verkabelung sowie IT-Verkabelung, Netz-Drucker, Multifunktionsgeräte und Mobile Datenträger. Die Kataloge werden ebenso wie die BSI-Standards sowohl in gedruckter Form als auch elektronisch veröffentlicht unter www.bsi.bund.de/gshb.

*Die IT-Grundschutzkataloge umfassen mittlerweile drei Ordner mit über 3.000 Seiten. Die Sammlung von Empfehlungen und Maßnahmen ist immer auf dem neuesten Stand der Technik.*


## Leichter Einstieg: Webkurse und das GSTOOL

Viele Anwender verbinden mit dem Begriff IT-Grundschutz die umfangreichen Kataloge mit ihrer Vielzahl von konkreten Empfehlungen für verschiedene typische IT-Umgebungen. IT-Grundschutz ist aber auch anders zu vermitteln. Neben den Standards bietet das BSI weitere Werkzeuge an, um ein angemessenes Sicherheitsniveau zu erreichen, wie zum Beispiel den Webkurs zum IT-Grundschutz, der einen leichten Einstieg in das umfassende Thema bietet, oder das GSTOOL.

Das GSTOOL unterstützt die gesamte Vorgehensweise nach IT-Grundschutz, beginnend bei der Stammdatenerfassung, über die Feststellung des Schutzbedarfs, den Soll-Ist-Vergleich (Basis-Sicherheitscheck), die Umsetzung bis hin zur anschließenden Sicherheitsrevision. Dazu gehört auch die ISO 27001 Zertifizierung auf Basis von IT-Grundschutz, die sowohl eine Prüfung des IT-Sicherheitsmanagements als auch der konkreten IT-Sicherheitsmaßnahmen vorsieht.

Nach der Veröffentlichung des leicht überarbeiteten GSTOOL 3.1 im Jahr 2004 hat das BSI mit der Version 4.0 im Jahr 2006 den mittlerweile über 9.000 Lizenzkunden eine deutlich erweiterte und optimierte Version des bewährten Produkts zur Verfügung gestellt. Zu den wesentlichen Erweiterungen des GSTOOL 4.0 gehören unter anderem die Anpassung an die 2005 grundlegend überarbeitete Struktur der IT-Grundschutz-Kataloge, die Möglichkeit, gelöschte Einträge wiederherzustellen und der Ausbau der Berichtsfunktion.

Mit dem Servicepack 1 (SP1) wurde der Funktionsumfang des GSTOOL 4.0 erweitert. Dazu gehört die Funktion „IT-Grundschutz-Management“, die mit freundlicher Unterstützung der Bayer Business Services GmbH realisiert wurde. Sie ermöglicht eine Versionierung, also die Archivierung alternativer Dateiversionen. Mit Unterstützung

des Zentrums für Informationsverarbeitung und Informationstechnik (ZIVIT) ist die Funktion „Mehrere Standard-Arbeitsbereiche“ dazu gekommen. Sie hat die Möglichkeiten zur Bedienung mehrerer Nutzer auf demselben Server, die Mandantenfähigkeit, erweitert. Zusätzlich wurde durch den Modus „Struktur Zielobjekte“ die schnellere logische und technische Verknüpfung von Zielobjekten ermöglicht. Derzeit wird die Version 4.5 des GSTOOL erarbeitet, die es erlaubt, Risikoanalysen durchzuführen. Insbesondere wird damit die vollständige Abbildung des BSI-Standards 100-3 umgesetzt.


*Das GS (Grundschutz)-Tool ist den Wünschen der Anwender folgend fortentwickelt worden und steht demnächst als GSTOOL Version 4.5 bereit.*

## Acht IT-Grundschutz-Tage

Regelmäßig veröffentlicht das BSI weitere Hilfsmittel zum IT-Grundschutz. Anfang 2007 ist beispielsweise eine Studie „Sicherheitseigenschaften von Standleitungstechnologien“ erschienen. Sie behandelt die Frage, wie verschiedene Standorte einer Behörde oder eines Unternehmens sicher vernetzt werden können, wenn die Technik auf dem IT-Grundschutz-Baustein „B 3.302 Router und Switches“ basiert. Die Studie liefert einen Überblick über häufig eingesetzte technische Lösungen für die Standortvernetzung und deren Sicherheitseigenschaften.

Das BSI präsentiert die verschiedenen Weiterentwicklungen und Projekte rund um IT-Grundschutz auf Tagungen, Messen und Workshops. 2006 und 2007 hat das BSI insgesamt acht IT-Grundschutz-Tage organisiert.


## Das Hochverfügbarkeitskompendium des BSI

Die Leistungsfähigkeit von Systemen in der Informationstechnologie hat sich in den vergangenen Jahrzehnten vervielfacht. Sie wurden dabei immer komplexer und dynamischer. Das liegt unter anderem an der zunehmenden Integration bestehender in neue Systeme und auch an neuen Funktionalitäten, die hinzugefügt wurden, ohne die Wechselwirkung mit bereits vorhandenen Komponenten vollständig zu verstehen. Des Weiteren bestehen IT-Infrastrukturen zunehmend aus generischen Software- und Hardware-Komponenten, die unter dem Gesichtspunkt der nahtlosen Zusammenarbeit (Interoperabilität) und Wiederverwendbarkeit produziert werden und weniger unter dem der Hochverfügbarkeit. Ein System gilt als hochverfügbar, wenn eine Anwendung auch im Fehlerfall weiterhin verfügbar ist und ohne unmittelbaren menschlichen Eingriff weiter genutzt werden kann.

Wenn man zusätzlich die wachsende Abhängigkeit des privaten und öffentlichen Lebens von der einwandfreien (uneingeschränkten) Funktion der informationstechnischen Systeme in Betracht zieht, erhält man einen Eindruck von den Herausforderungen, vor denen das IT-Management heute steht. Ein Beispiel: Nach dem schweren Erdbeben vor der Küste Taiwans im Dezember 2006 war der Internet-Zugang für Millionen von Menschen in Asien beeinträchtigt. Betroffen waren auch internationale Telefonverbindungen sowie der regionale Datenverkehr. Banken und Wertpapierhäuser beklagten Ausfälle ihrer Netze. In Südkorea kam der Handel mit der einheimischen Währung zeitweise zum Erliegen (Quelle: Spiegel vom 27. Dezember 2006, „Erdbeben bremst Internet in Ost-Asien“). Die Ereignisse verdeutlichen, dass vielerorts das Arbeiten ohne Informations- und Kommunikationstechnik kaum mehr möglich ist und viele geschäftliche Vorgänge davon abhängen, dass die IT ordnungsgemäß und sicher funktioniert. Fehler, Unfälle, Naturkatastrophen zu vermeiden ist unmöglich. Das Reduzieren von Schwachstellen im System, die zu einem Totalausfall führen, dagegen ist machbar.

Das bedeutet: Die für den alltäglichen Service erforderlichen IT-Ressourcen müssen so ausgerichtet sein, dass erwartete wie unerwartete Ereignisse lediglich die Verfügbarkeit von einzelnen Komponenten, nicht jedoch die Verfügbarkeit des Gesamtsystems beeinträchtigen. Das BSI entwickelt zurzeit ein Hochverfügbarkeitskompendium (HV-Kompendium), das entsprechende Maßnahmen beschreibt. Ihre Umsetzung wird ebenfalls Bestandteil des Kompendiums sein.

## Die Hochverfügbarkeitsanalyse

Hochverfügbarkeitsanalysen (HV-Analysen) sind ein wesentlicher Teil des Risikomanagements. Die Anforderungen an ein IT-System ergeben sich aus der Analyse der abzuwickelnden Geschäftsprozesse: Sie definieren das SOLL. Die im HV-Kompendium dargestellten Methoden zur Analyse der eingesetzten IT-Ressourcen ermöglichen eine Bewertung des IST (Service Delivery). Aus dem Vergleich von SOLL und IST lässt sich ableiten, welche Maßnahmen ergriffen werden müssen und wie hoch das Restrisiko ist. In den meisten Fällen geht es um eine Verbesserung der Verfügbarkeit und die Reduzierung der Restrisiken.

Ein besonderes Merkmal der HV-Analyse ist der ganzheitliche Ansatz. Wirklich bewerten lässt sich die Service-Verfügbarkeit erst dann, wenn alle zum Service beitragenden IT-Ressourcen einbezogen werden, einschließlich ihrer Wechselwirkungen. Bei der Modellierung der IT-Ressourcen wird ein objektorientierter Ansatz verfolgt, der die Basis für die Analyse der Wechselwirkungen darstellt. Bei der Ermittlung des Verfügbarkeits-IST kommen je nach Untersuchungsbereich und Datenbasis verschiedene qualitative und quantitative Methoden zum Einsatz.

Ein reibungsloser Ablauf von IT-Prozessen erfordert eine hinreichende Orientierung an Standards. Außerdem ist zur besseren Vergleichbarkeit der Analyseergebnisse mit denen anderer Verfahren eine Ausrichtung an verschiedenen Standards unverzichtbar. Der methodische Ansatz der HV-Analyse orientiert sich an Standards für IT-Organisation und IT-Systeme (zum Beispiel ITIL, COBIT, ISO, IEEE, IT-Grundschutz).

## Die Realisierung hoher Verfügbarkeit

Die Verfügbarkeit eines Systems definiert sich durch die Wahrscheinlichkeit, dass es an einem bestimmten Zeitpunkt zur Erfüllung seiner Aufgaben bereit steht. Das kann man durch eine Zahl (zum Beispiel „99,99 Prozent“) oder durch die Angabe eines Niveaus (zum Beispiel „grundsätzlich verfügbar“) ausdrücken.

Die Aufgabe eines IT-Verantwortlichen besteht meist darin, das im SOLL ermittelte Verfügbarkeitsniveau mit endlichen Mitteln zu erreichen. Der Handlungsbedarf, der sich aus der HV-Analyse ergibt, wird im Kompendium durch Szenarien, Architekturen und Maßnahmenbündel abgebildet, die jeweils einem Verfügbarkeitsniveau zugeordnet werden können.

Grundlegende Prinzipien der Verfügbarkeit (zum Beispiel Redundanz, Fehlertoleranz oder Robustheit) werden im Kompendium praxisnah dargestellt. Es enthält Empfehlungen für die Vorgehensweise und Hilfsmittel zur Umsetzung. Die Realisierung der einzelnen Schritte hin zu einem hoch verfügbaren System, erfordert in jedem Fall Expertenwissen in verschiedenen Bereichen (zum Beispiel Netzwerk, Infrastruktur oder Organisation). Die Veröffentlichung des HV-Kompendiums in seiner ersten Ausgabe ist, nach Vorstellung und Diskussion wesentlicher Inhalte im Expertenkreis, für 2008 geplant.


## Sichere Mobilkommunikation

Mobiltelefone sind über das Mobilfunknetz permanent „online“. Sie werden durch Angriffe über das Mobilfunknetz in ganz ähnlicher Weise bedroht wie stationäre Computer durch Angriffe über das Internet. Drahtlose Schnittstellen wie WLAN oder Bluetooth erlauben, sofern die Sicherheitsmechanismen nicht korrekt aktiviert sind, das Mitlesen von Daten und den Zugriff auf das Endgerät.

Das BSI hat sich der „Mobilfunksicherheit“ bereits seit vielen Jahren angenommen und konkrete Schutzmaßnahmen für verschiedene Anwendungsszenarien, Nutzergruppen und Schutzbedarfsanforderungen definiert.

Diese sind veröffentlicht

- in den Broschüren „GSM Mobilfunk – Gefährdungen und Sicherheitsmaßnahmen“, „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ sowie „Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen“,
- in der „Technischen Richtlinie Sicheres WLAN“ (TR-S-WLAN),
- auf der Internetseite www.bsi-fuer-buerger.de,
- in den IT-Grundschutz-Katalogen unter www.bsi.bund.de/gshb/


*Diese Broschüre gibt Administratoren Sicherheitsbeauftragten und Endnutzern drahtloser Kommunikationsanlagen wertvolle Hilfestellungen zur Bewertung und sicheren Nutzung solcher Systeme.*

Das Unternehmen T-Systems hat unter dem Namen SiMKo (Sichere Mobile Kommunikation) ein Produkt entwickelt, das es ermöglicht, mit mobilen Endgeräten einen verschlüsselten Zugang in das Regierungsnetz IVBB aufzubauen und darüber E-Mails mit dem Mail-Server der eigenen Behörde zu synchronisieren. Das BSI hat für das Produkt eine spezifische Einsatzempfehlung für Verschlusssachen (VS) der Einstufung „Nur für den Dienstgebrauch“ erteilt. Der Synchronisationsdienst SiMKo wird von T-Systems laufend weiter entwickelt. Außerdem hat das BSI zur Überwachung von Mobilfunkverboten beispielsweise in VS-Besprechungsräumen einen Mobilfunkdetektor entwickelt. Vier getrennte Kanalempfänger scannen sequentiell die Frequenzbänder GSM900, GSM1800, UMTS und DECT ab. Wird ein Mobiltelefonat entdeckt, löst das Gerät Alarm aus.

## 4.2 ISO 27001 – Zertifikate auf der Basis von IT-Grundschutz

*Mit der ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz hat das BSI eine besondere Art der Zertifizierung von Systemen geschaffen. Sie stellt eine Kombination aus der Prüfung nach DIN ISO/IEC 27001 und nach IT-Grundschutz dar.*

Bei ISO 27001 handelt es sich um eine internationale Norm für Informationssicherheits-Managementsysteme. Daneben stellen IT-Grundschutz-Kataloge und deren Empfehlungen inzwischen de facto einen Standard für IT-Sicherheit dar.

Die IT-Grundschutz-Kataloge erklären nicht nur, wie Informationssicherheit konzipiert werden soll, sondern geben auch sehr konkrete Hinweise, wie eine Umsetzung (auch auf technischer Ebene) aussehen kann. Das Vorgehen nach IT-Grundschutz ist eine erprobte und effiziente Möglichkeit, allen Anforderungen von ISO 27001 nachzukommen. Durch die Prüfung konkreter Sicherheitsmaßnahmen ist eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz wesentlich aussagekräftiger als eine reine ISO 27001-Zertifizierung.


Die Normenreihe ISO 270xx besteht aus verschiedenen Normen, die teilweise noch in der Entwicklung sind. Im März 2007 ist aus dieser Reihe die ISO 27006:2007 „Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems“ in Kraft getreten. Sie beschäftigt sich mit Anforderungen an die Stellen, die Zertifikate nach ISO 27001 vergeben. Das BSI hat diese Anforderungen umgesetzt und einige geringfügige Änderungen im Zertifizierungsschema vorgenommen. Beispiele dafür sind die Verlängerung der Laufzeit auf drei Jahre mit jährlichen Überwachungsaudits oder die Möglichkeit eines Voraudits. Nähere Informationen und eine Liste aller Zertifikate sind zu finden auf der Website www.bsi.bund.de/gshb/zert/.

# 4.3 Einführung von Technischen Richtlinien und Konformitätsprüfungen

*Mit der Entwicklung Technischer Richtlinien verfolgt das BSI das Ziel, technische Vorgaben für die Entwicklung, den Einsatz und die Prüfung sicherer und interoperabler IT-Lösungen festzulegen.*

Technische Richtlinien (TR) beschreiben funktionale und qualitative Anforderungen an IT-Produkte und -Systeme, die für deren Interoperabilität, Integration und Sicherheit entscheidend sind. Sie werden vom BSI je nach Bedarf in enger Kooperation mit Industrie und Wirtschaft entwickelt. Die Notwendigkeit von TR ergibt sich aus nationalen Sicherheitserfordernissen oder aus einem öffentlichen Interesse.

Die einschlägigen Bestimmungen betreffen insbesondere IT-Produkte und -Systeme, die für den Einsatz in hoheitlichen und demnach sicherheitskritischen Bereichen der Bundesrepublik Deutschland vorgesehen sind. Neben der Interoperabilität stehen dabei insbesondere Anforderungen an die elektronische Fälschungssicherheit und Betriebszuverlässigkeit im Vordergrund. Bei ihrer Einführung haben diese Richtlinien zunächst den formalen Status einer Empfehlung. Verbindlichkeit gewinnen sie jedoch dann, wenn die Vorgaben in Ausschreibungsverfahren verlangt, von Bedarfsträgern für ihren Zuständigkeitsbereich explizit gefordert oder in einem Gesetz oder in einer Rechtsverordnung ausdrücklich genannt werden.

### Technische Richtlinie für elektronische Reisepässe

Zur Produktion elektronischer Reisepässe müssen die Daten des Antragstellers bei den zuständigen Stellen (zum Beispiel den kommunalen Einwohnermeldeämtern) in hinreichender Qualität erfasst und an den Passproduzenten übermittelt werden. Die Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe (TR-PDÜ) gilt als verbindliche Vorgabe für alle technischen Systeme, die für diese Aufgabe eingesetzt werden.

### Prüfkriterien für elektronische Reisedokumente

Als vielleicht größte Herausforderung bei der Einführung elektronischer Dokumente hat sich die Sicherstellung der internationalen Interoperabilität der Reisepässe und der dazugehörigen Lesegeräte erwiesen. Die Technische Richtlinie elektronische Pässe (TR-ePass) definiert Prüfkriterien, die diese Interoperabilität sicherstellen.

**Konformitätsprüfungen nach Technischen Richtlinien**

Im Rahmen der Erweiterung seiner Akkreditierungs- und Zertifizierungstätigkeiten bietet das BSI seit Mitte des Jahres 2006 eine so genannte „Zertifizierung nach Technischen Richtlinien“ an. Hersteller und Vertreiber können sich die Konformität ihrer IT-Produkte oder -Systeme vom BSI durch ein Zertifikat bestätigen lassen. Voraussetzung ist eine erfolgreich durchlaufene Prüfung. Konformitätsprüfungen stellen sicher, dass ein IT-Produkt oder -System die Anforderungen gemäß den Vorgaben der jeweiligen TR des BSI vollständig und korrekt erfüllt. Technische Richtlinien liefern dazu sämtliche für die Konformitätsprüfung relevanten Prüfvorschriften und -spezifikationen. Die Durchführung erfolgt bei unabhängigen Prüfstellen. Sie sind vom BSI zugelassen und haben ihre Fachkompetenz gegenüber der Akkreditierungsstelle des BSI nachgewiesen.

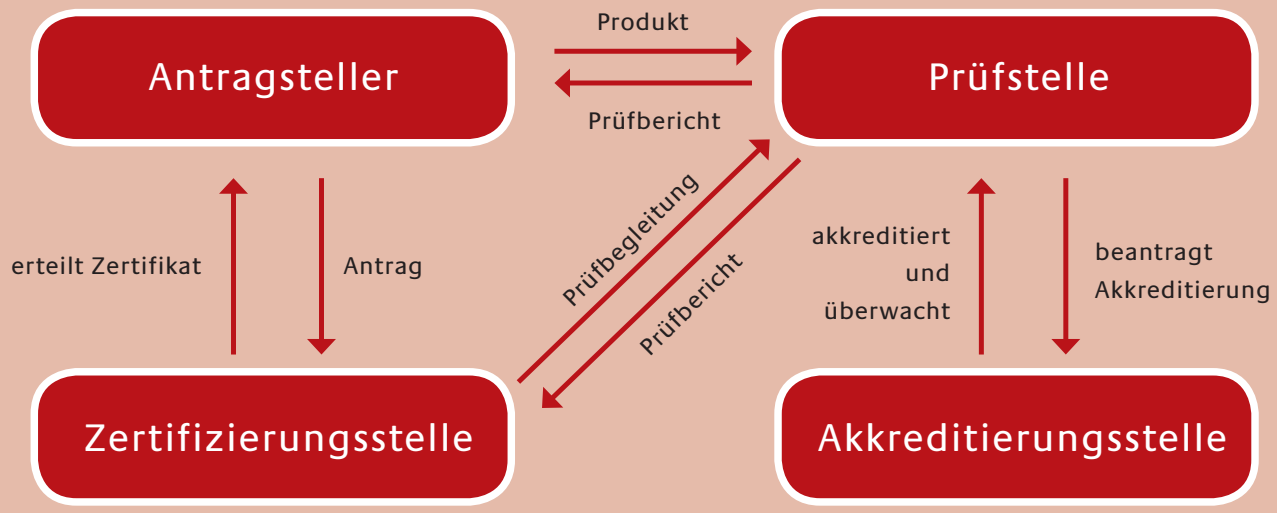
*Ab November 2007 werden auf dem elektronischen Reisepass der Bundesrepublik Deutschland Aufnahmen der Fingerabdrücke des jeweiligen Besitzers gespeichert. Um eine hinreichende Qualität der bei der Passbeantragung erfassten Fingerabdruckbilder sicherzustellen, dürfen dabei nur optische Sensoren eingesetzt werden, die eine entsprechende Zertifizierung durch das BSI gemäß Technischer Richtlinie 03104 vorweisen können. Hierzu zählen u.a. die beiden abgebildeten Fingerabdruckscanner des Unternehmens Cross x.*

**Akkreditierung von Prüfstellen**

Die erfolgreiche Einführung neuer Technischer Richtlinien und der dazu gehörenden Konformitätsprüfungen in den Jahren 2006/2007 wurde durch die Akkreditierung neuer Prüfstellen aktiv begleitet. Die Akkreditierung geeigneter Prüfstellen ist ein zentraler Bestandteil der Zertifizierung. Neben dem Nachweis der benötigten Fachkompetenz muss sichergestellt sein, dass eine Prüfstelle alle Voraussetzungen erfüllt, um eine unabhängige, objektive und hoch qualitative Prüfung durchführen zu können. Dabei ist vor allem ein funktionsfähiges Qualitätsmanagementsystem nach DIN EN ISO/IEC 17025 unerlässlich. Erst wenn alle benötigten Nachweise erbracht sind, erhält eine Prüfstelle die Akkreditierung des BSI und darf Konformitätsprüfungen durchführen.

Bereits im September 2006 erfolgte die Akkreditierung der „CETECOM ICT Services GmbH“ als Prüfstelle für elektronische Reisedokumente (TR-ePass). 2007 folgten das „Fraunhofer Institut für Angewandte Optik und Feinmechanik“ in Jena (TR-PDÜ) sowie die Prüfstelle der „Secunet Security Networks AG“, Essen (TR-ePass). Weitere Prüfstellen für verschiedene Bereiche von TR-PDÜ und -ePass befinden sich in der Akkreditierung.

**Zertifizierung nach Technischen Richtlinien**




Die Grafik zeigt die an einer Zertifizierung nach Technischen Richtlinien beteiligten Stellen und deren Aufgaben.

## Zertifikate nach Technischen Richtlinien

Gestützt durch die Einführung des elektronischen Reisepasses (ePass Stufe 2) zum 1. November 2007 wurde die Einführung von Konformitätsprüfungen nach Technischen Richtlinien von Herstellern entsprechender IT-Produkte schnell angenommen. So konnten bis September 2007 bereits zahlreiche Zertifizierungsverfahren erfolgreich abgeschlossen werden. Zum Beispiel wurde die Konformität von insgesamt sieben Fingerabdrucksensoren zur TR-PDÜ mit Zertifikaten bestätigt. Nicht nur nationale, sondern auch europäische und internationale Hersteller zeigen sich an den Technischen Richtlinien und dem neuen Zertifizierungsverfahren des BSI interessiert.

# 4.4 Technologiefeld „Hoheitliche Dokumente“

*Das BSI hat seine Projekte im Bereich hoheitlicher Dokumente in den Jahren 2006 und 2007 konsequent fortgesetzt. Feldversuche ebneten den Weg für die praktische Umsetzung biometrischer Systeme. Seit November 2007 wird der ePass der zweiten Generation ausgegeben, bei dem zusätzlich zwei Fingerabdrücke im Pass-Chip gespeichert sind.*

### Reisepass mit biometrischen Merkmalen – ePass

Zum 1. November 2005 hat Deutschland den elektronischen Reisepass (kurz ePass) eingeführt. Als erstes biometrisches Merkmal wurde dabei das Gesichtsbild des Passinhabers gespeichert. Die entsprechende EG-Verordnung sieht auch die Aufnahme von zwei Fingerabdrücken und deren Speicherung im Chip des ePasses vor. Damit wurde bei neuen Pässen am 1. November 2007 begonnen. Das BSI hat maßgeblich bei der technischen Gestaltung der Spezifikationen in Gremien der International Civil Aviation Organization (ICAO), der International Organization for Standardization (ISO) und der EU mitgewirkt. Dabei lag der Aufgabenschwerpunkt des BSI bei der Realisierung der IT-Sicherheitskonzeption im ePass. Als zentraler Anlaufpunkt für alle technischen Fragen betreibt das BSI die ePass-Hotline, die täglich von 8 bis 17 Uhr unter der Nummer 01805-27 43 00 erreichbar ist.

### Erfassung der Passanträge

Mit der Technischen Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe hat das BSI ein komplettes Regelwerk von der Erfassung der Antragsdaten über die Qualitätssicherung der biometrischen Daten bis hin zur Übertragung vorgelegt. Darüber hinaus hat das BSI zusammen mit dem Bundeskriminalamt ein Verfahren entwickelt, das die qualitativ hochwertige Erfassung von Fingerabdrücken gewährleistet. Die vom Passproduzenten entwickelten Softwarekomponenten wurden in einem Feldtest erprobt und optimiert. Die Richtlinie wurde über die Passdatenerfassungs- und -übermittlungsverordnung (PassDEÜV) für alle Beteiligten rechtsverbindlich.

### Zertifizierung von Fingerabdrucksensoren

Bei der Erfassung der Fingerabdrücke, die jemand abgibt, der einen Pass beantragt, ist eine hohe Qualität erforderlich, sonst lassen sie sich später nicht eindeutig verifizieren. Daher hat das BSI ein eigenes Zertifizierungsprogramm für Fingerabdrucksensoren entworfen, das Hersteller-unabhängig die Qualität der Sensoren misst. Nur zertifizierte Sensoren dürfen für die Erfassung eingesetzt werden.

## Biometrie bei der Grenzkontrolle

Im Kontext ePass und VISA hat das BSI in Zusammenarbeit mit der Bundespolizei begonnen, in verschiedenen Pilotprojekten die Verarbeitung biometrischer Daten an Grenzübergängen und auch mobil zu erproben. Ziel ist die Entwicklung von Verfahren zur Umsetzung biometrisch unterstützter Grenzkontrollen.

## Extended Access Control – Schutz für besonders sensitive Daten im ePass

Die im EU-Reisepass neben dem Gesichtsbild zusätzlich gespeicherten Fingerabdrücke müssen aus datenschutzrechtlichen Erwägungen besonders geschützt werden. Hierzu hat das BSI das Extended Access Control-Protokoll (EAC) entwickelt. Die Verwendung dieses Verfahrens ist nach der Entscheidung der EU-Kommission in den EU-Reisepässen aller Mitgliedstaaten verbindlich. Das EAC-Protokoll sieht einen Authentisierungsmechanismus sowohl zur Echtheitsprüfung des so genannten Radio-Frequency-Chips (RF-Chip) im ePass als auch für das Lesegerät vor. Das Lesegerät wird mit einem eigenen Schlüsselpaar und einem vom RF-Chip verifizierbaren Zertifikat ausgestattet, das definiert, auf welche Daten zugegriffen werden darf. Damit ist sichergestellt, dass Lesegeräte nur auf die Daten zugreifen können, für die sie auch legitimiert wurden.

Für den geplanten elektronischen Personalausweis hat das BSI die EAC-Spezifikation um zusätzliche Funktionen und Protokolle erweitert. In der nächsten Version kann zum Beispiel mit der „Online-Authentisierung“ eine sichere und datenschutzfreundliche Authentisierung des Nutzers über das Internet erfolgen.

*Durch biometrieunterstützte Grenzkontrollen kann der Missbrauch echter Dokumente durch unberechtigte, dem Passinhaber ähnlich sehende Personen (so genannte Look-Alike-Täuschung) verhindert werden.*

### PKI-Strukturen für den ePass

Für die Produktion der ePässe hat das BSI in seiner Funktion als oberste Zertifizierungsstelle für die digitale Signatur (Country Signing Certification Authority – CSCA) den Passhersteller (die Bundesdruckerei GmbH) mit Document Signer-Zertifikaten (DS) ausgestattet. Dadurch ist der Hersteller in der Lage, die im RF-Chip des ePasses gespeicherten Daten mit einer digitalen Signatur gegen nachträgliche Verfälschungen oder Manipulationen zu schützen. Gleichzeitig ist das BSI seit November 2007 oberste Zertifizierungsstelle für Lesegeräte im ePass-Kontext (Country Verifying Certification Authority – CVCA). Als solche hat sie die zum Lesen von Fingerabdrücken berechtigten Stellen im In- und Ausland mit Document Verifier-Zertifikaten (DV) ausgestattet.

### Protection Profiles für ePässe

Das BSI zertifiziert die in den ePässen enthaltenen RF-Chips nach den so genannten Protection Profiles (PP). Sie beschreiben die zu erfüllenden Sicherheitskriterien. Die für die deutschen Reisepässe vorgesehenen RF-Chips wurden nach dem neuen PP der Technischen Richtlinie EAC zertifiziert. Die Sicherheitskriterien dieser Protection Profiles werden europaweit zur Prüfung ICAO-konformer Chips herangezogen.

### „Golden Reader Tool“

Bei dem im Auftrag des BSI entwickelten „Golden Reader Tool“ (GRT) handelt es sich um eine Software-Applikation zum Lesen von ICAO-konformen maschinenlesbaren Reisedokumenten (eMRTD). Das BSI verfolgt mit dem GRT das Ziel, die Voraussetzungen für weltweite Interoperabilität im Bereich eMRTDs basierend auf den Vorgaben der ICAO zu schaffen. Das Golden Reader Tool wird ständig weiterentwickelt und ist heute bereits zum internationalen Standard für das Lesen von ePässen geworden.


*Im November 2005 wurde in Deutschland der elektronische Reisepass (ePass) eingeführt. Er enthält das digitale Passfoto als erstes biometrisches Merkmal im Chip. Seit November 2007 wird der ePass der zweiten Generation ausgegeben, bei dem zusätzlich zwei Fingerabdrücke im Chip gespeichert sind. Mit der neuen Technologie wird ein Höchstmaß an Fälschungssicherheit und Schutz vor Dokumentenmissbrauch erreicht.*

# 4.5 Middleware – Spezifikationen für elektronische Anwendungsprojekte

*Das Bundeskabinett hat am 9. März 2005 die Eckpunkte für eine gemeinsame eCard-Strategie beschlossen. Sie fasst die unterschiedlichen Karten- und Anwendungsprojekte des Bundes elektronischer Reisepass (ePass), elektronischer Personalausweis, elektronische Gesundheitskarte (eGK), elektronischer Einkommensnachweis (ELENA) und elektronische Steuererklärung (ELSTER) zusammen. Für Wirtschaft und Verwaltung bedeutet dies einen beträchtlichen Innovationsschub.*

Ziel ist dabei, einheitliche Standards zu schaffen, Synergieeffekte zu nutzen sowie die Interoperabilität zwischen den unterschiedlichen Anwendungen und Technologien sicher zu stellen. In Anlehnung an die eCard-Strategie der Bundesregierung wurde daher in Abstimmung mit den relevanten Behörden und übrigen Marktteilnehmern unter Federführung des BSI eine Spezifikation für ein eCard-API-Framework erstellt. Wichtig war es auch, im Rahmen des Frameworks nicht nur die „hoheitlichen" Kartenprojekte zu betrachten, sondern auch die von der Wirtschaft herausgegebenen (Signatur-)Karten mit einzubeziehen.

## Standards gesucht

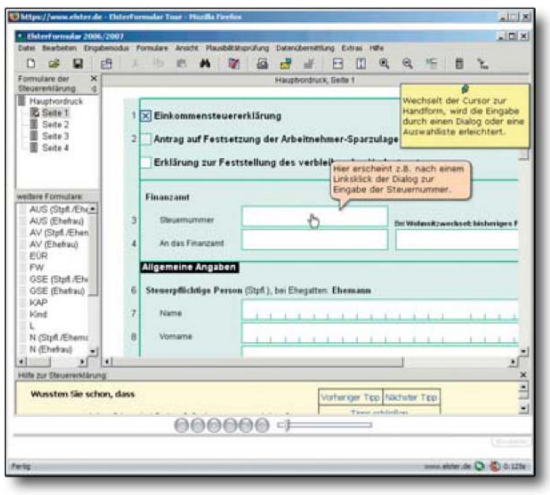
Eine Analyse der bereits im Markt etablierten Standards ergab, dass kein Standard die nötigen Anforderungen vollständig abdecken konnte. Manche wiesen gravierende Sicherheitsmängel auf, andere verlangten nach bestimmten Betriebssystemplattformen und wieder andere setzten beim Anwendungsentwickler detailliertes Spezialwissen über Smart-Card-Technologie voraus. Um die Vorteile der gemeinsamen eCard-Strategie nutzen zu können, musste jedoch von Anfang an sicher gestellt sein, dass von Entwicklerseite das Framework mit möglichst geringem Aufwand angesprochen werden und die resultierende Lösung von den Endanwendern möglichst intuitiv genutzt werden kann. Das Ergebnis war ein Webservices verwendendes Schichtenmodell. Wo von existierenden Standards sinnvoll Gebrauch gemacht werden konnte, wurde dies selbstverständlich getan. Um Anwendungsentwicklern die Arbeit zu erleichtern und damit die Nutzung von Smart-Cards zu fördern, wurden High-Level-Schnittstellen eingeführt. Waren Erweiterungen bestehender Standards nötig, wurden diese behutsam durchgeführt – nicht jedoch, ohne diese bereits von Beginn an mit den zuständigen Gremien auf nationaler, europäischer und internationaler Ebene (z.B. bei DIN, CEN und ISO) abzustimmen.

Die in der Technischen Richtlinie des BSI niedergelegte Softwarearchitektur stellt sicher, dass Hersteller in Zukunft wesentlich seltener kosten- und zeitintensive Re-Bestätigungen nach SigG/SigV durchführen müssen.

*Eine Herausforderung für die IT-Sicherheit: Mit der elektronischen Gesundheitskarte werden am Ende 80 Millionen Versicherte ausgestattet sein. Die Karte, die von den rund 200 Krankenkassen ausgegeben wird, vernetzt 21.000 Apotheken, 123.000 niedergelassene Ärzte, 65.000 Zahnärzte und 2.220 Krankenhäuser. Tests mit Echtdaten laufen in drei deutschen Regionen. Mehr zur elektronischen Gesundheitskarte: www.die-gesundheitskarte.de*


## Hersteller können Konformität unter Beweis stellen

Mittlerweile ist die sich aus den Arbeiten ergebende Spezifikation als Technische Richtlinie BSI 03-112 veröffentlicht. Hersteller, die diese komplett umgesetzt haben, können durch spezielle Tests die Konformität ihrer Lösungen unter Beweis stellen und erhalten bei Vorliegen aller Voraussetzungen ein entsprechendes Gütesiegel. Das Gleiche gilt für die Hersteller von Anwendungssoftware und Hardware. Sofern alle Komponenten erfolgreich getestet sind, kann ein Endanwender also sicher sein, dass Karte, Kartenleser und Software reibungslos zusammen funktionieren. In Zukunft kann der Anwender dann nicht nur – wie bereits jetzt möglich – qualifiziert elektronisch signieren, sondern sich beispielsweise in einem Online-Shop mit seinem Personalausweis elektronisch ausweisen oder ein auf seiner Gesundheitskarte gespeichertes Rezept online in einer Internetapotheke einlösen. Um als Bundesbehörde nicht wettbewerbsverzerrend in den Markt einzugreifen, wird das BSI keine eigene Implementierung der Technischen Richtlinie bereitstellen. Kommerzielle Anbieter haben jedoch schon entsprechende Produkte angekündigt.




*Die Software ELSTER bietet die Möglichkeit, Steuererklärungen elektronisch via Internet an das Finanzamt zu übermitteln.*

# „Innovationsmotor IT-Sicherheit“



lautete das Motto des 10. Deutschen IT-Sicherheitskongresses, zu dem das BSI vom 22. bis 24. Mai 2007 nach Bonn-Bad Godesberg rief. Bei der Eröffnung sagte Bundesinnenminister Dr. Wolfgang Schäuble: „Die IT-Sicherheit entwickelt sich immer mehr zu der entscheidenden Schlüsselfrage einer zukunftsorientierten Sicherheitspolitik. Jeder Nutzer trägt Verantwortung. Wir brauchen eine IT-Sicherheitskultur, in der alle verantwortlich handeln.“ Das BSI müsse künftig als die einzige staatliche IT-Sicherheitsbehörde IT-Sicherheit nach innen wie nach außen gewährleisten können.

Auf dem Kongress wurden in Vorträgen, Diskussionsrunden und einer begleitenden Ausstellung die vielfältigen Entwicklungen und Aspekte der Sicherheit in der Informationstechnik beleuchtet. Der Tagungsband zum 10. Deutschen IT-Sicherheitskongress ist im SecuMedia-Verlag erschienen und über http://buchshop.secumedia.de zu beziehen.

# 5.1 Bürgerportale – eine Infrastruktur für sichere Kommunikation

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

Elektronische Kommunikation ist in Verwaltung, Wirtschaft und Gesellschaft heute nicht mehr wegzudenken. Das Internet öffnet globale Kommunikationsräume. Doch seiner sicheren Nutzung stehen Hindernisse entgegen. Die Ursachen sind fehlendes Vertrauen, die Unsicherheit, ungewollt persönliche Informationen preiszugeben, oder das Gefühl, ein Außenstehender könne gezielt elektronische Verbindungen ausspionieren.

Grundsätzlich ist festzuhalten: Vertraulichkeit und Rechtsverbindlichkeit der Kommunikation sind in offenen Netzen nicht sichergestellt. Dazu kommt: Die Nachweismöglichkeiten für ein bestimmtes Handeln sind schwierig, Authentisierungen umständlich und hinter einer harmlos erscheinenden Mail verbergen sich mitunter gefährliche Spam-, Wurm- oder Phishing-Attacken. Problemspezifische Lösungen gibt es zwar bereits, doch sind sie im Allgemeinen sehr aufwändig und finden wenig Akzeptanz. Der moderne Staat steht deshalb vor der Aufgabe, im elektronischen Kommunikationsraum für eine Grundversorgung an Sicherheit, Verbindlichkeit und Vertraulichkeit zu sorgen. Staatliche Regulierung kann und muss jedoch nicht bedeuten, selbst eine Infrastruktur aufzubauen. Sie kann sich, sofern dies für die Sicherung der Grundversorgung ausreicht, darauf beschränken, Regeln zu definieren und ihre Einhaltung zu kontrollieren. Mit dem Projekt Bürgerportal hat der Bund diesen Weg eingeschlagen und entwickelt ein Konzept für eine sichere Kommunikation aller im Internet.


*Die ständig ergänzte Loseblattsammlung enthält neben Informationen zur Organisation und zum IT-Einsatz im E-Government insbesondere IT-sicherheitstechnische Empfehlungen.*

## Das Konzept der sicheren elektronischen Kommunikation

Bürgerportale sollen Bürgerinnen und Bürger, aber auch den Nutzern aus Wirtschaft und Verwaltung einen sicheren Ort im Netz schaffen und eine vertrauliche Kommunikation über das Internet ermöglichen. Dafür werden Dokumente und Daten unmittelbar, nachdem sie vom Nutzer über einen authentifizierten und verschlüsselten Kommunikationskanal an sein Bürgerportal übergeben worden sind, integritätsgeschützt und verschlüsselt zum Bürgerportal des Empfängers weitergeleitet.

Unmittelbar vor der Übertragung der Daten zum Empfänger entschlüsselt sie das Bürgerportal, prüft ihre Integrität und sendet sie über einen authentifizierten und verschlüsselten Kommunikationskanal an eine Client-Anwendung des Nutzers. Die Kommunikation zwischen den verschiedenen Bürgerportalen erfolgt genauso verschlüsselt und signiert wie innerhalb eines einzelnen Bürgerportals. Eine Reihe von Anbietern ist aufgefordert, Bürgerportale bereitzustellen, die sich durch unterschiedliche, über die Basisdienste hinausgehende Möglichkeiten voneinander unterscheiden können. Die Entscheidung fällt in einem Wettbewerb. Damit die Basisdienste auch über Bürgerportal-Grenzen hinweg nutzbar sind, werden die bestehenden Bürgerportale zu einem Bürgerportal-Verbund zusammengefasst. Die Nutzer bewegen sich in diesem Verbund in einer „geschlossenen Benutzergruppe“, also einem besonders geschützten Bereich.


## Die Basisdienste

Ziel ist es, eine vertrauliche und verbindliche Kommunikation bei eindeutiger Adressierbarkeit zu ermöglichen. Dafür sollen Bürgerportale die folgenden Dienste anbieten:

- Das Postfach steht für den Nutzer als elektronischer Briefkasten bereit. Damit kann er elektronische Nachrichten empfangen, speichern und verwalten. Das Postfach kann über eine elektronische und dem Bürger eindeutig zugeordnete Bürgerportal-Adresse erreicht werden.

- Zum verbindlichen Versenden von elektronischen Nachrichten steht dem Nutzer ein Versanddienst zur Verfügung. Über diesen Dienst lassen sich entsprechende Nachweise darüber erbringen, ob, wie und wann die Nachricht zugestellt wurde.

- Der Dokumentensafe bietet die Möglichkeit zur langfristigen Ablage und Verwaltung von elektronischen Dokumenten.

- Ein Authentisierungsdienst führt für Dritte, mit denen der Nutzer in Kontakt treten will, eine zuverlässige Authentifizierung durch.

Wer die Dienste in Anspruch nehmen möchte, muss sich registrieren lassen. Dabei muss er für den Anbieter eindeutig zu identifizieren sein. Dann bekommt er eine unverwechselbare Bürgerportaladresse in Form einer E-Mail-Adresse zugeordnet. Zur Anmeldung an seinem Bürgerportal-Account werden dem Nutzer unterschiedliche Authentisierungsmechanismen mit unterschiedlichen Authentisierungsniveaus angeboten, aus denen er wählen kann.

Auch der künftige elektronische Personalausweis kann zur Authentisierung dienen. Jeder Bürger könnte sich damit einfach und ohne weiter erforderliche Hard- und Software anmelden. Die Synergiepotentiale der unterschiedlichen E-Government-Projekte des Bundes werden also bereits bei der konzeptionellen Entwicklung berücksichtigt. Die Nutzer sollen die Möglichkeit haben, mit Standard-Software auf die Dienste der Bürgerportale zuzugreifen. Daher werden für den Zugang zu Postfächern und zum Versenden von Nachrichten per E-Mail auch Standard-E-Mail-Clients unterstützt. Außerdem wird der Zugriff auf die Dienste auch mittels Webbrowser über ein Web-Portal möglich sein.

## Vertrauen durch Sicherheit und Zertifizierung

Wesentlich für den Erfolg der Bürgerportale ist, dass sie die Sicherheit, die sie versprechen, auch gewährleisten. Grundlage dafür ist ein geeignetes IT-Rahmen-Sicherheitskonzept, das alles, was für die Infrastruktur relevant ist, mit einbezieht.

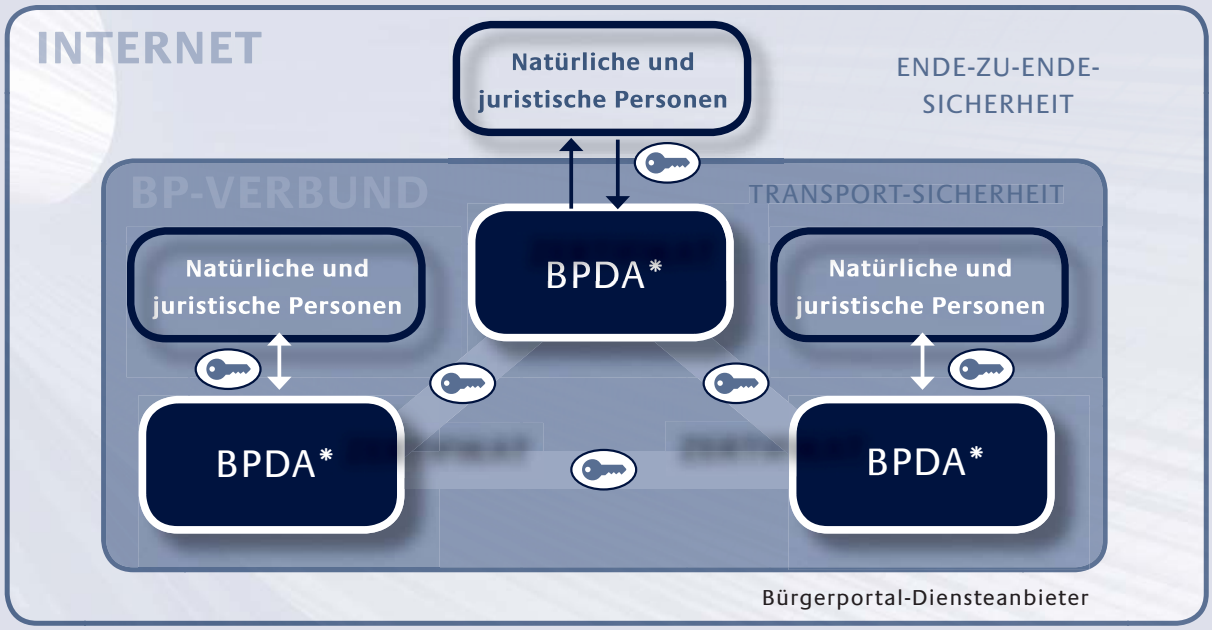
Das bedeutet: Das Konzept muss auch die Einsatzumgebung und die Art der Nutzung berücksichtigen. Ein IT-Rahmen-Sicherheitskonzept setzt eine umfassende Analyse der Risiken und des Schutzbedarfs voraus. Es definiert Anforderungen zur Umsetzung der Sicherheitsziele und empfiehlt konkrete Maßnahmen.

Ziel des vom BSI zu verantwortenden IT-Rahmen-Sicherheitskonzepts ist es, potentiellen Anbietern zu ermöglichen, ein angemessenes Sicherheitsniveau zu erreichen, gleichzeitig aber genügend Spielraum für die individuelle Gestaltung der Einsatzumgebung zu lassen. Damit haben Anbieter die Möglichkeit, ihre bereits bestehende Infrastruktur zu nutzen oder anzupassen. Auf diese Weise lässt sich der für Unternehmen effektivste Weg finden. Ein wesentlicher Grundstein für das Vertrauen in die Dienste besteht darin, dass alle Anbieter eine transparente und vergleichbare Sicherheit gewährleisten. In einem Zertifizierungsverfahren müssen sie gegenüber einer unabhängigen Stelle die Zuverlässigkeit ihrer Verfahren und Prozesse nachweisen. Neben der IT-Sicherheit sollen in diesem Verfahren auch die Funktionalität und Interoperabilität der Dienste, der Datenschutz und der Verbraucherschutz untersucht werden. Ein Zertifikat bestätigt die Konformität des Bürgerportals mit den Vorgaben und signalisiert dem Nutzer, dass er diesem Dienst vertrauen kann. Das Zertifizierungsverfahren, das mit Ausnahme der Bereiche Daten- und Verbraucherschutz ebenfalls in der Verantwortung des BSI liegt, soll – soweit möglich – an bestehende Verfahren anknüpfen.

So soll beispielsweise die IT-Sicherheitszertifizierung entsprechend ISO 27001 auf Basis von IT-Grundschutz durchgeführt werden. Entsprechende Anpassungen erfolgen nur dort, wo bürgerportalspezifische Besonderheiten dies erforderlich machen. Für einzelne, sicherheitskritische Soft- und Hardwarekomponenten ist eine Evaluierung und Zertifizierung auf Basis der Common Criteria vorgesehen.

Zusammenfassend lässt sich festhalten, dass das BSI seine Kernkompetenzen in das Projekt einbringt, indem es für das Sicherheits- sowie Zertifizierungskonzept verantwortlich ist. Damit leistet es einen wesentlichen Beitrag zur Umsetzung der Vision einer sicheren und verlässlichen Infrastruktur für eine vertrauliche und verbindliche elektronische Kommunikation.

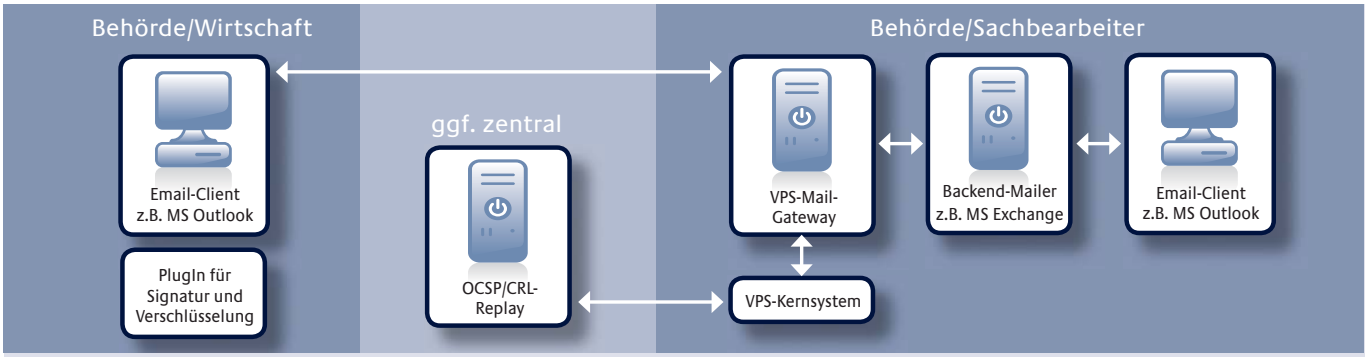
**Bürgerportale Sicherer Kommunikationsraum**




Bürgerportale sollen definierte Sicherheitsziele hinsichtlich

- Vertraulichkeit
- Authentizität
- Integrität und
- Nachvollziehbarkeit erreichen.

Das jeweilige Sicherheitsniveau der Bürgerportal-Dienste soll so hoch sein, dass die Nutzer selbst für häufige Einsatzszenarien keine zusätzlichen Sicherheitsmaßnahmen ergreifen müssen.




## VPS – die Virtuelle Poststelle des Bundes

Die Virtuelle Poststelle des Bundes (VPS), hervorgegangen aus BundOnline, bildet die Grundlage für sichere Kommunikation im E-Government. Die Teilkomponente VPS-Web hat den Prozess der Evaluierung nach Common Criteria erfolgreich durchlaufen.

Seit Ende des Jahres 2007 hat die VPS, die bisher auf Basis einer Herstellererklärung für qualifizierte Signaturen gemäß Signaturgesetz (SigG) eingesetzt werden konnte, das Gütesiegel einer bestätigten Signaturanwendungskomponente. Die E-Mail-Komponente VPS-Mail („Julia“) befindet sich derzeit bei 61 Behörden im Betrieb. Weiterhin ist das Verfahren zur VS-NfD-Zulassung durch das BSI angelaufen. Jedoch kann „Julia“ schon jetzt – bis zum Vorliegen der Zulassung – zum Verschlüsseln von VS-NfD-Mails genutzt werden.

Mit Trusted VPS stellt das BSI eine sichere Komplettlösung für das moderne E-Government zur Verfügung, welches insbesondere durch niedrigen Installations- und Administrationsaufwand überzeugt und die VPS um ein vollständiges Sicherheitskonzept erweitert. Interessierte Anwender können über das BSI die VPS Live-CD beziehen, welche einen einfachen Testbetrieb der VPS ermöglicht.

## 5.2 Zukunftsfonds und neue Technologien

*Der Zukunftsfonds ermöglicht dem BSI eigene anwendungsbezogene Forschungen auf verschiedenen Technologiefeldern. Der Fonds ist Grundlage für ein IT-Sicherheits-forschungs-Programm, das mit Mitteln in Höhe von 36.5 Millionen Euro für die Laufzeit 2006 bis 2009 ausgestattet ist.*

Eine intensive IT-Sicherheitsforschung ist unerlässlich, um der veränderten Bedrohungslage gerecht zu werden und den durch neue Technologien aufkommenden Gefährdungen rechtzeitig zu begegnen. Durch ein frühzeitiges Einbeziehen des BSI bei neuen IT-Sicherheitsfragestellungen in Deutschland besteht die große Chance, rechtzeitig zu agieren, anstatt – von der Bedrohungslage getrieben – nur zu reagieren.

### BSI-Programm zur IT-Sicherheitsforschung

Die Mittel für das IT-Sicherheitsforschungsprogramm (Zukunftsfonds) stammen aus dem mit sechs Milliarden Euro ausgestatteten Innovationsprogramm der Bundesregierung. Die Forschungen haben zum Ziel, anwendungsbezogene Neuerungen in den Technologiefeldern

- Internet-Frühwarnsysteme
- Trusted-Computing sowie
- Biometrie und Ausweissysteme

zu erarbeiten und in die Anwendung zu überführen.

Im Rahmen der Arbeiten werden folgende Themenschwerpunkte untersucht:

- **Entwicklung von Präventionstechnologien zur Abwehr neuartiger Angriffe im Internet**

  Um das Ziel der präventiven Erkennung und Abwehr der Gefahren im Bereich der IT zu erreichen, erforscht das BSI neue Lösungen. Ziel ist es, Software damit automatisch während der Erstellung oder der Inbetriebnahme auf Sicherheitslücken zu untersuchen. Sie können so schon bei der Entwicklung behoben oder vor dem Einsatz in sicherheitsrelevanten Bereichen erkannt werden.

- **Entwicklung von innovativen Technologien zur Sicherung der Internetnutzung und des Datenaustauschs**

  Ziel ist es, vernetzte IT-Landschaften vor Hackern und Schadprogrammen aus dem Internet zu schützen. Dazu sollen Technolo-gien und Werkzeuge entwickelt werden,

die gefährliche oder gefälschte E-Mails und Webseiten erkennen sowie Viren und Schadcodes zuverlässig abwehren.

- **Quantencomputerresistente Kryptoverfahren und Sicherheitstechnologien**

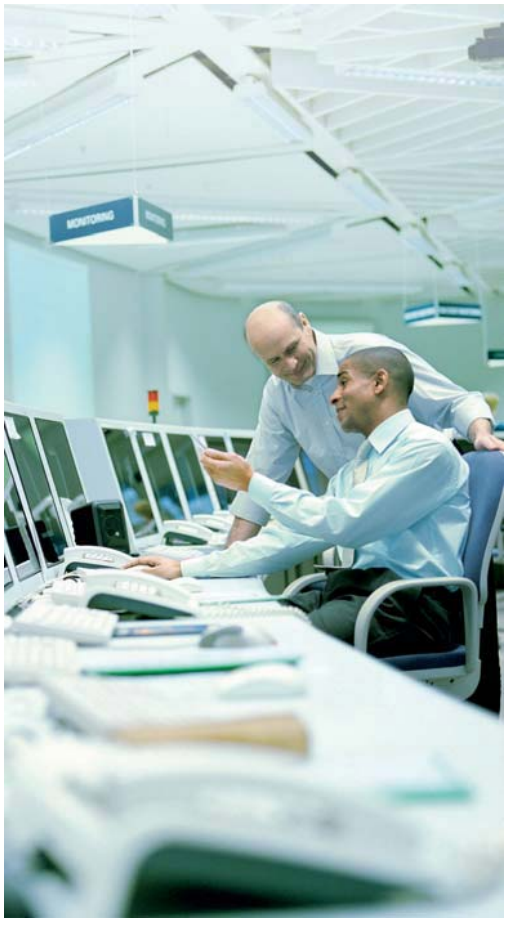
  Alternativen zu bestehenden Verfahren (z.B. Quantenkryptographie) und neue Lösungen für aufkommende Anwendungsszenarien (z.B. Multipointkommunikation) sollen identifiziert, prototypisch implementiert und sicherheitstechnisch gehärtet werden. Gleichzeitig werden die relevanten Anwendungen auf die dann notwendige Migration vorbereitet.

- **Frühwarnung vor IT-Angriffen zum Schutz von Informationsinfrastrukturen**

  Ziel ist die Erforschung der IT-Frühwarnung als Grundlage für die Entwicklung von IT-Frühwarnsystemen (IT-FWS). Es geht um die Entwicklung von Sensoren und Auswertesystemen (Soft- und Hardware), die IT-Angriffe wie Computerschadprogramme so früh wie möglich identifizieren können, um Gegenmaßnahmen zu entwickeln und die Nutzer zu warnen.

- **Forschung, Entwicklung und Weiterführung von vertrauenswürdigen und sich selbst schützenden IT-Systemen**

  PC-Clients, Server und mobile Geräte können mittels Software, aber auch in Form zusätzlicher Hardware, wie standardisierten Sicherheits-Chips (TPM), gesichert werden. Es sollen die noch ungeklärten notwendigen Bedingungen an Architekturen, Netzkomponenten, Betriebssysteme sowie Anwendungen für vertrauenswürdige und hochverfügbare IT-Systeme bestehender Lösungen (TPM) untersucht werden. Gleichzeitig sollen aber auch Soft- und Hardwarekomponenten als Alternativen zum TPM zur Erstellung einer sicheren und vertrauenswürdigen IT-Plattform erforscht werden.




- **Hochsichere Prozessorplattform für spezielle IT-Komponenten**

  Moderne, bisher nur für PC-Plattformen verfügbare Sicherheitsarchitekturen (Mikrokern-/Hypervisor-Integration, Smartcard-/TPM-Integration, geschützte Speicherbereiche, etc.) sollen auch für embedded Prozessorplattformen realisiert werden.

- **Neue Verfahren zur Identifikation und Lokalisierung**

  Neben der notwendigen Weiter- und Neuentwicklung biometrischer Verfahren und der entsprechenden Schutzmechanismen zeigt die kombi-

nierte Nutzung verschiedener biometrischer Merkmale Synergieeffekte, die zur Steigerung der Sicherheit bei der Erkennungsleistung genutzt werden können. Ziel des Projektes ist es, diese Effekte und Schutzmechanismen zu erforschen, zu entwickeln und prototypisch umzusetzen.

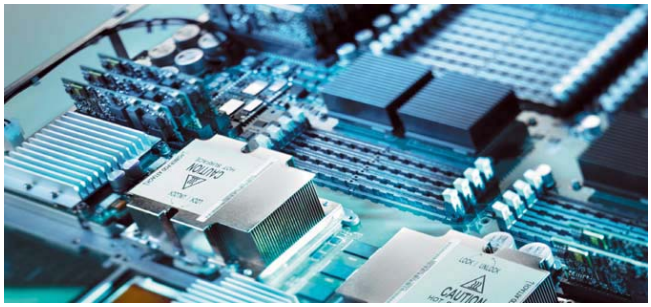
- **Entwicklung innovativer kontaktloser Sicherheits-Token für den breiten Einsatz**

  Ziel des Projektes ist die Erforschung und Erprobung neuer Basistechniken für kontaktlose Sicherheits-Token. Hierzu sollen u.a. neue Displays zusammen mit innovativen kryptographischen Konzepten zu kontaktlosen Sicherheits-Token kombiniert werden. So wird ein erheblicher Gewinn an IT-Sicherheit und Komfort erzielt. Weiterhin werden innovative kontaktlose Authentisierungsmechanismen erforscht.

- **Sicherheitsarchitektur für Mikro-Sensornetze**

  Ziel ist die Entwicklung einer breit anwendbaren Sicherheitsarchitektur für Sensorsysteme mit dem Schwerpunkt sichere Sensor-Identifikation und Kommunikation. Ausgehend von einer Felduntersuchung soll eine auf ausgesuchte Anwendungen zugeschnit-tene Sicherheitsarchitektur für Mikrosensoren und -aktoren entwickelt, prototypisch realisiert und im konkreten Einsatz erprobt und analysiert werden.

## Nachhaltigkeit



Von besonderer Bedeutung für das BSI ist die nachhaltige Wirkung der Ergebnisse der IT-Sicherheitsforschung. Sie dienen dem Ziel, neue Sicherheitstechnologien sowie Entwicklungsleitlinien und Prüfvorgaben zu erarbeiten und zu etablieren. Die IT-Sicherheitsforschung wird in sensitiven Anwendungsbereichen zu neuen Sicherheitstechnologien führen. Wenn es überdies gelingt, mit Forschungseinrichtungen und IT-Herstellern auf der einen Seite und für den Anwendungsbereich zuständigen Behörden auf der anderen Seite die neuen Systeme zu erarbeiten, dann ist das ein großer Schritt für die Förderung der IT-Sicherheit in Deutschland. Aber die Vorgehensweise bedeutet noch mehr: So kann IT-Sicherheitsforschung zu einem hervorragenden Exportförderinstrument deutscher IT-Sicherheitstechnologie ins Ausland werden.

# Amtsleitung und Ansprechpartner

## Präsident

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

## Vizepräsident

**Michael Hange,**
*Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik*

## Abteilung 1

**Dr. Hartmut Isselhorst,**
*Leiter der Abteilung 1 – Sicherheit in Anwendungen, Kritischen Infrastrukturen und in Netzen*

## Abteilung 2

**Dr. Gerhard Schabhüser,**
*Leiter der Abteilung 2 – Kryptographie und Abhörsicherheit*

## Abteilung 3

**Bernd Kowalski,**
*Leiter der Abteilung 3 – Zertifizierung, Zulassung und Konformitätsprüfungen, Neue Technologien*

## Abteilung Z

**Horst Samsel,**
*Leiter der Abteilung Z – Zentrale Aufgaben*

## Öffentlichkeitsarbeit

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

## Pressesprecher

**Matthias Gärtner,**
*Pressesprecher*
*E-Mail:*
*matthias.gaertner@bsi.bund.de*

# Impressum

Bundesamt
für Sicherheit in der
Informationstechnik

**Herausgeber**
Bundesamt für Sicherheit in der Informationstechnik – BSI
53175 Bonn

**Bezugsstelle**
Bundesamt für Sicherheit in der Informationstechnik – BSI
Referat 321 – Information und Kommunikation, Öffentlichkeitsarbeit
Postfach 20 03 63, 53133 Bonn
Tel: +49 (0) 228 99 95 82-0
E-Mail: publikationen@bsi.bund.de
Internet: www.bsi.bund.de

**Texte und Redaktion**
Sebastian Frank, BSI; Volker Thomas, Thomas Presse & PR

**Layout & Gestaltung**
Thomas Presse & PR, Berlin/Bonn
Grafik: Annette Conradt, Pierre Boom
Screen-Version: Ludwig Lang
Tel: +49 (0) 30 21 99 66 16
E-Mail: info@thomas-ppr.de
Internet: www.thomas-ppr.de

**Bildnachweis**
AVM GmbH, Berlin Partner/FTB-Werbefotografie, BMI/Photothek, Pierre Boom, BSI/Referat Öffentlichkeitsarbeit, Bundesanzeiger Verlagsgesellschaft mbH, Bundesbildstelle, Bundesdruckerei GmbH, Bundesministerium für Gesundheit (BMG), Cross Match Technologies GmbH, Deutsche Bahn AG, Elster/Bayerisches Landesamt für Steuern, Andreas Ernst, Fujitsu Siemens Computers GmbH, istockphoto, LinuxTag e.V., Messe Essen GmbH, Messe München GmbH, Polizei Mettmann, OHB-System AG, Reed Exhibitions Deutschland GmbH, Rohde & Schwarz GmbH, SecuMedia Verlags-GmbH, Security Networks AG, Sony Ericsson Mobile Communications AB, Studio Koslowski/ Bundesnetzagentur, SWR Media Services GmbH, Günter Wicker/Berliner Flughäfen, Xilinx Inc.

**Stand**
Juni 2008

Diese Datei ist Teil der Öffentlichkeitsarbeit der Bundesregierung; sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.