Bundesamt
für Sicherheit in der
Informationstechnik

Mit Sicherheit.

BSI Jahresbericht 2011/2012

Allianz für Cyber-Sicherheit
Mehr Schutz
durch Kooperation

Smart Meter
Sicherheit für
intelligente Netze

Kritische IT-Systeme
Effizienz auf Kosten
der Sicherheit?

Mit Sicherheit.

BSI Jahresbericht 2011/2012

Hans-Peter Friedrich,
Bundesminister des Innern

Liebe Leserinnen und Leser,

das Internet hat sich in den letzten Jahren zu einer Kritischen Infrastruktur wie Strom und Wasser entwickelt. Die Erschließung neuer Anwendungsbereiche wie Industrie 4.0, Smart Cities und Machine-to-Machine Communication können nur gelingen, wenn ein Ausbau der Breitbandversorgung erfolgt und die Bürgerinnen und Bürger Vertrauen in die Zuverlässigkeit und Sicherheit dieser Infrastruktur haben. Neue Gefährdungen wie Angriffe auf mobile Endgeräte und Cyber-Attacken stellen eine Herausforderung für die gesamte Gesellschaft und deren Institutionen dar. Das Ziel in den Jahren 2011 und 2012 war geprägt durch Gewährleistung von Sicherheit auf möglichst hohem Niveau, ohne dass hierdurch die wirtschaftliche Prosperität der Internetwirtschaft geschmälert wurde.

Die Cyber-Angriffe sind in den Jahren häufiger und professioneller geworden. Um dieser Entwicklung gezielt entgegenzutreten, hat die Bundesregierung die Cyber-Sicherheitsstrategie für Deutschland im Februar 2011 verabschiedet und mit der Einrichtung des Nationalen Cyber-Sicherheitsrates und des Nationalen Cyber-Abwehrzentrums einen wichtigen Meilenstein in Richtung mehr Sicherheit gesetzt.

Es war mir in der Vergangenheit ein besonderes Anliegen, mich um den Schutz der sogenannten Kritischen Infrastrukturen persönlich zu kümmern. Aus diesem Grunde habe ich im Sommer 2012 Gespräche mit Geschäftsführern und Vorstandsvorsitzenden von Betreibern Kritischer Infrastrukturen geführt. Ziel dieser Gespräche war es, zu sensibilisieren und herauszufinden, wie es mit der Sicherheit der Informationsinfrastrukturen in diesen Unternehmen aussieht. Das Ergebnis fiel unterschiedlich aus, sodass ich es für notwendig erachtete, einen Entwurf für ein IT-Sicherheitsgesetz ausarbeiten zu lassen.

Das Bundesamt war in den Jahren seines Bestehens nicht nur für mich, sondern auch für Bundesbehörden, die Wirtschaft und für Bürger immer ein kompetenter Ansprechpartner und Ratgeber in Fragen der Cyber- und IT-Sicherheit. Mit der weiteren Öffnung des BSI in Richtung Wirtschaft durch die „Allianz für Cyber-Sicherheit“ hat das BSI exemplarisch sein hohes Engagement und seine Innovationskraft unter Beweis gestellt. Gemeinsam mit dem BITKOM gegründet, soll die „Allianz für Cyber-Sicherheit“ dazu beitragen, Informationen und Warnungen zu Cyber-Attacken zwischen Staat und Wirtschaft leichter, schneller und zielgerichteter auszutauschen, um potenzielle Schäden möglichst gering zu halten. Nach einer Pilotphase ist die Mitgliederanzahl aus Wirtschaft und Verwaltung stark gewachsen.

Ich wünsche Ihnen durch eine interessante weiterführende Lektüre des Jahresberichts viele neue Anregungen für Ihren persönlichen Beitrag zur Cyber-Sicherheit.

Hans-Peter Friedrich
Bundesminister des Innern

Liebe Leserinnen und Leser,

lassen sich Online- und Offline-Welt heute noch voneinander trennen? Diese Frage mag im persönlichen Umfeld jeder für sich selbst beantworten. Fakt ist jedoch, dass die Vorteile der zunehmenden Vernetzung vieler Lebens- und Arbeitsbereiche ebenso wie viele Risiken, die uns im Netz begegnen, heute reale Auswirkungen auf unser Leben haben. Es ist keine Utopie mehr, dass Cyber-Angriffe zu zwischenstaatlichen Konflikten führen oder Kritische Infrastrukturen so manipulieren können, dass die Versorgung der Bevölkerung in Gefahr ist. Viel alltäglicher sind aber die kleinen und großen Gefahren im Netz, die uns reales Geld kosten oder bei denen Daten, die uns als reale Person ausmachen, in die falschen Hände geraten.

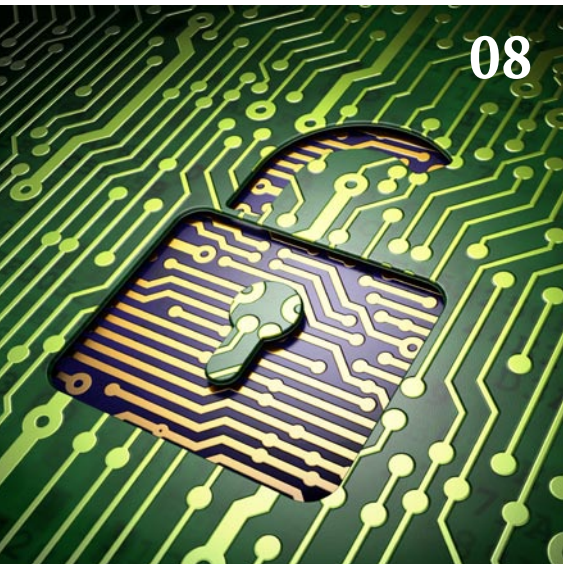
Auch im Unternehmen lassen sich On- und Offline immer weniger voneinander trennen. Unter dem Stichwort Industrie 4.0 schreitet die Informatisierung der Wirtschaft voran und immer häufiger werden industrielle Prozesse über IT und Internet gesteuert. Informationssicherheit wird damit ein unmittelbarer Faktor in der Wertschöpfungskette. Als Endverbraucher zeigt uns die im Zuge der Energiewende geführte Diskussion um intelligente Netze und „Smart Meter“, welche positiven und negativen Folgen diese Entwicklung bis in unsere Wohnzimmer haben kann.

Gleichzeitig sehen wir uns immer professioneller agierenden Angreifern gegenüber. Cyber-Angriffe werden dabei von unterschiedlichen Tätergruppen mit unterschiedlichen Zielsetzungen, teils jedoch mit enormen finanziellen und personellen Ressourcen durchgeführt. Angesichts dieser Herausforderungen muss sich das BSI immer wieder neuen Ansätzen öffnen und den Austausch mit anderen Beteiligten suchen. In dieser Hinsicht haben wir in den vergangenen zwei Jahren einige vielversprechende Entwicklungen auf den Weg gebracht. So hat das Nationale Cyber-Abwehrzentrum im Juni 2011 unter Federführung des BSI seine Arbeit aufgenommen. Diese Informationsdrehscheibe hat im Wesentlichen eine Verkürzung der Kommunikationswege zwischen den verschiedenen, im Falle eines Cyber-Angriffs beteiligten Behörden zur Aufgabe. Ziel ist hier vor allem der Erkenntnisgewinn über Angriffsmethoden, um entsprechende Präventions- und Schutzmaßnahmen zu entwickeln. Die Schaffung eines umfassenden Lagebilds hat auch die „Allianz für Cyber-Sicherheit“ zum Ziel, die das BSI gemeinsam mit dem Branchenverband BITKOM gegründet hat. Sie bildet eine Plattform zum Informationsaustausch mit Institutionen aus privater und öffentlicher Hand, die ihre Erfahrungen mit Cyber-Angriffen konsolidieren.

Ich freue mich, Ihnen mit dem Jahresbericht 2011/2012 einen aktuellen Einblick in die vielfältigen und herausfordernden Arbeitsfelder des BSI geben zu können, und wünsche Ihnen eine anregende Lektüre.

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Michael Hange,
Präsident
des Bundesamtes für Sicherheit
in der Informationstechnik



Cyber-Sicherheit – Schutz und Abwehr

IT-Sicherheit gestalten – Mindeststandards setzen

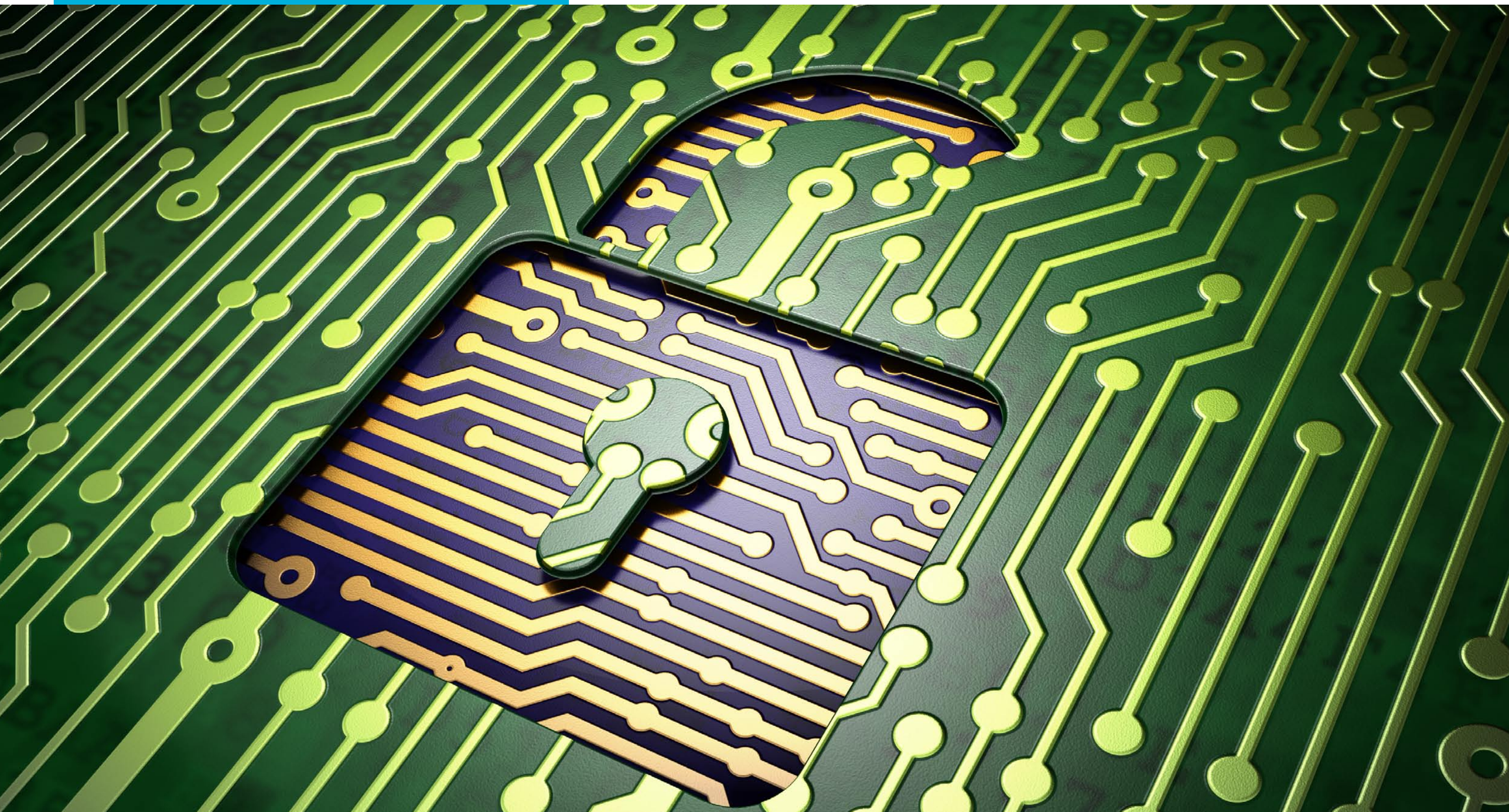
Cyber-Sicherheit – Schutz und Abwehr

IT-Sicherheit gestalten – Mindeststandards setzen

Technologie – sichere Lösungen

Weichen stellen – Zukunft planen

Cyber-Sicherheit – Schutz und Abwehr



Die Cyber-Sicherheits-strategie für Deutschland und ihre Umsetzung

Interview mit Staatssekretärin Cornelia Rogall-Grothe,
Beauftragte der Bundesregierung für Informationstechnik

Informationstechnologie ist in fast allen Lebensbereichen etabliert. Sie bietet unseren Bürgerinnen und Bürgern beinahe täglich neue Möglichkeiten. Auch Unternehmen, Wissenschaft und Verwaltung profitieren von der zunehmenden Digitalisierung und Vernetzung unserer Lebens- und Arbeitswelt. Sie birgt jedoch auch Risiken, denn viele Bereiche sind heute in hohem Maße abhängig von funktionierender IT und sicheren Informationsinfrastrukturen. Vor diesem Hintergrund hat die Bundesregierung 2011 die Cyber-Sicherheitsstrategie für Deutschland beschlossen. Ziel ist es, die Cyber-Sicherheit auf einem der Bedeutung und der Schutzwürdigkeit der vernetzten Informationsinfrastrukturen angemessenen Niveau zu gewährleisten, ohne die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen.

Frau Staatssekretärin Rogall-Grothe, vor zwei Jahren wurde die Cyber-Sicherheitsstrategie für Deutschland beschlossen. Was hat sich seitdem verändert? Ist der Cyber-Raum sicherer geworden?

Wir beschäftigen uns nicht erst seit 2011 mit dem Thema Cyber-Sicherheit. Die Cyber-Sicherheitsstrategie ist eine konsequente Weiterentwicklung der bisherigen IT-Sicherheitspolitik und der IT-Sicherheitsaktivitäten auf Bundesebene. Mit den Umsetzungsplänen BUND und KRITIS haben wir beispielsweise schon lange vor 2011 in der Bundesverwaltung ebenso wie im Bereich der Kritischen Infrastrukturen Maßnahmen und Prozesse etabliert.

Wir beobachten eine zunehmende Professionalisierung von Angreifern und Angriffsmethoden und somit eine zunehmend dynamische Gefährdungslage, auf die schnell und umfassend reagiert werden muss. Mit der Cyber-Sicherheitsstrategie haben wir einen mehrstufigen Ansatz entwickelt, der Privatanwender genauso einschließt wie die Wirtschaft. Da man die Gewährleistung von Sicherheit als einen – wohl nicht abschließbaren – Prozess begreifen muss, können wir unseren Standort nicht als „am Ziel angekommen" definieren, wir sind aber bereits ein gutes Stück vorangekommen.

Welche Schwerpunkte wollen Sie in den nächsten Monaten setzen?

Die Gewährleistung von Sicherheit im Cyber-Raum und der Schutz der Kritischen Informationsinfrastrukturen sind zu existenziellen Fragen des 21. Jahrhunderts geworden und erfordern ein hohes Engagement des Staates.

Gleichwohl ist dies eine Herausforderung, die der Staat nicht allein, sondern nur gemeinsam mit Wirtschaft und Wissenschaft lösen kann. Insofern ist die von BSI und BITKOM initiierte Allianz für Cyber-Sicherheit im Rahmen der Umsetzung der Cyber-Sicherheitsstrategie ein wichtiger Meilenstein.

Darüber hinaus legen wir nach wie vor ein besonderes Augenmerk auf den Schutz Kritischer Infrastrukturen. Bundesinnenminister Dr. Friedrich hat im Sommer 2012 eine Reihe von konstruktiven Gesprächen mit Vorständen und Verbänden aus den relevanten KRITIS-Sektoren geführt. Dabei hat sich gezeigt, dass das Schutzniveau sehr unterschiedlich ist. Angesichts der angespannten Bedrohungslage und aufgrund der ständig wachsenden Abhängigkeit von der IT sind jedoch widerstandsfähige IT-Systeme und Netze flächendeckend für alle wichtigen Infrastrukturbereiche notwendig.

Mit hochrangigen Vertretern aus den Wirtschaftsverbänden, IT- und Anwenderunternehmen, IT-Sicherheitsunternehmen, der Wissenschaft sowie Ressort- und Ländervertretern habe ich an einem sogenannten Runden Tisch über eine Verbesserung der Rahmenbedingungen für IT-Sicherheitshersteller in Deutschland gesprochen. Die Einberufung dieses Runden Tisches war Teil und ist Folge des „Acht-Punkte-Programms zum besseren Schutz der Privatsphäre“, das Bundeskanzlerin Dr. Merkel am 19. Juli 2013 vorgestellt hatte. An diesem Runden Tisch haben wir uns insbesondere auch darüber Gedanken gemacht, mit welchen konkreten Maßnahmen die nationale technologische Souveränität gestärkt werden kann. Denn die Fähigkeit, auch bei einer zunehmenden Digitalisierung Sicherheitsrisiken noch zutreffend selbständig einschätzen und die notwendigen Sicherheitsmaßnahmen selbst definieren zu können, wird entscheidend sein.

Dabei kommt es auch auf die Frage an, an welchen besonders relevanten kritischen Punkten nur Produkte von verlässlichen und vertrauenswürdigen Herstellern zum Einsatz kommen sollten. Damit auch in Zukunft eine ausreichende Zahl vertrauenswürdiger Hersteller in Deutschland ihre Produkte anbietet, haben wir am Runden Tisch verschiedene Vorschläge erarbeitet. Hierzu zählen z. B. die Bündelung der Nachfrage von Bund, Ländern und Kommunen, um auf diese Weise einen relevanten Markt für IT-Sicherheitslösungen zu schaffen, bei stärkerer Berücksichtigung nationaler IT-Sicherheitsinteressen bei öffentlichen Vergaben. Ferner wurde u. a. auch die Harmonisierung von IT-Sicherheitsstandards in der EU zur Förderung eines einheitlichen Marktes und der Ausbau von zertifizierten IT-Sicherheitsdienstleistern zur Beratung von Unternehmen sowie der weitere Ausbau der FuE-Anstrengungen als erforderlich erachtet. Wir werden diese Vorschläge innerhalb der Bundesregierung nun mit Blick auf die anstehende Legislaturperiode im Einzelnen prüfen und bewerten.

Wie sehen die konkreten Vorschläge zur Verbesserung der Cyber-Sicherheit in Deutschland aus?

Die Qualität und Sicherheit unserer Infrastrukturen ist und muss auch in Zukunft ein Standortvorteil Deutschlands bleiben. Hierbei wird es maßgeblich auf die IT-Sicherheit ankommen. Das Bundesinnenministerium hat deshalb den Referentenentwurf für ein IT-Sicherheitsgesetz erarbeitet. In dem Entwurf setzen wir drei Schwerpunkte: Die Betreiber Kritischer Infrastrukturen, die aufgrund der möglichen Folgen eines Ausfalls oder einer Beeinträchtigung naturgemäß eine besondere gesamtgesellschaftliche Verantwortung haben, sind zu einer Erhöhung des Schutzes der von ihnen eingesetzten Informationstechnik und zur Verbesserung ihrer Kommunikation mit dem Staat zu verpflichten. Des Weiteren müssen wir die Telekommunikations- und Telemediendiensteanbieter, die eine Schlüsselrolle für die Sicherheit des Cyber-Raums haben, stärker als bisher hierfür in die Verantwortung nehmen. Auch ist das BSI als nationale IT-Sicherheitsbehörde in seinen Aufgaben und Kompetenzen zu stärken. Und weil Internetprovider eine große Verantwortung für die Sicherheit der Kundensysteme tragen, da Schadsoftware häufig über deren Systeme transportiert wird, enthält der Referentenentwurf auch spezifische Vorschläge in Richtung der Provider-Verantwortung. So sollen die Nutzer beispielsweise von ihren Providern über bekannt gewordene Störungen ihrer eigenen Systeme unterrichtet werden. Auch sollen sie von den Providern, soweit dies möglich und zumutbar ist, Hinweise zur Beseitigung der Störungen zur Verfügung gestellt bekommen.

Mir ist bewusst, dass Teile der deutschen Wirtschaft lieber weiterhin ausschließlich auf freiwillige Kooperation setzen würden. Ich bin jedoch der Überzeugung, dass wir einen gesetzlichen Rahmen brauchen. Allein mit freiwilligen Maßnahmen sind wir in der Vergangenheit hinter unseren Zielen zurückgeblieben. Das Maß der Selbstregulierung ist aber auch in unserem Gesetzentwurf so hoch wie möglich angesetzt. Die geforderten Mindeststandards hinsichtlich der IT-Sicherheit Kritischer Infrastrukturen beispielsweise sollen maßgeblich von den betroffenen Verbänden und Betreibern selbst als branchenspezifische Standards entwickelt und anschließend staatlich anerkannt werden.

CERT-Bund:
Eine Erfolgsgeschichte im Dienste der IT-Sicherheit

In einem tagesaktuellen Geschäft wie der IT-Sicherheit hat man nur selten Gelegenheit, innezuhalten und zurückzuschauen. Ein Jubiläum ist eine solche Möglichkeit – und ein Jubiläum hat CERT-Bund, das Computernotfallteam der Bundesverwaltung, 2012 feiern können: 15 Jahre zuvor, 1997, wurde das CERT des BSI in das internationale Forum of Incident Response and Security Teams (FIRST) aufgenommen und damit nach seiner Gründung im Jahr 1994 auch international sichtbar.

Kauto Huopio, Chief Specialist, Finnish Communications Regulatory Authority (FICORA)/CERT-FI

„The Internet is a global phenomenon – cyber threats do not stop at country borders. An essential part of effective ICT crisis management is international networking and cooperation between CERTs in Europe and worldwide. CERT-FI shares a mutual trust relationship with CERT-Bund that benefits our daily work in Finland and on an international level."

Stefan Ritter,
Referatsleiter Lagezentrum
und CERT-Bund

Die Geschichte des CERT-Bund – die Abkürzung steht für Computer Emergency Response Team – begann in den 1990er Jahren. Bereits 1989 gab es unter der Federführung des Bundesministeriums des Innern eine Arbeitsgruppe aus Mitarbeitern des BMI-Fachreferats, der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung, des Bundesamts für Verfassungsschutz (BfV), des Bundesnachrichtendiensts (BND) und des Bundesrechnungshofs, die unter der Bezeichnung „KITS (Kommunikationskreis IT-Sicherheit)“ ein Alarmierungskonzept bei IT-Sicherheitsvorfällen entwickelte. In diesen frühen Jahren der IT-Sicherheit war die Bedrohung durch Computerviren bereits relevant, wobei es jedoch verglichen mit der heutigen Zeit nur einen Bruchteil an Schadprogrammen gab. Mit dieser Gefahr hat sich zunächst die BND-Zentralstelle für Chiffrierwesen befasst, aus der sich später die Zentralstelle für die Sicherheit in der Informationstechnik herausbildete, die wiederum eine der Keimzellen des 1991 auf besonderer gesetzlicher Grundlage gegründeten BSI war. Dort wurde das Referat „Abwehr von Schadprogrammen“ eingerichtet, das u. a. die Aufgabe hatte, vor Viren zu warnen.

Damals hatten Computerviren und -würmer allerdings noch einen eher exotischen Charakter: Es gab lediglich ein bis zwei neue Viren pro Monat. Zur Warnung reichte die regelmäßige Veröffentlichung im Bundesanzeiger-Blatt. Um auf die Bedrohung durch diese Viren zu reagieren, hat das BSI Anfang der 90er Jahre der Bundesverwaltung ein Antivirenprogramm zur Verfügung gestellt. Dazu wurde eine Master-Diskette ans BSI geliefert, das dann mittels einer hauseigenen Kopierstation 500 Disketten erstellte, diese in Handarbeit etikettierte und vierteljährlich an die Bundesverwaltung versendete.

Antivirusdisketten aus den 90er Jahren

Die Zahl der Computerviren vermehrte sich in den folgenden Jahren jedoch explosionsartig. Somit musste sich auch der Warnansatz vor einzelnen Viren hin zu leichter überschaubaren Hinweisen auf Schwachstellen und Patches in den Programmen und Anwendungen wandeln.

Jahrtausend-Probleme und Liebesbriefe

1994 wurde dann das erste BSI-interne Computer Emergency Response Team (CERT) eingerichtet. Man hatte erkannt, dass nicht nur die Abwehr von Schadprogrammen und der Hinweis auf Schwachstellen, sondern auch die Reaktion auf IT-Sicherheitsvorfälle wichtig sind. Ein solcher IT-Sicherheitsvorfall, wenn nicht gar eine weltweite IT-Krise, drohte augenscheinlich zum Jahreswechsel 1999/2000, als der „Millenium-Bug" beziehungsweise das „Jahr-2000-Problem" nicht nur die deutschen Computerbesitzer beschäftigte. Die Angst vor Programmabstürzen und Fehlfunktionen aufgrund des bisher üblichen zweistelligen Datumsformats, das nach dem Jahrtausendwechsel auf einmal vierstellig sein musste, führte auch in der Bundesverwaltung zu eingehenden Analysen der IT-Systeme und massiven Vorbereitungen auf deren möglichen Ausfall. Das BSI übernahm dabei die Federführung in der entsprechenden Projektgruppe. Die Vorbereitung erwies sich als sehr gut und so verstrich die alkoholfreie Silvesternacht des Jahres 1999/2000 für den Krisenstab im BSI weitgehend ereignislos. Spätestens als in der Nacht bekannt wurde, dass Australien und Japan ohne größere Probleme den Jahreswechsel geschafft hatten, war man auch in Deutschland etwas gelassener.

Kurz danach schlug der Virus „Love-Letter" zu, der sich wurmähnlich massenhaft verbreitete und mit seiner verführerischen Betreffzeile („I love you") ein durchschlagender Erfolg wurde. Als Konsequenz auf diese Ereignisse eröffnete der damalige Bundesinnenminister Otto Schily (SPD) 2001, nur wenige Tage vor den Terroranschlägen des 11. Septembers, im BSI das Team CERT-Bund als eigenständiges Referat mit zunächst sechs Mitarbeitern.

IT-Sicherheit ist international

Der Millenium-Bug ebenso wie der Love-Letter-Virus zeigten, dass die IT-Sicherheit ein Thema ist, das mit kooperativem Ansatz auch über Staatsgrenzen hinaus betrachtet werden muss. CERT-Bund hat sich daher aktiv an der Gründung von zwei mittlerweile sehr erfolgreichen Arbeitskreisen beteiligt: dem deutschen CERT-Verbund und der European Governmental CERT-Group.

Der deutsche CERT-Verbund entwickelte sich aus der Idee, die vielen mittlerweile vorhandenen CERTs besser zu vernetzen und sich untereinander auszutauschen. Etwa ein Dutzend Teams war anfangs bereit, ein Non Disclosure Agreement (Vertraulichkeitsvereinbarung) zu unterzeichnen, zum Teil ergänzt durch einen Code of Conduct für eine besonders intensive und engagierte Zusammenarbeit. Mittlerweile sind bereits 30 Teams aus Verwaltung, Wirtschaft und Forschung im CERT-Verbund aktiv.

Die European Governmental CERT-Group ist der Zusammenschluss der technischen Experten zunächst einer Handvoll europäischer Regierungs-CERTs. Alle Teams standen im Bereich IT-Sicherheit vor denselben Herausforderungen und wollten sich vor diesem Hintergrund operativ auch international besser austauschen. Grundlage für die mittlerweile sehr fruchtbare und erfolgreiche Zusammenarbeit ist ein besonderes Vertrauen, das sich über die Jahre entwickelt hat und das es ermöglicht, auch über Landesgrenzen hinweg offen über Bedrohungen und Probleme reden zu können. Die Gruppe ist auf mittlerweile 13 Länder und 14 Teams angewachsen, die sich durch ein sehr strenges Auswahlverfahren qualifizieren müssen. Dieser Kreis ist für das BSI oft Quelle seiner wertvollsten Informationen und Frühwarnungen.

Einrichtung des Nationalen IT-Lagezentrums

2005 erhielt das Referat CERT-Bund im Rahmen des Nationalen Plans zum Schutz der Informationsinfrastrukturen den Auftrag, ein IT-Lagezentrum und IT-Krisenreaktionszentrum einzurichten. Aufgabe des Lagezentrums ist es, jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland zu verfügen, um somit den Handlungsbedarf und die Handlungsoptionen bei IT-Sicherheitsvorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft schnell und kompetent einschätzen zu können.

Das nationale IT-Lagezentrum des BSI

Mit der Novellierung des BSI-Gesetzes 2009 erhielt das BSI durch § 7 die rechtliche Grundlage und Befugnis, öffentliche Warnungen vor IT-Produkten und -Dienstleistungen auszusprechen. Mit dieser Befugnis geht das BSI sehr sorgsam um, denn eine öffentliche Warnung und die damit verbundene Medienaufmerksamkeit können erhebliche Auswirkungen auf Reputation und Geschäftserfolg des betroffenen Unternehmens haben. Aus der Erfahrung lässt sich jedoch auch sagen, dass der Paragraf 7 zu einer wesentlichen Verbesserung der Kontakte und der Zusammenarbeit des BSI mit den IT-Herstellern geführt hat.

Vertrauen als Grundlage der Zusammenarbeit

Die genannten Meilensteine zeigen, wie sich CERT-Bund angesichts einer dynamischen Bedrohungslage weiterentwickelt hat. Es gibt jedoch einige grundlegende Aspekte, die entscheidend für seine Leistungsfähigkeit sind.

- So konnte sich CERT-Bund über die Jahre als zentrale Anlaufstelle bei IT-Sicherheitsvorfällen zunächst in der Bundesverwaltung, später auch im Bereich der Kritischen Infrastrukturen sowie im internationalen Umfeld etablieren. Als unabhängige Einrichtung ohne kommerzielle Interessen genießen BSI und CERT-Bund eine besondere Vertrauensstellung.
- Zu diesem institutionellen Vertrauen kommt das persönliche Vertrauen in die Mitarbeiter, die in vielen Gremien präsent sind und aktiv den Austausch suchen. Dieses persönliche Vertrauen gründet sich auf die umfangreiche Fachexpertise und den großen Erfahrungsschatz, den die Mitarbeiter von CERT-Bund u. a. durch den täglichen Umgang mit IT-Schwachstellen und -Vorfällen aufbauen konnten.
- Die Vernetzung mit anderen CERT-Teams im In- und Ausland ebenso wie mit anderen Akteuren der IT-Sicherheit ist ein wesentlicher Faktor für die schnelle Reaktionsfähigkeit von CERT-Bund, denn sie gestattet es, umgehend die notwendigen Ansprechpartner zu finden und vertraulich Informationen über Schwachstellen, Bedrohungen und Sicherheitsvorfälle zu erlangen.

In den fast zwei Jahrzehnten seines Bestehens haben sich das CERT des BSI und das daraus hervorgegangene CERT-Bund im dynamischen Umfeld der IT-Sicherheit stetig weiterentwickelt und einen guten Ruf bei Zielgruppen und Partnern erarbeitet. Auf dieser Basis ist CERT-Bund auch in Zukunft gut gerüstet, um seine Aufgaben zu erfüllen und weiterhin für mehr IT-Sicherheit in Staat, Wirtschaft und Gesellschaft zu sorgen.

LÜKEX

Ende 2011 fand zum fünften Mal die „Länderübergreifende Krisenmanagementübung (EXercise)“ (LÜKEX) statt. Als nationale Übungsreihe im strategischen Krisenmanagement zielt LÜKEX darauf ab, das gemeinsame Krisenmanagement von Bund und Ländern auf politisch-administrativer Ebene bei außergewöhnlichen Gefahren- und Schadenslagen zu optimieren. Hauptverantwortlich für die Planung und Steuerung der LÜKEX ist das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Bisherige Themen waren etwa Stromausfall, Terroranschlag und „Schmutzige Bombe“.

2011 wurde im Rahmen der LÜKEX ein IT-Sicherheitsszenario durchgespielt, bei dessen Vorbereitung und Durchführung das BSI und das nationale IT-Lagezentrum eine zentrale Rolle spielten. Quer durch Deutschland kam es dabei fiktiv zu schwerwiegenden IT-Vorfällen mit zum Teil erheblichen Auswirkungen auf das öffentliche Leben und die wirtschaftlichen Abläufe. Aufgabe für die Teilnehmer war es, gemeinsam nach den Ursachen der Vorfälle zu suchen und deren Auswirkungen zu begrenzen.

Die Krisenstäbe des Bundes und der Länder, mehrere beteiligte Bundesbehörden sowie Vertreter von Kritischen Infrastrukturen befassten sich damit mit einem Thema, das vorher eher den IT-Spezialisten vorbehalten war und mit dem sie bislang kaum Erfahrung sammeln konnten. Nun galt es, sich kurzfristig in die Besonderheiten einer IT-Bedrohung hineinzudenken, die Abhängigkeit des Staates und der Gesellschaft von der IT zu erkennen und angemessene Entscheidungen zu treffen.

Das Nationale Cyber-Abwehrzentrum

Am 16. Juni 2011 eröffnete Bundesinnenminister Dr. Hans-Peter Friedrich das Nationale Cyber-Abwehrzentrum in Bonn und stellte gemeinsam mit den Präsidenten der beteiligten Behörden die Aufgaben der neuen „Informationsdrehscheibe“ der Presse vor. Das Cyber-Abwehrzentrum wurde als gemeinsame Plattform zum schnellen Informationsaustausch und zur besseren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Sicherheitsvorfälle errichtet. Unter der Federführung des BSI und mit direkter Beteiligung des Bundesamtes für Verfassungsschutz (BfV) und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) hatte das Cyber-Abwehrzentrum bereits am 1. April 2011 seine Arbeit aufgenommen. Die drei Behörden stellen gemeinsam die zehn festen Mitarbeiterinnen und Mitarbeiter des Cyber-Abwehrzentrums, die in den Räumlichkeiten des BSI in Bonn zusammenarbeiten. Seit Juni 2011 wirken als assoziierte Behörden auch das Bundeskriminalamt (BKA), die Bundespolizei (BPol), das Zollkriminalamt (ZKA), der Bundesnachrichtendienst (BND) sowie die Bundeswehr mit. Das Cyber-Abwehrzentrum ist Bestandteil der vom Bundesministerium des Innern erarbeiteten Cyber-Sicherheitsstrategie für Deutschland, die von der Bundesregierung am 23. Februar 2011 beschlossen wurde.

In den ersten zwei Jahren stand die Bearbeitung von bekannt gewordenen IT-Sicherheitsvorfällen im Fokus der Arbeit des Cyber-Abwehrzentrums. Eine der Herausforderungen dabei war es, bei zum Teil sehr unterschiedlichen Behördenkulturen sowie auch unterschiedlichem Wissens- und Erfahrungsstand in der Cyber-Sicherheit eine effiziente Bearbeitung der Vorfälle zu organisieren. Die Bearbeitung der Fälle gliedert sich in die Arbeitsschritte technische Analyse, Täterermittlung (wenn möglich), Ermittlung von Zielen von Cyber-Angriffen, Abschätzung von Schadenspotenzial und Schadenshöhen sowie in die Formulierung von Handlungsempfehlungen. Letztere richten sich insbesondere an die Zielgruppen, die im Fokus von Cyber-Angriffen stehen.

Da das Cyber-Abwehrzentrum sich als Informationsdrehscheibe versteht, steuert jede beteiligte Behörde Informationen bei und verwendet ihrerseits die konsolidierten und verdichteten Ergebnisse des Cyber-Abwehrzentrums im Rahmen der jeweiligen Zuständigkeiten. Die Optimierung dieses Input/Output-Verfahrens ist dabei ein stetiger Prozess. Der institutionalisierte Informationsaustausch und die Einbringung verschiedener Betrachtungsweisen eines IT-Sicherheitsvorfalls tragen dazu bei, dass aktuelle Erkenntnisse wesentlich schneller zu wirkungsvollen Präventiv- oder Gegenmaßnahmen führen.

Seit seiner Gründung wurden im Cyber-Abwehrzentrum rund 800 IT-Sicherheitsvorfälle bearbeitet. Die am Cyber-Abwehrzentrum beteiligten Behörden führen dazu eine regelmä-

ßige IT-Lagebeobachtung durch und geben ausgewählte, konkrete IT-Sicherheitsvorfälle zur Auswertung ins Cyber-Abwehrzentrum. Dort werden die technischen Hintergründe und Auswirkungen durch das BSI bewertet, nachrichtendienstliche Bezüge werden durch das Bundesamt für Verfassungsschutz eingebracht. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe bewertet den Vorfall hinsichtlich möglicher Auswirkungen auf Infrastrukturen. Im Bedarfsfall werden auch die assoziierten Behörden zur Lageeinschätzung hinzugezogen. Die im Cyber-Abwehrzentrum gewonnen Erkenntnisse fließen dann zurück an alle beteiligten Behörden und werden dort im Rahmen der jeweiligen Zuständigkeit genutzt, beispielsweise zur Umsetzung von Präventions-, Gegen- und Sensibilisierungsmaßnahmen.

Die wichtigsten Fälle

- PATRAS: Kompromittierung des von mehreren deutschen Behörden verwendeten GPS-basierten Zielverfolgungsystems PATRAS durch eine Hackergruppe.
- Duqu: Schadprogramm, das Informationen über SCADA-Systeme ausspioniert. Mögliche Verbindung zu Stuxnet-Urhebern. Vermutlich nachrichtendienstlicher Hintergrund.
- Gauss: Schadprogramm zur Ausspähung von Banktransaktionen. Vorkommen hauptsächlich in Ländern des Mittleren Ostens. Vermutlich nachrichtendienstlicher Hintergrund.
- Flame/Mini-Flame: Spionageprogramme, die hauptsächlich in Ländern des Mittleren Ostens auffällig wurden. Vermutlich nachrichtendienstlicher Hintergrund.
- Shamoon/Disttrack: Zerstörerisches Schadprogramm, das erfolgreich zur Sabotage der IT-Infrastruktur des saudischen Unternehmens Saudi Aramco, eines der größten Erdölförderunternehmen der Welt, eingesetzt wurde.
- Vielfache gezielte Angriffe auf Bundesbehörden mit unterschiedlicher thematischer Ausrichtung

Die Allianz für Cyber-Sicherheit: Mehr Schutz durch Kooperation

Dr. Hartmut Isselhorst,
Abteilungsleiter Cyber-Sicherheit

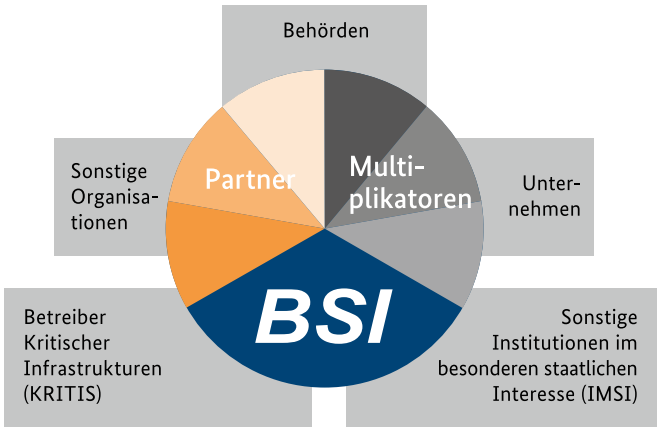
Die rasant voranschreitende Vernetzung von IT-Systemen über das Internet bietet beinahe täglich neue Möglichkeiten und Perspektiven sowohl für Privatanwender als auch für Organisationen, Unternehmen und Verwaltung. Annähernd jeder Lebens- und Wirtschaftsbereich ist heute Teil des Cyber-Raums. Diese Entwicklung fordert von allen Beteiligten eine stetige Auseinandersetzung mit dem unbestreitbar großen innovativen Potenzial einerseits – andererseits aber auch mit den Risiken und Sicherheitsmaßnahmen, die notwendig sind, um IT sicher und zuverlässig zu betreiben. Die Gründung der Allianz für Cyber-Sicherheit war in diesem Zusammenhang ein wichtiger Schritt.

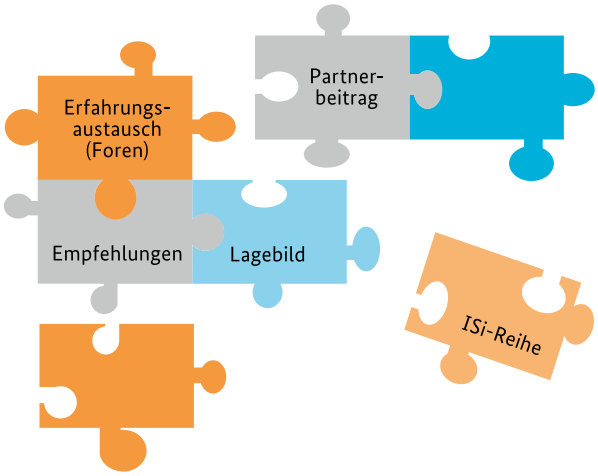
„Seit Beginn der Pilotphase im Mai und dem Start des öffentlichen Betriebs im Oktober 2012 konnten über 70 Partner und 24 Multiplikatoren gewonnen werden."

Die Angriffsmethoden im Cyber-Raum sind in den vergangenen Jahren immer professioneller geworden, die Zeitabstände, in denen der Modus Operandi eine neue Qualität erreicht, werden kürzer. Das Spektrum reicht dabei von Überlastangriffen (Denial-of-Service) durch Aktivisten und Erpresser über die Manipulation von Internet-Banking-Vorgängen durch Kriminelle bis hin zu Ausspähung und Sabotage durch fremde staatliche Stellen. Viele Angriffsziele können dabei relativ einfach attackiert und die Angriffswege effektiv verschleiert werden. Das Ausmaß der Bedrohung wird deutlich, wenn man die zahlreichen Cyber-Spionage-Angriffe auf deutsche Firmen oder die massiven Cyber-Sabotage-Angriffe auf US-Banken betrachtet.

Die Dynamik, mit der sich die Bedrohungslage entwickelt, zeigt, dass Institutionen aus dem privaten und öffentlichen Sektor dringend wirksame Strategien benötigen, um diesen Gefahren zu begegnen. Dazu gehören insbesondere praktikable Lösungen, Maßnahmen und Prozesse zum prä-

Die Allianz für Cyber-Sicherheit bietet bedarfsgerechte Informations- und Partizipationsmöglichkeiten





Teilnehmer
erhalten öffentliche Cyber-Sicherheits-Informationen.

Freiwillig Registrierte
erhalten zusätzlich aktuelle Informationen zur Cyber-Sicherheitslage, aktuelle Kurzmitteilungen, reglemäßige Newsletter und nicht öffentliche Informationen.

KRITIS und INSI
erhalten zusätzliche Warnmeldungen per E-Mail und vertrauliche Informationen.

Partner
erhalten die selben Informationen wie die Teilnehmer der Allianz für Cyber-Sicherheit.

erstellen kostenlose Partnerbeiträge für die Allianz für Cyber-Sicherheit, initiieren und leiten Erfahrungsaustausche.

Multiplikatoren
verbreiten die Informationen der Allianz für Cyber-Sicherheit an die Zielgruppen und unterstützen beim Erfahrungsaustausch.

Lagebild
Darstellungen zur aktuellen Sicherheitslage, z. B. BSI-Schwachstellenampel als Indikator für das momentane Gefährdungspotenzial gängiger Softwareprodukte aufgrund von bekannten Schwachstellen.

Empfehlungen
zur Cyber-Sicherheit (Auszug):
- sichere Nutzung von PCs unter Windows/Ubuntu,
- Einsatz sozialer Medien im Unternehmenskontext,
- sichere Bereitstellung von Web-Angeboten, zum Malware-Schutz und zur Handhabung von Schwachstellen.

Partnerbeiträge
Aktive Beiträge von Partnern, z. B. Gefährdungsberichte, Schwachstellenreports, Sicherheitshinweise.

Erfahrungsaustausch
Organisation der Teilnahme an regionalen und überregionalen Foren.

ISi-Reihe
Umfassende Informationen für Behörden und Wirtschaft zur Internet-Sicherheit, z. B. zur sicheren Anbindung lokaler Netze an das Internet unter Einsatz von IPv6.

ventiven Schutz und zur professionellen Reaktion auf Cyber-Angriffe. Aufgrund der geteilten Verantwortung für die Sicherheit der Netze und Systeme kann weder der Staat noch die Wirtschaft diese Aufgabe alleine bewältigen. Vielmehr ist eine koordinierte Zusammenarbeit aller Akteure in Verwaltung, Privatwirtschaft und Wissenschaft erforderlich.

Als Plattform für diese Zusammenarbeit in Deutschland haben der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) und das BSI im Rahmen der Umsetzung der Cyber-Sicherheitsstrategie der Bundesregierung die Allianz für Cyber-Sicherheit gegründet. Ziele dieser Allianz sind:

- die Risiken des Cyber-Raums für Deutschland zu bewerten und angemessene Sicherheitsmaßnahmen zu konzipieren und zu realisieren,
- die nationale Fähigkeit zum Schutz im Cyber-Raum, zur Abwehr von Cyber-Angriffen und zur Bewältigung von Cyber-Krisen zu stärken und
- im internationalen Vergleich eine führende Rolle im Bereich Cyber-Sicherheit einzunehmen.

Um diese Ziele zu erreichen, setzt die Allianz für Cyber-Sicherheit vor allem auf die Säulen Informationsverteilung und Erfahrungsaustausch. Wirksame Strategien zum Umgang mit entsprechenden Gefahren können nur erarbeitet werden, wenn die notwendigen Informationen über die Bedrohungslage, gängige Methoden der Täter sowie über Schutz- und Sofortmaßnahmen vorliegen. Die Allianz für Cyber-Sicherheit baut hierfür einen umfangreichen Informationspool auf, der überwiegend frei zugängliche Dokumente rund um das Thema Cyber-Sicherheit enthält und kontinuierlich aktualisiert wird. Darüber hinaus stehen auch nicht öffentliche Dokumente für freiwillig registrierte Teilnehmer zur Verfügung. Neben der zentra-

Prof. Dieter Kempf, Präsident des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM)

„In den letzten Monaten hat sich das Bewusstsein für IT-Sicherheit in Deutschland grundlegend verändert. Inzwischen ist jedem klar: Unternehmen müssen sich nicht nur gegen Cyber-Kriminelle wehren, sondern auch gegen die Ausspähung durch Geheimdienste anderer Staaten. Dabei spielt es für die Unternehmen letztlich keine Rolle, von wem oder woher die Cyber-Angriffe stammen. Sie müssen ihre eigenen Daten, die Daten ihrer Mitarbeiter und die Daten ihrer Kunden bestmöglich schützen. Mit der Allianz für Cyber-Sicherheit hat das BSI in enger Kooperation mit BITKOM und zahlreichen weiteren Organisationen eine Initiative gestartet, die den Unternehmen umfangreiche Informationen zum Thema IT-Sicherheit liefert sowie den Allianzpartnern zusätzlich eine Plattform für den Wissens- und Erfahrungsaustausch bietet. Unser gemeinsames Ziel ist aktueller denn je: die deutsche Wirtschaft widerstandsfähiger gegen Cyber-Angriffe zu machen. Das funktioniert nur, wenn Unternehmen sensibilisiert werden und dieses Bewusstsein in praktisches Handeln umsetzen. Daran werden wir auch im kommenden Jahr zusammen intensiv arbeiten."

len Bereitstellung von Informationen initiiert und unterstützt die Allianz auch den direkten Erfahrungsaustausch von Unternehmen, beispielsweise in branchenbezogenen Foren oder regionalen Stammtischen.

Über ein Formular auf der Website www.allianz-fuer-cybersicherheit.de können Institutionen außerdem freiwillig – gegebenenfalls anonym – Cyber-Sicherheitsangriffe, die sie festgestellt haben, an das BSI melden. Solche Meldungen sind wertvoll, um das Lagebild zu vervollständigen.

Die Dienstleistungen der Allianz für Cyber-Sicherheit erbringt das BSI nicht allein. Ansatz der Allianz ist die Kooperation, und so konnten seit Beginn der Pilotphase im Mai und dem Start des öffentlichen Betriebs im Oktober 2012 über 70 Partner und 24 Multiplikatoren gewonnen werden. Partner der Allianz können Institutionen werden, die durch aktive Beiträge die Cyber-Sicherheit in Deutschland gestalten, fördern und verbessern möchten, beispielsweise indem sie für die Teilnehmer Hintergrundinformationen aufbereiten oder kostenlose Beratungs- oder IT-Sicherheitsdienstleitungen anbieten.

Typische Multiplikatoren der Allianz sind Verbände, Gremien oder Medienunternehmen, die die Informationen der Allianz in die Fläche tragen und so dabei unterstützen, möglichst viele Institutionen zu erreichen. Alle Beiträge der Partner und Multiplikatoren sind für die Teilnehmer der Allianz für Cyber-Sicherheit kostenlos.

Durch die Teilnahme am Erfahrungsaustausch oder einen aktiven Beitrag im Rahmen der Allianz für Cyber-Sicherheit können Institutionen daran mitwirken, die Cyber-Sicherheit in Deutschland gemeinschaftlich zu verbessern und aktiv zu gestalten. Alle deutschen Unternehmen und Organisationen sind aufgerufen, sich an diesem Prozess als Teilnehmer, Partner oder Multiplikatoren zu beteiligen, um so das gemeinsame Ziel eines sicheren Cyber-Raums zu erreichen, der auch weiterhin fast täglich neue Möglichkeiten eröffnet.

Allianz für Cyber-Sicherheit

Web:
https://www.allianz-fuer-cybersicherheit.de

E-Mail:
info@cyber-allianz.de

Allianz für Cyber-Sicherheit

IT-Sicherheit gestalten – Mindeststandards setzen

Sicherheit für intelligente Netze:
Das Smart Meter Gateway

Dennis Laupichler,
Leiter der Projektgruppe Energiewirtschaftsgesetz
und Smart Metering Systems

Angesichts knapper werdender Rohstoffe und der damit zunehmenden Bedeutung erneuerbarer Energien ist die Energieversorgung in Deutschland und europaweit im Wandel. Quellen wie Sonne und Windkraft lassen sich nicht planen oder steuern wie Kohle- oder Kernkraftwerke. Darüber hinaus führt die zunehmende Zahl dezentraler Erzeuger, wie z. B. Photovoltaik-Anlagen, zu schwer vorhersehbaren Schwankungen und erheblichen Herausforderungen bei der Stabilität im Stromnetz. Da elektrische Energie nur begrenzt gespeichert werden kann, steht die Energieversorgung vor einem Paradigmenwechsel: War es bisher üblich, genauso viel Strom zu erzeugen wie verbraucht wurde, so soll zukünftig möglichst dann Energie konsumiert werden, wenn diese zur Verfügung steht. Basis einer solchen Energieversorgung ist ein intelligentes Netz, das Energieerzeugung und -verbrauch effizient verknüpft und ausbalanciert. Kernbausteine eines solchen Netzes sind intelligente Messsysteme, auch „Smart Metering Systems“ genannt. Sie sollen für eine aktuelle Verbrauchstransparenz und die sichere Übermittlung von Messdaten sorgen sowie elektronische Verbrauchsgeräte und Erzeugungsanlagen so steuern, dass eine bessere Lastverteilung im Netz ermöglicht wird.

Da es beim Aufbau und der Nutzung eines intelligenten Netzes nicht zuletzt auch um die Verarbeitung personenbezogener Daten geht, sind die Sicherheit und der Schutz eben jener eine zentrale Voraussetzung für die öffentliche Akzeptanz intelligenter Messsysteme. Die zukünftigen Energieversorgungssysteme, insbesondere die dafür verwendeten intelligenten Messsysteme, erfordern somit verbindliche und einheitliche sicherheitstechnische Vorgaben und funktionale Anforderungen. Das BSI entwickelt daher Schutzprofile nach Common Criteria (CC – Allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologie) sowie Technische Richtlinien, die eine international vergleichbare Sicherheitszertifizierung der entsprechenden Geräte ermöglichen. Hierdurch nimmt Deutschland bei der Umsetzung von intelligenten Messsystemen in Europa eine Vorreiterrolle ein.

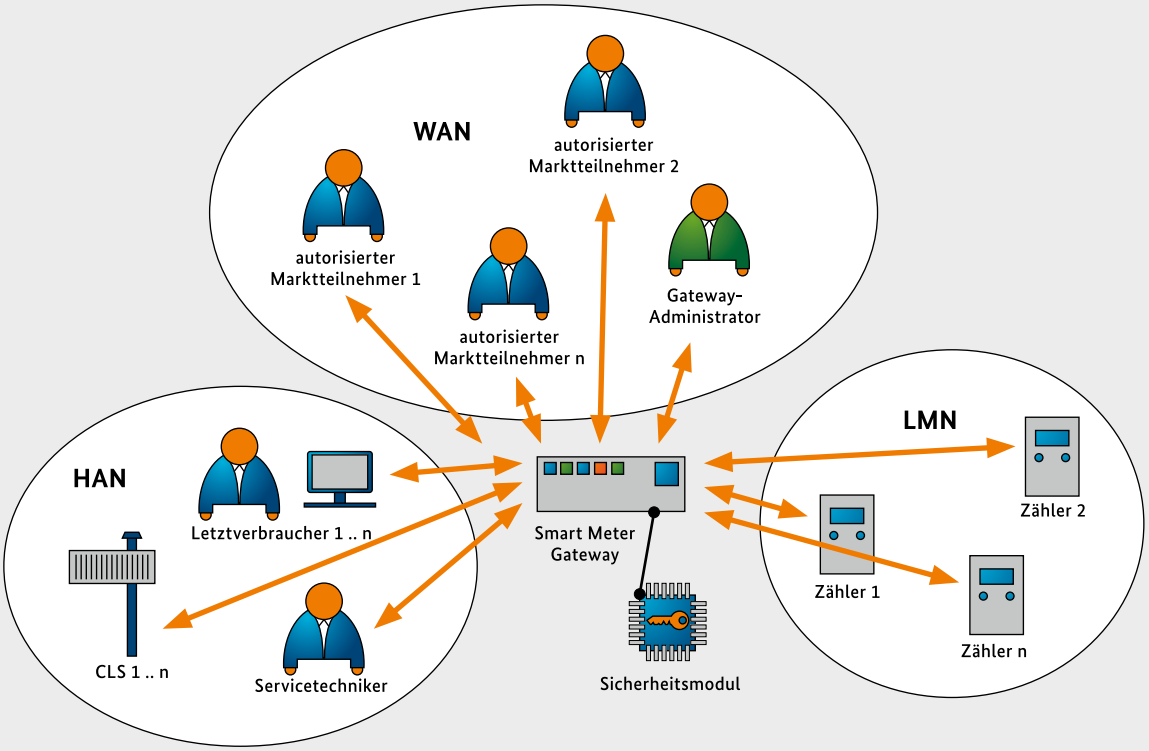
Schutzprofil und Technische Richtlinie

Aufgrund der Verarbeitung und Zusammenführung personenbezogener Daten sowie möglicher negativer Rückwirkungen auf die Energieversorgung ergeben sich wie bereits erwähnt hohe Anforderungen an den Datenschutz und die IT-Sicherheit von intelligenten Messsystemen. Vor diesem Hintergrund wurde das BSI im September 2010 vom Bundeswirtschaftsministerium beauftragt, ein Schutzprofil (Protection Profile, PP) sowie daran anschließend eine Technische Richtlinie (TR) für die Kommunikationseinheit eines intelligenten Messsystems (Smart Meter Gateway) zu erarbeiten, um einen einheitlichen technischen Sicherheitsstandard für alle Marktakteure zu gewährleisten.

Ein Schutzprofil zeigt strukturiert Bedrohungen für den sicheren und datenschutzfreundlichen Betrieb auf und legt die Mindestanforderungen für entsprechende Sicherheitsmaßnahmen fest. Auf Basis des Schutzprofils können dann Produkte getestet werden, die nach einer positiven Prüfung ein Zertifikat erhalten und somit nachweislich das Schutzziel erfüllen. Zugleich lässt das Schutzprofil dem Hersteller aber auch Spielraum bei der technischen Ausgestaltung der Sicherheitsanforderungen. Dies ermöglicht selbst bei unterschiedlicher Ausführung einen einheitlich hohen Sicherheitsstandard und gewährleistet im Fall neuer technischer Möglichkeiten eine kontinuierliche Innovation der Produkte. Die Sicherheitsanforderungen im Schutzprofil sind somit technologieunab-

Das Smart Meter Gateway und seine Umgebung

Im WAN kommuniziert das SMGW mit den externen Marktteilnehmern und insbesondere auch mit dem SMGW-Administrator. Im LMN kommuniziert das SMGW mit den angebundenen Zählern (Strom, Gas, Wasser, Wärme) eines oder mehrerer Letztverbraucher. Die Zähler kommunizieren ihre Messwerte über das LMN an das SMGW. Im HAN des Letztverbrauchers kommuniziert das SMGW mit den steuerbaren Energieverbrauchern beziehungsweise Energieerzeugern (Controllable Local Systems, CLS, also etwa intelligente Haushaltsgeräte, Kraft-Wärme-Kopplungs- oder Photovoltaik-Anlagen). Des Weiteren stellt das SMGW Daten für den Letztverbraucher beziehungsweise für den Service-Techniker im HAN bereit.



hängig und beziehen sich im Wesentlichen auf Aspekte, die durch Datenschutz, d.h. die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und Datensicherheit, also insbesondere die Vertraulichkeit, Integrität und Authentizität, motiviert sind. Darüber hinaus sind zur Gewährleistung der Interoperabilität der verschiedenen in einem intelligenten Messsystem vorhandenen Komponenten jedoch auch rein funktionale Vorgaben zu erarbeiten und die im Schutzprofil getroffenen Sicherheitsanforderungen näher auszugestalten. Diese zusätzlichen Aspekte finden sich in der Technischen Richtlinie (BSI TR-03109) wieder.

Bund und Wirtschaft erarbeiten Sicherheitsstandards gemeinsam

Sicherheitsstandards können nur dann erfolgreich sein, wenn sie auf breite Akzeptanz bei Herstellern und Anwendern stoßen. Daher hat das BSI diese von Anfang an in die Erstellung und Weiterentwicklung von Schutzprofil und Technischer Richtlinie eingebunden. In mehreren Kommentierungsrunden konnten Verbände aus den Bereichen Telekommunikation, Energie, Informationstechnik, Wohnungswirtschaft und Verbraucherschutz umfangreich und maßgeblich an beiden Dokumenten

mitwirken. Insgesamt hat das BSI etwa 1.200 Kommentare zum Schutzprofil und mehr als 3.100 Kommentare zur Technischen Richtlinie verzeichnet. Diese Zahlen belegen das hohe Interesse, das dem Thema in Fachkreisen und zunehmend auch in der Politik beigemessen wird.

Smart Meter Gateway: Dreh- und Angelpunkt des Messsystems

In einem intelligenten Messsystem bildet die Kommunikationseinheit, das Smart Meter Gateway (SMGW), die zentrale Komponente, die Messdaten von Zählern empfängt, speichert und diese für Marktakteure aufbereitet. Das SMGW kommuniziert dabei zur Verbrauchsdatenübertragung wie auch zu seiner Administration mit verschiedenen Komponenten und beteiligten Marktakteuren (siehe Grafik).

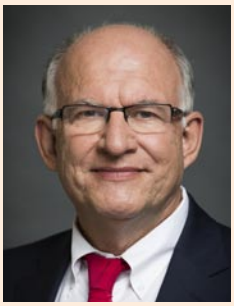
Durch seine zentrale Aufgabe des Empfangs, der Verarbeitung und des Versands der Messdaten werden besondere Anforderungen hinsichtlich der Sicherheit an das SMGW gestellt. Deswegen werden die Kommunikationsflüsse zwischen dem SMGW sowie den übrigen Komponenten und beteiligten Marktakteuren verschlüsselt und somit in Bezug auf Integrität, Authentizität und Vertraulichkeit abgesichert. Das SMGW bedient sich hierzu eines sog. Sicherheitsmoduls, das zum einen als sicherer Speicher für das zur Verschlüsselung erforderliche kryptographische Schlüsselmaterial dient. Zum anderen stellt es die kryptographischen Kernroutinen für Signaturerstellung und -prüfung, Schlüsselgenerierung, Schlüsselaushandlung sowie Zufallszahlengenerierung für das SMGW bereit.

Abgeleitet von der Systemarchitektur muss ein SMGW darüber hinaus drei physikalische Schnittstellen bereitstellen: Jeweils eine für das Weitverkehrsnetz (Wide Area Network, WAN), das Lokale Metrologische Netz (Local Metrological Network, LMN) sowie das Heimnetz (Home Area Network, HAN).

Um an diesen Schnittstellen vielfältige Anwendungszwecke abdecken zu können, müssen zunächst die notwendigen Kommunikationsprotokolle verbindlich und einheitlich festgelegt werden. Damit kann ein SMGW unabhängig von den zugrunde liegenden Hard- und Software-Eigenschaften auch mit Komponenten anderer Hersteller interagieren. So ist im Falle eines Zählerwechsels oder beim Tausch eines steuerbaren Geräts gewährleistet, dass das SMGW weiterhin verwendet werden kann.

Schutz der Privatsphäre („by design“)

Bei der Entwicklung des Schutzprofils und der Technischen Richtlinie werden neben der Datensicherheit auch Datenschutzanforderungen für das Smart Meter Gateway berücksichtigt. Dies ist notwendig, um das Erzeugen von detaillierten Nutzerprofilen und das damit einhergehende große Ausforschungspotenzial in Bezug auf die Lebensgewohnheiten des Endkunden zu verhindern. Hierzu können Auswertungsprofile im SMGW so gestaltet werden, dass für verschiedene dezentral abgebildete Tarifprofile nur die notwendigen, abrechnungsrelevanten Verbräuche zur Verfügung gestellt werden. Dadurch wird die geforderte Datenvermeidung und notwendige Datensparsamkeit erreicht. Das sog. Tarifierungskonzept



Peter Schaar,
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

„Die Einführung intelligenter Messsysteme muss von der Schaffung verbindlicher Standards für den technischen Datenschutz sowie die IT-Sicherheit begleitet werden. Daher ist es positiv, dass ich als Bundesbeauftragter für den Datenschutz und die Informationsfreiheit bereits frühzeitig an der Entwicklung der Schutzprofile und Technischen Richtlinien zu Smart Meter beteiligt wurde. So konnten meine Mitarbeiterinnen und Mitarbeiter von Anfang an darauf hinwirken, dass die Anforderungen des Datenschutzes und der Datensicherheit angemessen berücksichtigt werden. Die entsprechenden Vorschläge wurden vom Bundesamt für Sicherheit in der Informationstechnik und vom Bundesministerium für Wirtschaft und Technologie aufgegriffen. Datenschutz und Datensicherheit können dazu beitragen, dass der für die Energiewende bedeutsame Einsatz von Smart Meters von den Betroffenen akzeptiert wird. Die dabei erhobenen detaillierten Daten über den Energieverbrauch sind hoch sensibel, lassen sich aus ihnen doch tiefgreifende Erkenntnisse über die individuellen Lebensgewohnheiten gewinnen.“

der Technischen Richtlinie definiert hierzu die möglichen Operationen und Parameter, die für die verschiedenen Anwendungszwecke herangezogen werden können. Das SMGW sorgt zudem bei einer Auswertung von Netzstatusdaten dafür, dass nur pseudonymisierte Daten an externe Marktakteure wie z. B. den Netzbetreiber versendet werden. In Fällen besonderer Zweckbindung können bestimmte Netzzustandsdaten mit Zähler-Bezug versendet werden.

Gesetzliche Einbauverpflichtungen

Das Energiewirtschaftsgesetz (EnWG) vom 21. Februar 2013 enthält neben umfangreichen Vorgaben zum bereichsspezifischen Datenschutz auch eine Kernvorschrift (§ 21e), in der für bestimmte Fälle ein verpflichtender Einbau eines zertifizierten Messsystems vorgeschrieben ist. Für den Einbau des Messsystems ist jedoch nicht der private Verbraucher, sondern der zuständige Messstellenbetreiber verantwortlich. Messstellenbetreiber werden demnach verpflichtet, bei Gebäuden, die neu an das Energieversorgungsnetz angeschlossen oder einer größeren Renovierung unterzogen werden, sowie bei Kunden mit einem Jahresverbrauch von mehr als 6.000 Kilowattstunden zertifizierte Messsysteme zu verbauen. Des Weiteren müssen nach dem Erneuerbare-Energien-Gesetz (EEG) oder Kraft-Wärme-Kopplungsgesetz (KWKG) die Betreiber neu errichteter Energien-Anlagen bei einer installierten Leistung von mehr als 7 Kilowatt zertifizierte Messsysteme verbauen.

Intelligente Steuerung führt zu Einsparungen

Intelligente Messsysteme können besonders bei den verbrauchsstarken Gruppen (Haushalte und Gewerbe) ihren Nutzen entfalten, da Energieeinspar- wie auch -verlagerungspotenziale in stärkerem Maße vorhanden sind als bei verbrauchsschwachen Gruppen. Für weitere Pflichteinbaufälle hat das Bundeswirtschaftsministerium eine Kosten-Nutzen-Analyse erstellen lassen. Insbesondere im Einspeise- und Lastmanagement wird ein hohes Potenzial von Smart Metering festgestellt, sodass eine Erweiterung der Pflichteinbaufälle auf alle EEG- und KWK-Alt- und Neuanlagen größer als 0,25 Kilowatt empfohlen wird. Durch eine Steuerung von dezentralen Lasten und Erzeugern über intelligente Messsysteme können im Gegenzug Einsparungen beim Netzausbau in den Verteilernetzen erzielt werden. Bis 2022 könnte nach Prognose der Kosten-Nutzen-Analyse ein Roll-out von 11,9 Mio. intelligenten Messsystemen erreicht werden.

Zertifizierung durch das BSI

Um sicherzustellen, dass ein Smart Meter Gateway den gesetzlichen Vorgaben an Sicherheit und Interoperabilität genügt, muss es sowohl nach Schutzprofil als auch nach Technischer Richtlinie durch das BSI zertifiziert werden. Des Weiteren bedarf es aufgrund des Eichrechts einer Zulassung durch die Physikalisch-Technische Bundesanstalt (PTB). Bei der Entwicklung des Schutzprofils und der Technischen Richtlinie wurde darauf geachtet, dass möglichst viele eichrechtlichen Anforderungen der PTB in die Dokumente des BSI einfließen, um Mehraufwände und Doppelprüfungen im Zertifizierungs- und Zulassungsprozess zu vermeiden und Synergieeffekte zu erzielen.

Der Referentenentwurf zur Verordnung über technische Mindestanforderungen an den Einsatz intelligenter Messsysteme (Messsystemverordnung – MsysV) nach § 21i EnWG hat am 23. September 2013 gemeinsam mit dem Schutzprofil SMGW (V1.2) inklusive Sicherheitsmodul (V1.0) und Technischer Richtlinie 03109 (V1.0) erfolgreich das europäische Notifizierungsverfahren durchlaufen. Gemäß der EU-Richtlinie 98/34/EG sind die Mitgliedstaaten dazu verpflichtet, der EU-Kommission die Entwürfe nationaler technischer Vorschriften mitzuteilen, um Handelshemmnisse rechtzeitig zu erkennen und zu verhindern. Für eine Verabschiedung im nationalen Rechtsetzungsverfahren ist nun nach einem Kabinettbeschluss noch die Zustimmung des Bundestages und des Bundesrates erforderlich. Darüber hinaus wird die Technische Richtlinie systematisch weiterentwickelt, um Rückflüsse aus den Entwicklungsarbeiten bei den Herstellern sowie den Zertifizierungsverfahren aufzunehmen. Hierbei werden Pilotprojekte und Testregionen wertvolle Informationen liefern.

Das BSI hat auf seiner Website einen Themenschwerpunkt „Smart Metering Systems“ eingerichtet. Dort sind neben Hintergrundinformationen auch Informationen zu Schutzprofil und Technischer Richtlinie abrufbar.

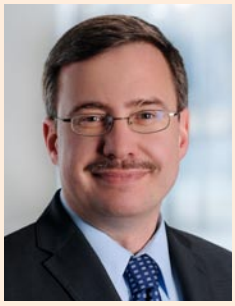
Web:
www.bsi.bund.de/SmartMeter

Zertifizierte Sicherheit für unsere Gesellschaft auf dem Daten-Highway

Joachim Weber,
Fachbereichsleiter
Zertifizierung und Standardisierung

Die Informationstechnik hat längst alle gesellschaftlichen Bereiche erfasst und ist weltweit ein selbstverständlicher, teilweise unsichtbarer Bestandteil des Alltags geworden. Immer mehr Aufgaben werden von immer schnelleren, komplexeren, weltweit vernetzten informationstechnischen Systemen übernommen. Die Funktionsweise von IT-Produkten, -Systemen und -Anwendungen ist für die meisten Nutzer jedoch ohne fundiertes Fachwissen nicht immer durchschaubar.

Gerade deshalb ist es wichtig, dass die Anwender Vertrauen in die IT haben können, von der so viele Lebens- und Arbeitsbereiche abhängig sind. Vertrauen kann aber nur dann entstehen, wenn man sich auf die IT-Produkte und -Anwendungen verlassen kann. Das gilt vor allem für die Sicherheit von Daten im Hinblick auf Vertraulichkeit, Verfügbarkeit und Integrität.



Thomas Rosteck,
Vize President und General Manager für Division Chip Card und Security, Infineon Technologies

„Für die Vermarktung von Infineons Sicherheitsprodukten im Chipkarten- und Embedded-Security-Bereich ist in vielen Fällen die Sicherheitszertifizierung nach Common Criteria eine notwendige Anforderung der Kunden. Die deutschen Sicherheitszertifikate werden wegen der hohen Kompetenz des BSI insbesondere bei Government-ID-Produkten, Bank- und Kreditkarten, aber auch zunehmend für in Geräte eingebaute Sicherheitschips weltweit sehr geschätzt und helfen, Sicherheitsniveaus international vergleichbar zu machen. Als Marktführer für Sicherheitschips seit über 15 Jahren kann Infineon so das hohe Sicherheitsniveau seiner Produkte nachweisen und deutsche Sicherheitslösungen im internationalen Wettbewerb platzieren."

Um einen sicheren Umgang mit Daten und informationsverarbeitenden Systemen zu gewährleisten, ist es erforderlich, Sicherheitsstandards zu entwickeln und einzuhalten – aktuell und konkret angepasst an den jeweiligen Grad der Gefährdung. Das BSI mit seinem auf gesetzlicher Grundlage verankerten Bereich der IT-Sicherheitszertifizierung überprüft als fachlich anerkannte und neutrale Stelle die Sicherheit von Informationstechnologie. Durch seine Zertifikate und Prüfsiegel trägt das BSI einen wesentlichen Teil dazu bei, das nötige Vertrauen in die IT zu schaffen.

Die IT-Sicherheitszertifizierung des BSI wendet sich mit ihrem Angebot an die Anwender und Hersteller von Informationstechnik. Zielgruppen sind neben den öffentlichen Verwaltungen von Bund, Ländern und Kommunen auch private Nutzer und Unternehmen. Das BSI übernimmt hier die Aufgabe, Zertifizierungen von IT-Produkten und -Systemen durchzuführen und im Vor-

feld die dafür benötigten Prüfkriterien und technischen Grundlagen zu entwickeln. Neben diesen Kriterien sind auch ein darauf aufbauendes Verfahren zur Durchführung von Zertifizierungen sowie qualifizierte Prüfstellen oder Auditoren Grundlage für die Erteilung eines Zertifikats. Ihre fachliche Kompetenz weisen diese über eine vom BSI ausgestellte Bescheinigung beziehungsweise eine Anerkennung für ihr Prüfgebiet aus.

Durchschnittlich fünf Zertifikate pro Woche

In folgenden Dienstleistungsbereichen hat das BSI 2012 IT-Sicherheitszertifizierungen durchgeführt:

Art der Zertifizierung	Anzahl der erstellten Zertifikate in 2012
Zertifizierung von Produkten nach den Common Criteria	88
Zertifizierung von Produkten nach Technischen Richtlinien des BSI (Konformitätsprüfung)	38
Zertifizierung von Systemen nach ISO 27001 auf der Basis von IT-Grundschutz	20
Anerkennung von Prüfstellen	16
Zertifizierung von IT-Sicherheitsdienstleistern	6
Zertifizierung und Anerkennung von Personen	100

Die Bandbreite der vom BSI zertifizierten Produkte und Angebote ist dabei sehr hoch. Derzeit befindet sich eine Reihe von Produkten aus vielfältigen Technikbereichen in der Zertifizierung, beispielsweise Firewalls, Mailserver, Datenbankserver, Smartcard-Controller, Signaturkarten, Gesundheitskarten, biometrische Verifikationssysteme, Betriebssysteme und Chipkarten-Lesegeräte.

Diese zertifizierten Produkte finden sich in vielen Bereichen des täglichen Lebens wieder. So hat beispielsweise jeder neuere deutsche Reisepass oder Personalausweis einen zertifizierten Sicherheitschip. Auch die Gesundheitskarte mit der dahinter stehenden Sicherheitsinfrastruktur ist vom BSI zertifiziert. Das gilt ebenfalls für die Anbieter von Dienstleistungen im Umfeld der vor Kurzem eingeführten De-Mail.

Glossar

Zertifizierung von Personen:
Verfahren zur Prüfung und Bewertung von Personen zum Nachweis der Einhaltung bestimmter Anforderungen. Zur Zertifizierung müssen diese Personen im Rahmen einer Kompetenzfeststellung ihre Fachkompetenz nachweisen (Auditoren, Revisoren und Berater, Penetrationstester etc.)

Zertifizierung von Produkten und Systemen:
Verfahren zur Prüfung und Bewertung von Produkten oder Systemen zum Nachweis der Einhaltung bestimmter Kriterien (Common Criteria, Technische Richtlinien, ISO27701 auf der Basis von IT-Grundschutz) mit der Erteilung eines Zertifikats.

Zertifizierung von Stellen:
Verfahren zur Prüfung und Bewertung einer Stelle, die eine spezielle Prüfung oder Konformitätsbewertung durchführen kann. Das BSI zertifiziert IT-Sicherheitsdienstleister (Penetrationstester, Revisoren und Berater) sowie Prüfstellen für die BDBOS (Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben), ohne dass die Prüfergebnisse der Stellen durch ein Sicherheitszertifikat des BSI bestätigt werden.

Zertifizierung von IT-Sicherheitsdienstleistungen:
Verfahren zur Prüfung und Bewertung einer Dienstleistung eines Anbieters (De-Mail-Provider, Web-Services, Cloud-Services).

Anerkennung von Stellen: Verfahren zur Kompetenzfeststellung von Stellen, die für die Zertifizierungsstelle(n) des BSI Produktprüfungen mit dem Ziel einer Sicherheitszertifizierung durchführen.

Bestätigung: Ergebnisbericht einer Evaluierung von Produkten oder Sicherheitskonzepten für akkreditierte Zertifizierungsdiensteanbieter (ZDA) zur Ausführung von qualifizierten Signaturen.

Achim Hildebrandt,
Referatsleiter Pass- und Ausweiswesen; Identifizierungssysteme, Bundesministerium des Innern

Die Einführung des neuen Personalausweises zum 1. November 2010 war mit dem Ziel verbunden, den bisherigen Personalausweis durch ein Dokument abzulösen, das auch den Anforderungen der digitalen Welt gerecht wird. Über zwei Jahre nach der Erstausgabe ist der neue Personalausweis im Leben der Bürger angekommen. Das handliche Scheckkartenformat sowie seine gleichermaßen ansprechende wie fälschungssichere Gestaltung sind beliebt: Fast 20 Millionen Bürger haben sich den neuen Personalausweis bereits ausstellen lassen.

Der neue Personalausweis – 20 Millionen Nutzer in zwei Jahren

Die Nachfrage ist damit höher als die reguläre Auswechselquote nach Ablauf der zehnjährigen Ausweisgültigkeit. Für den gestiegenen Preis, der die Produktionskosten auch der neuen elektronischen Funktionen und die Verwaltungskosten der Kommunen erstmals realistisch abbildet, gibt es zumeist Verständnis. Der neue Personalausweis gilt weltweit als fälschungssicherstes Ausweisdokument und das Interesse an seinen neuen Funktionen wächst – national ebenso wie international.

Der Personalausweis bietet dabei drei neue Funktionen, die auf freiwilliger Basis von den Bürgern genutzt werden können. Sie können erstens zusätzlich zum biometrischen Lichtbild ihre Fingerabdrücke als biometrisches Merkmal speichern lassen. Damit lehnt sich der Personalausweis an die EU-Regelungen für Pässe an. Sie können zweitens die Online-Ausweisfunktion eingeschaltet lassen, die es ihnen ermöglicht, sich und ihr Gegenüber im Internet sowie an Terminals und Automaten sicher und eindeutig zu identifizieren. Drittens können in naher Zukunft digitale Dokumente mit der Unterschriftsfunktion rechtsverbindlich unterzeichnet werden.

Anwendungen schaffen – Marktpotenzial nutzen

Die Nutzung der elektronischen Online-Ausweisfunktion ist stark abhängig von den Angeboten, die den Bürgern in ihrer Kommune oder von Seiten der Wirtschaft zur Verfügung stehen. Sie wird von den Anwendern besonders häufig dort angeschaltet, wo Kommunen und Länder selbst den elektronischen Identitätsnachweis für ihre Bürgerdienste im Internet anbieten. In einigen dieser Kommunen liegt die Quote derjenigen, die die Online-Ausweisfunktion aktiviert lassen, bei über 70 Prozent. In anderen Personalausweisbehörden liegt diese Quote leider noch im einstelligen Bereich. Im Durchschnitt haben etwa 30 Prozent der Ausweisinhaber in Deutschland die Online-Ausweisfunktion aktiviert. Schon dies bedeutet ein beträchtliches Potenzial für Verwaltung und Wirtschaft im Internet, das andere Karten kaum erreichen.

Web:
www.personalausweisportal.de

Es gibt zahlreiche Anbieter von Hard- und Software für die elektronische Identitätsfunktion des Ausweises; was fehlt, sind jedoch alltägliche Anwendungsangebote im Internet. Hier ist die Wirtschaft aufgerufen, die mit der eID gegebene höhere Sicherheit und das vorhandene Marktpotenzial deutlich stärker zu nutzen. Es geht um die Bereitstellung von attraktiven alltagstauglichen Angeboten. Wie das gehen kann, zeigen Unternehmen, die ihren Kunden neue Services auf Basis der Online-Ausweisfunktion bieten: z. B. SCHUFA-Auskünfte oder der elektronische Lohnstreifen für zweieinhalb Millionen mittelständische Unternehmen mit mehr als elf Millionen Arbeitnehmerinnen und Arbeitnehmern im Lohn- und Gehaltsportal der DATEV e. G. Sieben große Versicherungen bündeln für ihre Kunden ihre Dienstleistungen im Netz fast vollständig online. Die Registrierung und den Zugang zu De-Mail mit der Online-Ausweisfunktion stellen die De-Mail-Anbieter im Netz zur Verfügung.

Digitales Bürgeramt

Der Staat geht mit guten Beispielen voran, etwa im Rahmen des E-Government-Gesetzes und der vom Bundesministerium des Innern initiierten E-Government-Initiative. Durch neue Angebote bei der Online-Ausweisfunktion können die Bürger Verwaltungsangelegenheiten bequem und ohne Wartezeiten von zu Hause aus erledigen.

So bieten Städte wie Ingolstadt, Würzburg, Münster, Hagen oder Aachen ihren Einwohnern rund um die Uhr die Beantragung von Melderegister- und Gewerberegisterauskünften sowie weitere Verwaltungsverfahren online an. Die Deutsche Rentenversicherung ermöglicht mit dem E-Service jederzeit den Zugriff aufs Rentenkonto. Künftig können überall auch Führungszeugnisse online beantragt werden. Das Interesse von Behörden und Unternehmen an einer Integration der Online-Ausweisfunktion in ihre Dienstleistungen wuchs 2012 deutlich schneller als zuvor. Das liegt auch daran, dass die Bundesländer zunehmend die rechtlichen Rahmenbedingungen für zentrale Zertifikate schaffen, sodass ihre Kommunen Bürgerservice-Portale mit integrierter eID-Funktion nutzen und einbinden können. Dadurch realisieren sie medienbruchfreies E-Government ohne eigene Investitionen in Entwicklungen, Zertifikate und eID-Server. Baden-Württemberg, Bayern, und Rheinland-Pfalz bieten bereits Portallösungen an, weitere Länder wie Niedersachsen und Nordrhein-Westfalen kommen in Kürze hinzu.

Neuer Ausweis – neue Möglichkeiten

Die Möglichkeiten des neuen Personalausweises sind unbestritten und sie werden immer besser angenommen. Er genießt gerade auch deshalb ebenso wie der Elektronische Reisepass national und international ein großes Ansehen. Die Mechanismen, die den Chip in den Ausweisdokumenten – und damit die persönlichen Daten der Bürger – vor Fälschung und Missbrauch schützen, hat das BSI entwickelt. Auf diesem Erfolg werden wir aufbauen und weitere benutzerfreundliche, alltagstaugliche Einsatzmöglichkeiten der eID-Funktion des Personalausweises für Bürgerinnen und Bürger entwickeln. Ein aktuelles Schlüsselthema ist die Integration von Hard- und Software für die Online-Ausweisfunktion in Smartphones und mobile Geräte sowie in Automaten und Terminals. Das BSI, das Fraunhofer Institut für Offene Kommunikationssysteme und andere Partner wie die Bundesdruckerei sind hier mit mittelfristigen Projekten auf dem Weg zu den benötigten Lösungen.

Ingrid Grüning,
Referentin für Sicherheit in eID-Anwendungen

De-Mail:
Sicherheitsanker in der Kommunikation

Gemäß einer Erhebung des Statistischen Bundesamts verfügten 2011 über Dreiviertel aller Haushalte und mehr als 80 Prozent der Unternehmen über einen Online-Zugang. Auch ein Großteil der Kommunikation im privaten wie im geschäftlichen Bereich läuft über das Internet, beispielsweise über Chats, Foren, soziale Netzwerke und E-Mails. Die herkömmliche E-Mail hat jedoch trotz ihrer großen Verbreitung und ihrer Akzeptanz in der Bevölkerung als Kommunikationsmittel auch Schwächen, vor allem unter sicherheitstechnischen Gesichtspunkten. Sie ist vergleichbar mit einer Postkarte: Die versendeten Informationen liegen mehr oder weniger offen, Unbefugte können jederzeit mitlesen. Zudem kann nicht überprüft werden, ob der Empfänger die Nachricht tatsächlich erhalten hat. Zum Versand privater und vertraulicher Informationen ist die E-Mail also nur bedingt geeignet.

Abhilfe schafft hier die De-Mail, deren Konzept sich speziell an den Bedürfnissen der Anwender nach Sicherheit und Zuverlässigkeit orientiert. Dieser Anspruch wird u. a. dadurch erfüllt, dass De-Mail architektonisch auf einem geschlossenen Kommunikationsverbund basiert, in dem nur vom BSI akkreditierte Diensteanbieter zugelassen sind. Diese müssen zuvor umfangreiche Prüfprozesse auf Basis von Technischen Richtlinien des BSI sowie der Datenschutzkriterien des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) absolvieren.

De-Mail hat nicht den Anspruch, die herkömmliche E-Mail zu ersetzen. Vielmehr eröffnet die Technologie neue Möglichkeiten für ausgewählte Einsatzzwecke, um die klassischen Vorteile der E-Mail als schnelles und unkompliziertes Medium mit einem hohen Anspruch an Sicherheit, Vertraulichkeit und Unverfälschbarkeit zu verbinden.

Gesetzliche Basis zur sicheren Kommunikation

Die „Grundsteinlegung“ für die Markteinführung von De-Mail erfolgte im Mai 2011 mit Inkrafttreten des „Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften“ (De-Mail-Gesetz). Das Gesetz bildet in Verbindung mit der „Technischen Richtlinie 01201 De-Mail“ des BSI die Basis für die Entwicklung und Umsetzung entsprechender Dienste durch interessierte Unternehmen. Als zuständige Behörde unterstützt das BSI seither die potenziellen Anbieter auf ihrem Weg durch den vielschichtigen Akkreditierungsprozess, in dessen Verlauf sie beweisen müssen, den hohen Anforderungen der Technischen Richtlinie und des De-Mail-Gesetzes gerecht werden zu können. Hierzu zählt das Erbringen von Testaten in den Bereichen Funktionalität, Interoperabilität und IT-Sicherheit, in die die Ergebnisse von obligatorischen Penetrationstests und einer Informationssicherheitsrevision (IS-Revision) einfließen. Zusätzlich erforderlich ist ein Zertifikat des Bundesdatenschutzbeauftragten. Weiterhin sind die Zuverlässigkeit und Fachkunde des Personals sowie die Erfüllung der gesetzlich geregelten Deckungsvorsorge nachzuweisen.

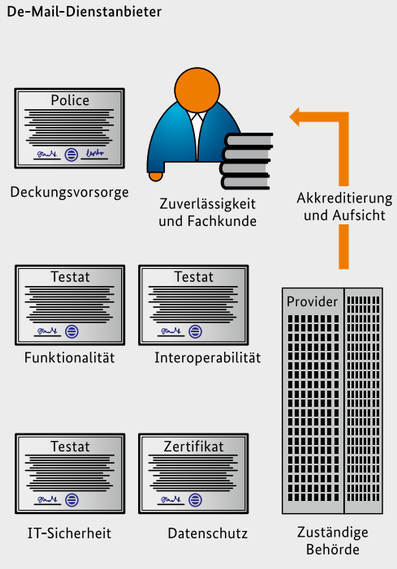
Sind alle Anforderungen erfüllt, erteilt das BSI nach Sichtung und Prüfung der eingereichten Unterlagen und Nachweise die Akkreditierung als Voraussetzung für die Aufnahme des Unternehmens als De-Mail-Diensteanbieter am Markt.

Seit Frühjahr 2012 haben bereits drei Diensteanbieter diesen Prozess erfolgreich durchlaufen und bieten sowohl Privatpersonen als auch Wirtschaft und Verwaltung ihren Service an. Weitere potenzielle Anbieter sind bereits in den Akkreditierungsprozess eingestiegen. Die jeweils aktuelle Liste der zugelassenen Unternehmen wird unter www.bsi.bund.de veröffentlicht.

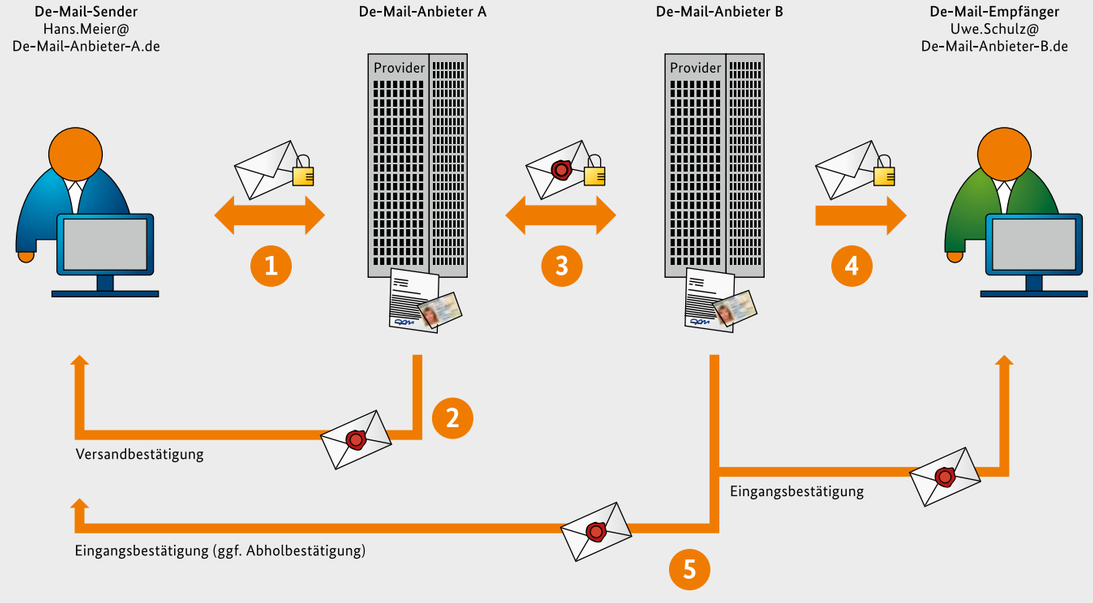
Einfache Handhabung, hohe Sicherheit

Im Bereich Sicherheit bietet De-Mail einige Vorteile gegenüber der normalen E-Mail. So können sowohl die Identität der Kommunikationspartner als auch Versand und Eingang von De-Mails jederzeit zweifelsfrei nachgewiesen werden. Die Inhalte können auf ihrem Weg durch das Internet nicht mitgelesen oder gar verändert werden.

Das BSI ist zuständig für die Akkreditierung der Anbieter von De-Mail-Diensten



Versand und Empfang erfolgen nur innerhalb des De-Mail-Verbundes



Denn abgesicherte Anmeldeverfahren und Verbindungen zu den Anbietern sorgen ebenso wie verschlüsselte Transportwege für einen vertraulichen Versand und Empfang der Nachrichten. Neben diesen sicherheitstechnischen Vorteilen bietet De-Mail für den Anwender noch weitere attraktive Nutzungsoptionen – z. B. durch Synergieeffekte mit dem neuen Personalausweis. So kann dieser per freigeschalteter eID-Funktion (Online-Ausweisfunktion) sowohl für die Online-Identifizierung bei der Erstregistrierung eines De-Mail-Nutzers eingesetzt werden als auch später für die optimal abgesicherte Anmeldung beim jeweiligen De-Mail-Konto.

Weitere nützliche Einsatzmöglichkeiten eröffnen sich durch eine individuelle Wahl und Kombination verschiedener Versandoptionen, durch die sich der Weg der De-Mail verfolgen und im Nachhinein belegen lässt. In diesem Zusammenhang stehen etwa die Versandoptionen „Versandbestätigung“ und „Eingangsbestätigung“ zur Verfügung.

Zusätzlich können auch die Kategorien „Persönlich“ und „Absender-bestätigt“ beim Versand gewählt werden. Diese setzen im ersten Fall für das Lesen durch den Empfänger und im zweiten Fall für das Verschicken durch den Absender jeweils eine Anmeldung/einen Login mit hohem Sicherheitsniveau zum eigenen De-Mail-Konto voraus. In Verbindung mit der so sichergestellten Authentizität sowohl des Senders als auch des Empfängers kann der Absender beispielsweise aufzeigen, dass eine Nachricht eines bestimmten Inhaltes zu einem bestimmten Zeitpunkt an eine eindeutig bestimmte Person, Firma oder Institution gesendet und in deren Postfach hinterlegt wurde.

Der Einstieg in De-Mail ist für die Anwender sehr einfach. Für größere Unternehmen und Institutionen aus Wirtschaft und Verwaltung existieren Anbindungslösungen über Gateways, die das System effizient in eine bereits bestehende interne Mail-Infrastruktur integrieren. Private Anwender oder kleinere Unternehmen können zum Senden und Empfangen von De-Mails die vom jeweiligen Diensteanbieter bereitgestellte Weboberfläche nutzen. In der Anwendung funktioniert das Ganze in der Regel genauso einfach wie die normale E-Mail.

Weitere Perspektiven

Aufgrund der Konzeption von De-Mail als geschlossenes System sind sowohl die absoluten Zahlen der Konten und der damit erreichbaren Personen als auch die Attraktivität der von Wirtschaft und Verwaltung angebotenen Einsatzszenarien wichtige Faktoren, die sich gegenseitig befruchten und damit einen wichtigen Beitrag zum weiteren Erfolg von De-Mail leisten können. Um diesen Prozess zu fördern, hat die Bundesregierung im September 2012 das E-Government-Gesetz auf den Weg gebracht, das u. a. Bundesbehörden unter bestimmten Voraussetzungen dazu verpflichten soll, Bürgerinnen und Bürgern die direkte Adressierbarkeit und Kontaktaufnahme per De-Mail zu ermöglichen. Darüber hinaus sollen auf Basis des E-Government-Gesetzes neben der qualifizierten elektronischen Signatur auch die eID-Funktion des neuen Personalausweises sowie die absenderbestätigte De-Mail die bisher in vielen Angelegenheiten erforderliche Schriftform ersetzen können.

Zusätzlich bietet die laufende E-Government-Initiative des Bundesministeriums des Innern gute Voraussetzungen, um weitere Einsatzmöglichkeiten in diesem Bereich zu erschließen und damit die Akzeptanz der neuen Technologien in der Bevölkerung zu erhöhen – etwa durch die Unterstützung von Pilotvorhaben der Verwaltung unter Einbeziehung des neuen Personalausweises und/oder von De-Mail. Durch die zusätzliche Integration von effizienteren und möglichst medienbruchfreien (also voll elektronischen) Verfahren in laufende Prozesse, z. B. bei Antragsverfahren, profitiert nicht nur die Verwaltung selbst, sondern auch der Bürger. Ihm bleiben so unter Umständen aufwendigere Behördengänge erspart.

De-Mail
So einfach wie E-Mail, so sicher wie Papierpost.

Web:
www.de-mail.de

Potenzialanalysen für Kritische Geschäftsprozesse

Kurt Klinner,
Leiter des Referats Informationssicherheitsberatung in Projekten

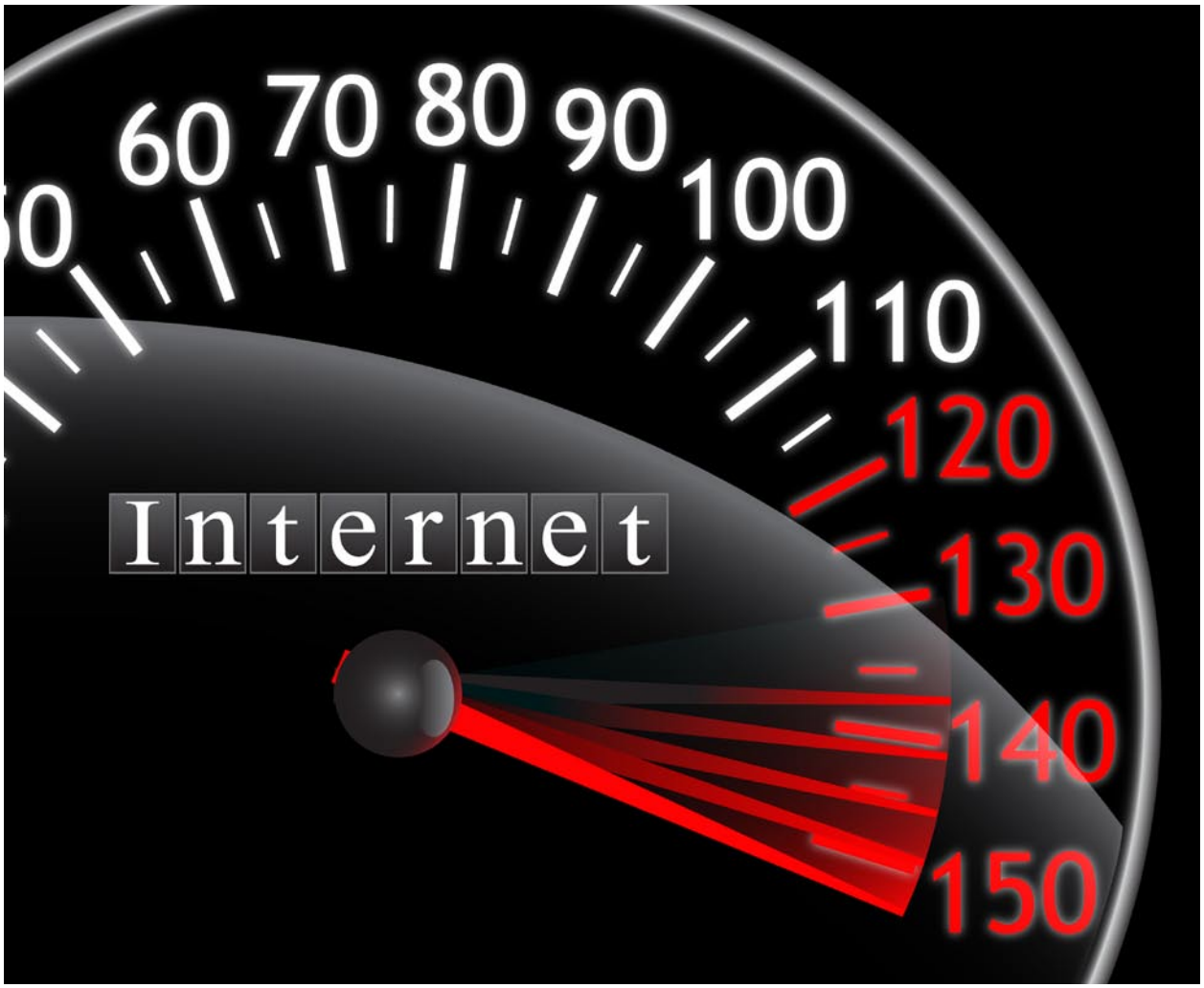
In der Wirtschaft ebenso wie in der Verwaltung gibt es kaum noch einen Geschäftsprozess, der nicht von Informationstechnologie abhängt. Insbesondere Kritische Geschäftsprozesse erfordern eine besondere Verlässlichkeit der IT-Systeme. Denn fallen diese aus, kann das erhebliche Folgen für das Unternehmen oder die Organisation haben. Um dies zu vermeiden, arbeitet das BSI an der Entwicklung eines speziellen Steuerungsinstrumentes.

Gerade in Bezug auf die Verlässlichkeit der IT sind besondere Vorkehrungen vonnöten. Teilaspekte sind dabei Robustheit und Redundanz, und diese wirken wiederum entscheidend auf die Verfügbarkeit. Zudem gewinnen Faktoren Einfluss, die als Qualität von Kultur und Technik innerhalb der Organisation und als Professionalität der Mitarbeiter anzusehen sind. Diese Potenziale können nach den Prozessmodellen der IT-Governance (Control Objectives for Information and Related Technology, CobiT; IT Infrastructure Library, ITIL) als qualitative Indikatoren zur Steuerung von IT-Leistungen eingesetzt werden. Im Sinne der IT-Governance liefern diese Potenziale den bewertbaren Nutzen der IT für Geschäftsprozesse und Geschäftserfolg. Sie dienen der Verlässlichkeit, wenn sie einen Nutzen produzieren, der sich positiv auf die Verfügbarkeit auswirkt oder der eine hinreichende Widerstandskraft gegen schädigende Einflüsse aufbringt.

In der Praxis stehen Unternehmen und Institutionen damit vor der Herausforderung, ihre jeweiligen Potenziale zu bewerten und jene Bereiche zu identifizieren, in denen nutzbare Potenziale unter den Anforderungen liegen und daher optimiert werden müssen. Zur Bewertung von Potenzialen führen oben genannte Prozessmodelle Reifegradmodelle ein, die davon ausgehen, dass sich einfache Systeme zu komplexen Systemen weiterentwickeln. Überträgt man diese Betrachtungsweise auf das Beispiel der Entwicklung des Automobils, so lassen sich folgende Entwicklungsstufen erkennen:

Reifegrad	1	2	3	4	5
Bezeichnung	Initial	Definiert	Standardisiert	Gesteuert	Integriert
Beschreibung der Entwicklungsstufe	Funktion erfüllt	Vehikel zum Transport von Personen oder Gütern	Orientierung an Standards/Sicherheitsstandards	Elektronische Steuerungskomponenten	Kommunikationssysteme, interaktive Steuerung
Beispiel mit Kriterien/ Merkmalen	Entstehung der ersten Motorkutschen	Differenzierung in PKW und LKW	Einführung von Sicherheitsgurten, Kopfstützen	Einführung von ABS, Airbag, elektronischer Motorsteuerung	Einführung von Fahrassistenzsystemen, Notbremssystemen

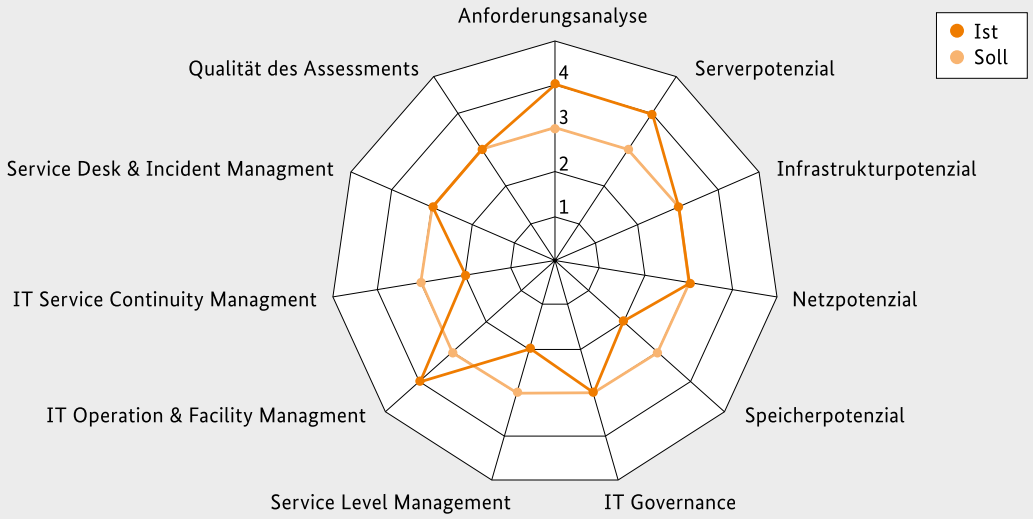
Tabelle 1: Reifegradmodell Automobilentwicklung



Ergebnisreport	
Zusammenfassung	
Betrachtete Organisation:	Unternehmen XY
Assessment-Datum:	01.08.2011
Assessor:	Hans Mustermann
Untersuchungsbereich:	Geschäftsprozess Rechnungsplanung

Gesamtpotenzial: Stufe 2 **Soll-Potenzial: Stufe 3**

HV-Assessment Gesamtergebnis



Da Automobile hoch komplexe Systeme sind, ist für eine fundierte Analyse zudem die Untersuchung einzelner Komponenten-Cluster wie Motor, Fahrwerk oder Innenraum erforderlich. Auf der Grundlage des vorstehenden Reifegradmodells sind somit weitere spezifische Reifegradmodelle zu entwickeln, welche die Potenzialstufen in spezifischen Kriterien der Komponenten-Cluster beschreiben.

Der methodische Ansatz der Reifegradmodelle wurde im Rahmen eines Projekts des Bundesamts für Sicherheit in der Informationstechnik (BSI) auf die Analyse von IT-Architekturen im Umfeld Kritischer Geschäftsprozesse übertragen und für die Bewertung von Verlässlichkeitspotenzialen weiterentwickelt. Elf besonders relevante Kriterien wurden dabei in einem Steuerungsinstrument zur Bewertung des Verlässlichkeitspotenzials zusammengefasst. Mittlerweile steht beim BSI der Prototyp einer Anwendung für die Analyse und IT-Steuerung zur Verfügung. Mithilfe dieser Anwendung erhalten Organisationen einen Vergleich der vorhandenen Potenziale (Ist-Linie im oben stehenden Kiviat-Diagramm) mit den gesetzten Anforderungen (Soll-Linie) und können so eventuell vorliegende Unterdeckungen identifizieren. Der Nutzen für Unternehmen und behördliche Organisationen stellt sich durch den Einstieg in einen kontinuierlichen Verbesserungsprozess zur Steigerung von Effektivität und Effizienz in IT-Architekturen und IT-Prozessen ein. Nicht zuletzt bringen optimierte Architekturen und Strukturen durch die Steigerung von Professionalität und Verlässlichkeit einen IT-Sicherheitsgewinn mit sich.

Neben einer Gesamtbetrachtung können auch Detailauswertungen in den elf untersuchten Architektur-Clustern angefertigt werden, die Umsetzungsempfehlungen mit Verweisen auf die IT-Grundschutzstandards, den Maßnahmenkatalog des Hochverfügbarkeits (HV)-Kompendiums oder auf die Prozessmodelle von ITIL und CobiT enthalten. Das BSI hat die vorstehenden Konzepte zur Steuerung der IT auf der Grundlage von Verfügbarkeits- bzw. Verlässlichkeitspotenzialen im Rahmen der Fortschreibung des HV-Kompendiums zur Version 1.6 entwickelt. Diese neue Version wurde zur CeBIT 2013 veröffentlicht und steht auf der Website des BSI unter www.bsi.bund.de zur Verfügung.

Kommunikation – mobil und geschützt

Smartphones – schick, aber unsicher?

Matthias Hirsch und Dr. Christian Schridde,
Referenten für sicheres mobiles Arbeiten

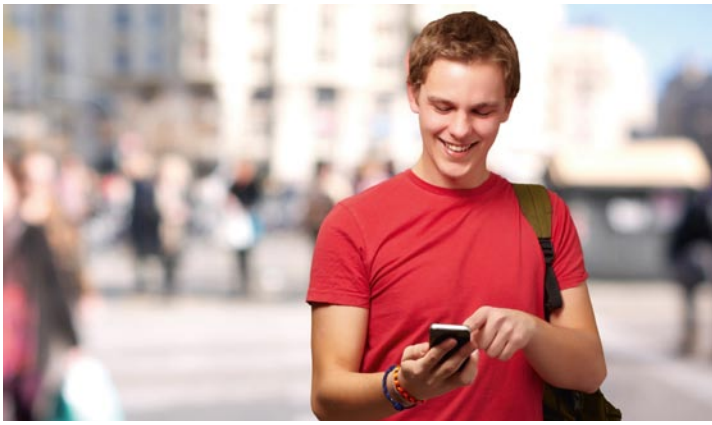
Seit Längerem ist bekannt, dass Handys und Smartphones nicht abhörsicher sind. Das liegt zum einen daran, dass der für die Kommunikationsstrecke zwischen Endgerät- und Basisstation eingesetzte Kryptoalgorithmus in den älteren Versionen entzifferbar ist. Zum anderen sind die Verbindungsstrecken von den Basisstationen zu den Vermittlungsstellen sowie zwischen den Vermittlungsstellen unverschlüsselt.

Noch nicht so intensiv untersucht sind hingegen die Gefährdungen durch Cyberangriffe, mit denen sich der folgende Beitrag befasst. Die zahlreichen nützlichen Funktionen von Smartphones und Tablets im Alltag sind mittlerweile für immer mehr berufliche und private Nutzer unverzichtbar: mobiles Internet, Navigations-, Ortungs- und Kartendienste, E-Mail- und Synchronisationsdienste, Spiele sowie viele weitere Anwendungen, auch Apps genannt, möchte man nicht mehr missen. Im gleichen Maße, in dem Smartphones und Tablets funktional zu PCs aufgeschlossen haben, sind aber auch die aus dem PC-Bereich seit Langem bekannten Sicherheitsrisiken für Smartphones und Tablets relevant geworden.

Die klassischen Sicherheitsrisiken für GSM-Mobiltelefone betrafen vor allem den Missbrauch mobiler Telefonie und SMS. Dazu gehörten etwa die unerkannte Umleitung von Verbindungen auf Bezahldienste, das Abhören von Telefongesprächen oder das Mitlesen von SMS sowie die unbefugte Nutzung des Handyvertrags durch den Dieb eines Mobiltelefons. Diese Bedrohungen bestehen nach wie vor, auch für moderne Smartphones. Hinzugekommen ist jedoch eine Reihe von Sicherheitsrisiken für neue Anwendungen, die durch Smartphones erst möglich wurden, beispielsweise Mobile Banking, Ortung, mobiler Zugriff auf vertrauliche Daten sowie der mobile Zugriff auf Dienste und Benutzerkonten im Internet. Angriffe auf diese Dienste und Daten sind vor allem über die breitbandigen und vielfältigen IP-basierten Netzzugänge (UMTS, LTE, WLAN) eines Smartphones möglich geworden. Dabei sind Smartphones und Tablets im Vergleich zu stationären PCs noch lohnendere Ziele, denn hier sind viele persönliche Daten des Benutzers auf einem Gerät konzentriert. Hinzu kommt, dass man bei Smartphones und Tablets nicht von der vergleichsweise sicheren Betriebsumgebung eines stationären PC ausgehen kann.

Angriffe auf Smartphones in Zahlen

Einer Studie der European Network and Information Security Agency (ENISA) zufolge wird die Anzahl der Smartphones im Jahre 2013 die Anzahl der PCs erstmals



übersteigen. 2012 waren einer Untersuchung des European Information Technology Observatory (EITO) zufolge 70 Prozent aller in Deutschland verkauften Mobiltelefone Smartphones. Smartphones sind damit zu einem Hauptzugangstor zum Internet geworden.

Es ist nicht verwunderlich, dass mit den Verkaufszahlen auch die Anzahl der gemeldeten Angriffe auf Smartphones stetig steigt. Die Threat-Landscape-Studie der ENISA vom November 2012 hat gezeigt, dass unter den 16 häufigsten Gefahren für die IT-Sicherheit die Zahl der Angriffe auf mobile Geräte am stärksten wächst.

Verlust und Diebstahl des Smartphones

Betrachtet man nur Smartphone-spezifische Angriffe, stellt der Verlust oder Diebstahl eines Gerätes die häufigste Ursache von Datenverlust dar. Der Grund ist klar: Ein Smartphone trägt man stets bei sich, und die Gefahr, es zu verlieren, ist damit erheblich größer als bei anderen Kommunikationsgeräten. Und gerade weil ein Smartphone bei vielen Benutzern einen Punkt konzentrierter Information darstellt, ist der Verlust und der damit einhergehende Datenabfluss umso gravierender.

Einige Hersteller bieten eine nachträgliche Fernlöschung („Remote-Wipe“) an, bei der die Einstellungen oder Daten des verlorenen oder gestohlenen Smartphones zurückgesetzt beziehungsweise gelöscht werden oder das Gerät für die Nutzung insgesamt gesperrt wird. Auch Zugangspasswörter wie Gerätecode und SIM-PIN bieten bedingten Schutz, je nachdem, in welchem Zustand ein Gerät in unbefugte Hände gerät.

Malware und Spyware

Die zweithäufigste Ursache für den Datenverlust entsteht durch Apps – und zwar durch solche, die mehr tun, als sie eigentlich sollten. Dazu gehören z. B. Taschenlampen-

Verlauf der Entdeckung neuer Schadsoftware vom 01.01.2011 bis 30.09.2012.

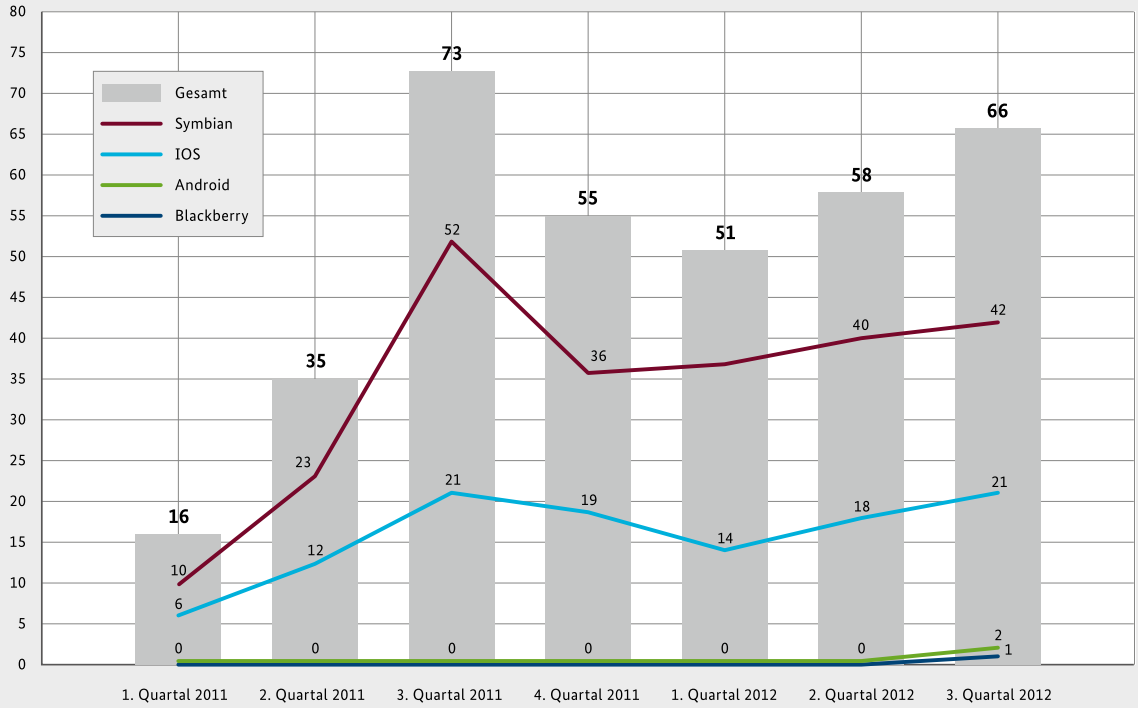


Abbildung 1: Neu erkannte Angriffsfamilien und Varianten (Quelle: F-Secure)

Apps, die auf das lokale Telefonbuch zugreifen können, oder Spiele, die die Berechtigung haben, eine SMS zu versenden. Solche Apps greifen auf Ressourcen und Möglichkeiten des Smartphones zu, die mit ihrer eigentlichen Funktion nichts zu tun haben. Die Betriebssysteme gewährleisten zwar, dass der Benutzer diese Zugriffe vor der Installation freigeben muss. Viele Benutzer klicken solche Abfragen mit einem „OK“ durch, um endlich die App starten zu können. Leider machen sich nur die wenigsten Anwender Gedanken, welche Auswirkungen diese Freigaben später für sie haben könnten. Zwar ist nicht jede App, die mehr Funktionen wahrnimmt als nötig, zwangsläufig „böse“. Dennoch sind erhebliche Risiken vorhanden, die vom Datendiebstahl über die Möglichkeit, den Nutzer zu lokalisieren, bis hin zum Identitätsdiebstahl reichen.

Andere Schadsoftwarevarianten wie Würmer, Trojaner oder Viren, die man aus dem PC-Bereich kennt, stellen mittlerweile auch für Smartphones ein relevantes Risiko dar. Diese klassischen Schadfunktionen kann man sich beispielsweise via App auf das Smartphone laden. Während bei früheren Mobiltelefonen die Anwendungen ausschließlich durch den Hersteller des Mobiltelefons geliefert wurden, liegt bei modernen Smartphones die Verantwortung für sichere Software einerseits bei den zahlreichen App-Programmierern, andererseits bei den Appstore-Betreibern, die die Sicherheit der Apps mehr oder weniger gründlich überprüfen. Nicht zuletzt hat jedoch auch der Nutzer eine Verantwortung: Er kann das Risiko durch sein Downloadverhalten beeinflussen.

Als Schutzmaßnahmen bieten sich Virenschutzprogramme und Personal Firewalls in Form von Apps an, die allerdings technisch bedingt Sicherheit nicht in dem Umfang bieten, wie er in der PC-Welt üblich ist. Updates zur Behebung von Sicherheitslücken und Bugs werden durch die meisten Betriebssystemhersteller regelmäßig verteilt. Dies gilt jedoch leider nicht für Updates, deren Verteilung in der Verantwortung unterschiedlicher Smartphonehersteller liegt. Diese werden mitunter verspätet oder gar nicht verteilt.

Angriffe und Zugriff über lokale Netze

Eine weitere Smartphone-typische Möglichkeit des Datendiebstahls ergibt sich aus dem Nutzungskonzept von mobilen Geräten, etwa im Bereich der Netzkonnektivität. Smartphones sind ständig auf der Suche nach einer Internet-Verbindung, nicht nur über den Provider der SIM-Karte, sondern auch über offene WLAN-Hotspots. Dies geschieht je nach Konfiguration auch automatisch und ohne Meldung an den Nutzer. Einem Angreifer eröffnet dies die Möglichkeit, ein dem Smartphone bekanntes und erlaubtes Netzwerk vorzutäuschen, in das sich das Smartphone dann automatisch einwählt. Sämtliche Daten werden dann über die Systeme des Angreifers geleitet, ohne dass der Benutzer dieses erkennt. Je nachdem, wie ambitioniert der Angreifer vorgeht, kann er die zwischen Smartphone und Server ausgetauschten Daten aufzeichnen oder manipulieren.

„Anwender sollten sich auch der Risiken bewusst sein, die mit der Nutzung von Smartphones einhergehen."

Risiken erkennen

Smartphones bieten vielfältige Möglichkeiten und können das private und geschäftliche Leben an vielen Stellen komfortabler und leichter machen. Anwender sollten sich jedoch auch der Risiken bewusst sein, die mit der Nutzung eines Smartphones einhergehen. Die Verantwortung für die Sicherheit von Smartphones verteilt sich dabei auf die Hersteller von Geräten, Apps und Betriebssystemen sowie die Mobilfunknetz- und Appstore-Betreiber. Nicht zuletzt ist aber auch der private wie professionelle Nutzer gefordert.

Angesichts dieser verteilten Verantwortlichkeiten ist die Verbesserung der IT-Sicherheit von Smartphones eine komplexe Aufgabe, in die das BSI in koordinierender und sensibilisierender Funktion eingebunden ist. Als neutrale Instanz führt das BSI Gespräche mit allen Beteiligten und moderiert so den Lösungsprozess. Zudem klärt das BSI im Rahmen seiner Website www.bsi-fuer-buerger.de über Sicherheitsrisiken auf und gibt Anwendern nützliche Hinweise im Umgang mit Smartphones. Für die dienstliche Nutzung von Smartphones in der Bundesverwaltung hat das BSI darüber hinaus eine unmittelbare Verantwortung. Das Ziel ist hier, sichere mobile Lösungen für alle Arbeitsbereiche und Anwendungsfälle anzubieten. Ausgehend vom ermittelten Bedarf werden dazu durch Ausschreibungen oder eigene Entwicklungsprojekte genau die technischen Lösungen maßgeschneidert, die in einem modernen Arbeitsprozess benötigt werden.

Web:
www.bsi-fuer-buerger.de/MobileSicherheit

SINA Workflow: Medienbruchfreies Arbeiten für höchste Sicherheitsanforderungen

Wie gelangt die richtige Information an den richtigen Mitarbeiter – und nur an diesen? In der Arbeit mit Verschlusssachen ist besondere Sorgfalt gefordert, um Inhalte vor dem unberechtigten Zugriff Dritter zu schützen. Eine nicht autorisierte Weitergabe oder Veröffentlichung hat strafrechtliche Konsequenzen, im schlimmsten Fall drohen mehrjährige Haftstrafen. Im Umgang mit Verschlusssachen ist es daher zwingend erforderlich, alle gesetzlichen und regulativen Vorgaben einzuhalten – auch bei elektronischer Verarbeitung.

> *„Im Fokus steht die Maximierung der Benutzerfreundlichkeit bei gleichzeitiger Gewährleistung höchster Sicherheitsansprüche."*

Der Name SINA (Sichere Inter-Netzwerk Architektur) steht in der Bundesverwaltung für die geschützte Bearbeitung, Speicherung und Übertragung von Verschlusssachen über das Internet. Unter anderem sind bereits SINA Virtual Workstations als Arbeitsplatzrechner beziehungsweise als mobile Laptops in der Bundesverwaltung im Einsatz. Als neuestes Kind der SINA-Familie befindet sich derzeit SINA Workflow in der Entwicklung – eine Softwarelösung, die die medienbruchfreie Bearbeitung von Verschlusssachen ermöglichen wird.

Oliver Zendel,
Referent für die Entwicklung informationssichernder Systeme

Das Produkt SINA Workflow wurde speziell konzipiert, um geheimhaltungsbedürftigen elektronischen Informationen bis zum Einstufungsgrad GEHEIM einen maximalen Schutz zu bieten. Der Schutz erstreckt sich dabei über den kompletten Lebenszyklus elektronischer Verschlusssachen:

- Erstellung und Erfassung
- Identifikation/Authentisierung
- Verarbeitung
- Speicherung
- Verwaltung
- Prozessunterstützung
- Protokollierung und Nachweise
- Zugriffsschutz und Schutz der Vertraulichkeit

Auf diese Weise können nicht nur Zugriffsrechte verwaltet werden, sondern es lässt sich beispielsweise auch vorschriftenkonform nachweisen, wer welche Änderungen am Dokument vorgenommen hat. Der SINA Storage Service erlaubt ein zentrales verschlüsseltes Speichern im Netzwerk. Mit dem SINA Registry Service werden das Gruppieren von Verschlusssachen zu Akten und Vorgängen sowie nachvollziehbare und verbindliche Mitzeichnungen möglich. So kann SINA Workflow zukünftig eine rein elektronische Verarbeitung von Verschlusssachen ohne Medienbrüche ermöglichen.

Das BSI startete das Entwicklungsprojekt Ende 2011. Im Jahr 2012 konnte gemeinsam mit einem Pilotanwender aus der Bundesverwaltung die erste Version geplant und umgesetzt werden. Eine besondere Bedeutung kam dabei der Erstellung des Fachkonzeptes zu, das in enger Zusammenarbeit mit den späteren Anwendern entwickelt wurde. Ziel dieses Vorgehens war es, möglichst frühzeitig sicherzustellen, dass die geplanten Funktionen geeignet sind, um die fachlichen Aufgaben der Anwender zu unterstützen. Im Fokus der Entwicklung steht – wie bei allen SINA-Produkten – die Maximierung der Benutzerfreundlichkeit bei gleichzeitiger Gewährleistung höchster Sicherheitsansprüche.

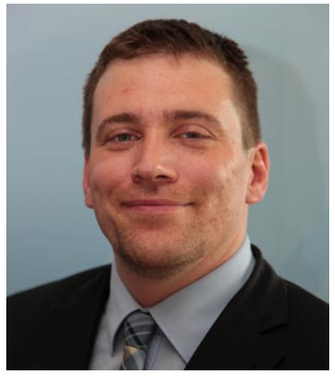
Nach der Identifikation und Abstimmung der fachlichen Anforderungen, Prozesse und Anwendungsfälle stellte die Erstellung einer geeigneten, sicheren IT-Architektur für den angestrebten Einsatzfall GEHEIM die größte Herausforderung dar. Auch in dieser Phase war die enge Zusammenarbeit mit den Pilotanwendern sehr hilfreich, da identifizierte Konflikte von fachlichen Anforderungen und dem angestrebten Sicherheitsniveau im Interesse aller Beteiligten frühzeitig aufgelöst werden konnten.

Aktuell findet beim Pilotanwender der Aufbau und der Betrieb der ersten Version statt. Die Erfahrungen im Piloten werden helfen, das Produkt für den Einsatz in der gesamten Bundesverwaltung zu optimieren.

Technologie –
Sichere Lösungen

Kritische IT-Systeme im Internet: Effizienz auf Kosten der Sicherheit?

Die Zeiten, in denen lediglich klassische Client- und Serversysteme mit dem Internet verbunden waren, sind schon lange passé. Nicht zuletzt der massive Kostendruck für die Herstellung und den Betrieb technischer Gerätschaften aller Art hat die Konvergenz von Netzen und Systemen massiv vorangetrieben.



Holger Junker,
Referatsleiter Cyber-Sicherheit in kritischen IT-Systemen, Anwendungen und Architekturen

Sogenannte Embedded Devices – also Rechner, die in einen technischen Kontext eingebunden sind und Funktionen im Bereich Steuerung, Regelung, Überwachung oder Datenverarbeitung übernehmen – sind heutzutage zumeist an ein Netzwerk oder auch direkt an das Internet angebunden. Besonders kritisch können sog. Cyber-Physical Systems sein – also Embedded Devices, die eine enge Kopplung des Cyberraums mit der realen Welt umsetzen. Beispiele hierfür finden sich in der Medizintechnik, der Gebäudeautomation oder im Bereich Automotive. Spätestens seit der Entdeckung des Schadprogramms Stuxnet 2010 sind zudem industrielle Steuerungsanlagen (Industrial Control Systems, ICS) im Fokus der Öffentlichkeit. Dazu gehören etwa Anwendungsfälle wie Fabrikautomation oder Prozesssteuerung (z. B. Raffinerien oder Kläranlagen), bei denen Sicherheitsvorfälle mitunter Auswirkungen auf Kritische Infrastrukturen haben können. Solche internetverbundenen IT-Systeme sind aufgrund ihrer Exposition prinzipiell dem Risiko ausgesetzt, durch Hacker, Botnetze oder Malware angegriffen zu werden.

Alles Stuxnet, oder was?!

Schadprogramme wie Stuxnet, Duqu oder Flame haben gezeigt, mit welchem Aufwand Cyber-Attacken unternommen werden können. Offensichtlich gibt es Angreifer, die bei hinreichender Motivation in nahezu jedes System eindringen. Es ist eine Binsenweisheit, dass es keine hundertprozentige Sicherheit gibt. Doch in der Regel sind es nicht die zielgerichteten und mit großem Aufwand entwickelten Schadprogramme, welche die Existenz eines Unternehmens bedrohen. Aufgrund der zunehmenden Verbreitung von Standardkomponenten in industriellen Anlagen kann allgemeine Malware zu massiven Produktionsausfällen führen.

Die Sabotage der Produktion ist nur der letzte Schritt eines Angriffs. Meist gelingt es Angreifern, über das allgemeine Office-Netz in das Unternehmen einzudringen. Der aktuelle Incident Response Summary Report 2009–2011 (http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf) des US-amerikanischen ICS-CERT gibt beispielsweise an, dass bei sieben von 17 berichteten Vorfällen im Bereich industrieller Steuerungsanlagen Spear Phishing – also ein zielgerichteter Phishing-Angriff – eine zentrale Rolle gespielt hat.

Bürogeräte als Opfer eines Angriffs

Moderne Bürogeräte – also Drucker, Scanner, Kopierer oder Faxgeräte – verfügen typischerweise über eine Netzwerkschnittstelle, um sie etwa in die Office-Infrastruktur eines Unternehmens zu integrieren. Dies eröffnet prinzipiell Möglichkeiten für Angriffe. Zudem sind die in den Geräten enthaltenen Funktionen mitunter nicht sicher implementiert, dafür aber in der Standardkonfiguration aktiviert. Manchmal können sie gar nicht deaktiviert werden.

Mit Suchmaschinen kann ein Angreifer leicht eine Vielzahl solcher Systeme identifizieren. So wurden in einer Stichprobe des BSI in kürzester Zeit Tausende von Bürogeräten in Deutschland gefunden, die über das Internet erreichbar und nicht oder nur unzureichend geschützt sind. Allein für eine bekannte Produktreihe eines großen Herstellers konnten schnell mehr als 2.000 Geräte identifiziert werden. Betroffen hiervon sind große und kleine Unternehmen gleichermaßen, genauso wie Hochschulen und Forschungsinstitute.

Bei fehlender oder schwacher Authentisierung kann ein Angreifer beispielsweise gescannte oder gedruckte

Dokumente herunterladen oder Änderungen an der Gerätekonfiguration vornehmen. Authentisierungsmechanismen können dabei mitunter einfach umgangen werden. Zudem sind viele dieser Geräte mit Schwachstellen behaftet. Somit sind Geräte prinzipiell angreifbar, wenn sie mittels einer IP-Adresse über das Internet erreichbar sind.

Wie hacke ich ein Gebäude?

Ein realer Fall aus dem Bereich Buildung Automation einer Institution im Technologiesektor zeigt die Gefährdungen solcher Cyber-Physical Systems. Im konkreten Fall war wegen fehlender Authentisierung eine direkte Manipulation der Steuerung möglich.

- Sobald der Zugriff auf die Weboberfläche der Gebäudesteuerung erreicht ist, können sämtliche zur Verfügung stehenden Funktionen genutzt werden. Hierzu gehören etwa die beliebige Änderung von Raumtemperaturen, das Betätigen von Schaltern, das Ver- oder Entriegeln von Fenstern und Türen sowie das Deaktivieren von Bewegungsmeldern.
- Es können beliebige Einstellungen geändert werden – sogar Passwörter. Auch die Firmware kann manipuliert werden.
- Da die Anzahl der HTTP-Sessions beschränkt ist, kann der Angreifer verhindern, dass das Bedienpersonal Zugriff auf die Weboberfläche bekommt. Hierzu muss er einfach mehrere Browserfenster zur Weboberfläche der Gebäudesteuerung öffnen.

Lösungswege

Für Hersteller von Komponenten sowie Integratoren empfiehlt sich die Etablierung geeigneter Prozesse, die die Bereitstellung sicherer Produkte ermöglichen. Ein ganzheitlicher Ansatz in Form eines Secure Development Lifecycle (SDL) sollte von der Konzeption über die Produkterstellung und die Unterstützung der Kunden bis hin zum End-of-Life des Produkts gewährleistet sein. Das BSI unterstützt in diesem Bereich u.a. bei der Sicherheitsanalyse von Komponenten sowie mit Vorgaben und Empfehlungen für eine sichere Entwicklung.

„Betreiber sollten die Sicherheit ihrer kritischen IT-Systeme in Form eines Information Security Management Systems (ISMS) ganzheitlich betrachten."

Betreiber sollten die Sicherheit ihrer kritischen IT-Systeme in Form eines Information Security Management Systems (ISMS) ganzheitlich betrachten. Das BSI bietet neben dem IT-Grundschutz als Basis für ein ISMS eine Vielzahl von Empfehlungen und Hilfsmitteln, um die Sicherheit von kritischen IT-Systemen, Cyber-Physical Systems und Industrial Control Systems zu verbessern. Dabei werden insbesondere auch spezifische Herausforderungen betrachtet, welche etwa industrielle Anwendungsbereiche von der konventionellen IT-Sicherheit unterscheiden. Mit diesen und weiteren Unterstützungsangeboten des BSI ist es möglich, kritische internetverbundene (oder anderweitig vernetzte) IT-Systeme hinreichend sicher und gleichzeitig kosteneffizient zu betreiben.

Industrie 4.0

Der Begriff Industrie 4.0 soll die vierte industrielle Revolution zum Ausdruck bringen: die Informatisierung der klassischen Industrien. Das Konzept der intelligenten Fabrik soll sich in diesem Prozess auf die gesamte Wertschöpfungskette ausdehnen. Durch Selbstoptimierung, Selbstkonfiguration und Selbstdiagnose der Produktion soll die Kosteneffizienz optimiert und Deutschland als Produktionsstandort gefestigt werden. Mit Industrie 4.0 wird die Anzahl der – mitunter unternehmensübergreifenden – Kommunikationsbeziehungen drastisch steigen. Diese gilt es entsprechend abzusichern. Da die Produktionsprozesse nicht mehr nur im eigenen Unternehmen ablaufen, sind neben geeigneten Lösungen für das Identitätsmanagement insbesondere sichere Konzepte für den Produkt- und Know-how-Schutz gefragt. Zudem müssen Konzepte wie Cloud Computing sicher in die Produktions-IT integriert werden. Von besonderer Bedeutung ist aber, dass auf dem Weg zur Industrie 4.0 die bestehenden Sicherheitsaspekte von Anfang an berücksichtigt werden.

Cloud Computing – Sicherheit durch Standards

Alex Essoh,
Referent für Grundlagen der Informationssicherheit und IT-Grundschutz

Fritz Bollmann,
Referent für die Zertifizierung von Produkten

Als vor einigen Jahren der Begriff Cloud Computing in die öffentliche Diskussion gelangte, gab es nicht wenige, die darin nur ein weiteres Schlagwort der IT-Industrie sahen. Speziell die Fachwelt war sich schnell einig, dass Cloud Computing ähnlich dem war, was man bis dahin unter Begriffen wie Outsourcing, Grid Computing oder Application Service Providing diskutiert hatte. Genauso einig war man sich aber auch darüber, dass Cloud Computing das Potenzial hat, die Bereitstellung und Nutzung von Informationstechnologie nachhaltig zu verändern. Mittlerweile zeigen nicht nur viele Marktstudien, sondern auch unzählige Angebote, die sich an Endverbraucher wie Geschäftskunden richten: Die Cloud hat den Hype-Status verlassen und ist in der Realität angekommen.

Viele Regierungen und andere Institutionen unterstützen und fördern heute in ihrem jeweiligen Einflussbereich Cloud Computing als Zukunftsmodell zur Bereitstellung und Nutzung von IT. In den USA, dem Land mit den derzeit meisten und umsatzstärksten Cloud-Computing-Anbietern, wurde beispielsweise die „Cloud First Policy“ etabliert. Sie verpflichtet US-Bundesbehörden, vor einer neuen IT-Investitionsentscheidung immer zuerst Cloud-Computing-Alternativen zu evaluieren. Auch in Europa hat die EU-Kommission mit der Veröffentlichung ihrer Strategie zu Cloud Computing („Freisetzung des Cloud-Computing-Potentials in Europa“) im September 2012 ein deutliches Signal für ein verstärktes Engagement in diesem Bereich gesetzt und gleichzeitig Schlüsselaktionen identifiziert. In Deutschland ist Cloud Computing eine zentrale Komponente der IKT-Strategie „Deutschland Digital 2015“ und wurde im Rahmen des Nationalen IT-Gipfel-Prozesses als bedeutendes Thema für die Technologie- und Standortpolitik Deutschlands identifiziert.

Die Vorteile des Cloud Computing wie Flexibilität der Nutzung und Bereitstellung von IT-Ressourcen, potenzielle Kostenreduktion sowie eine umwelt- und ressourcenschonende IT-Nutzung werden in der öffentlichen Diskussion nicht mehr angezweifelt. Auch über die wesentlichen Hindernisse besteht weitestgehend Einigkeit: Hierzu zählen uneinheitliche Datenschutzregelungen und intransparente Verträge ebenso wie eine unzureichende Interoperabilität der Cloud-Computing-Plattformen oder Probleme bei der Portabilität der Daten. Wichtigster Hemmschuh ist jedoch nach wie vor die Frage nach der Sicherheit und Vertraulichkeit der Informationen, die man in der Cloud vorhält. Derzeit existiert noch keine international akzeptierte Sicherheitszertifizierung für Cloud-Angebote. Das BSI sieht hier dringenden Handlungsbedarf und hat sich daher das Ziel gesetzt, durch die Entwicklung von Mindeststandards die Informationssicherheit in der Cloud durch die Unterstützung und die Zusammenarbeit mit der Industrie zu verbessern.

Von nationalen Eckpunkten zu internationalen Mindeststandards

Um eine breite Akzeptanz zu erreichen, müssen Sicherheitskriterien für Cloud-Lösungen praxisnah und angemessen sein. Daher erfolgt die Erstellung der Kriterien in enger Zusammenarbeit mit Marktteilnehmern und Anbietern. Als ersten Schritt auf dem Weg zu einem Sicherheitsstandard hat das BSI ein Eckpunktepapier mit Mindestsicherheitsanforderungen an Anbieter von Cloud-Lösungen veröffentlicht und zur Diskussion gestellt. Zahlreiche Kommentare und Ergänzungen von Anbietern und Anwendern sind in das Papier eingeflossen, bevor die finale Fassung im Mai 2011 veröffentlicht wurde. Das Eckpunktepapier kann von Cloud-Service-

Providern als Leitlinie für die Umsetzung von Sicherheitsmaßnahmen genutzt werden – potenziellen Nutzern dient es als erste Orientierung in Fragen Sicherheit.

Das BSI betrachtet in seinem Eckpunktepapier elf als kritisch identifizierte Bereiche der Cloud-Computing-Sicherheit. Zusätzlich wird eine Reihe von „Best Practice"-Beispielen zur Absicherung dieser Bereiche genannt. Neben Sicherheitsanforderungen aus der klassischen IT wie Sicherheitsarchitektur, ID- und Rechtemanagement werden auch Themen behandelt, die bei der Auslagerung von Daten, Anwendungen und Prozessen in eine Public Cloud besondere Relevanz erhalten. Hierzu zählen Transparenz, Vertragsgestaltung, Datenschutz und Mandantenfähigkeit.

„Ein wesentlicher Erfolgsfaktor der Cloud heute ist Vertrauen: Die Anwender müssen Vertrauen haben in die Sicherheit der Daten, in die Infrastrukturen und letztlich auch in die Anbieter von Cloud-Diensten."

Mit dem Eckpunktepapier hat das BSI eine gute Basis gelegt, auf der weitere Aktivitäten für eine Schaffung von Mindestsicherheitsstandards beim Cloud Computing aufbauen können. Angesichts der besonderen Eigenschaften der entsprechenden Plattformen, etwa Abstraktion der Ressourcen, Elastizität oder serviceorientierte Architektur, ist die Cloud auch im Rahmen von IT-Grundschutz relevant. Daher erstellt das BSI auch hierfür entsprechende Bausteine wie etwa Cloud-Management, -Nutzung und -Storage sowie Web Services. Darüber hinaus wird der BSI-Standard 100-2 zur Integration von Cloud-Aspekten in die IT-Grundschutz-Vorgehensweise angepasst.

Wolken sind international

Schon per Definition ist Cloud Computing ein Thema, das Grenzen überschreitet und nicht rein national betrachtet werden sollte. Weltweit gibt es daher eine Vielzahl von Initiativen, die sich mit Fragestellungen rund um die Entwicklung neuer beziehungsweise der Weiterentwicklung bestehender Standards beschäftigt. Das BSI beteiligt sich etwa an den EU-Initiativen „Cloud Coordinations Standards" (ETSI) und „European Cloud Partnership" (ECP/C4E). Letztere hat eine Konsolidierung von Vergabeanforderungen des öffentlichen Sektors bei der Beschaffung und Nutzung von Cloud-Computing-Diensten zum Ziel. Durch eine EU-weite

Nutzung gemeinsamer Vergabeanforderungen soll erreicht werden, dass sich kommerzielle Diensteanbieter an die Bedürfnisse des europäischen Sektors anpassen. Das BSI bringt hier vor allem seine Expertise im Bereich der IT-Sicherheitszertifizierung sowie in der Entwicklung von Sicherheitsvorgaben ein. Bei der Entwicklung dieser Vorgaben wird das BSI nicht nur klassische IT-Sicherheitsfragestellungen beachten, sondern auch einen besonderen Schwerpunkt auf die technische Umsetzung von Datenschutzvorgaben legen. Grundlage dazu ist der im Januar 2012 vorgelegte Entwurf zur EU-Datenschutzverordnung.

Ein wesentlicher Erfolgsfaktor der Cloud heute ist Vertrauen: Die Anwender müssen Vertrauen haben in die Sicherheit der Daten, in die Infrastrukturen und letztlich auch in die Anbieter von Cloud-Diensten. Dieses Vertrauen kann jedoch nur entstehen, wenn es unabhängige und transparente Sicherheitsstandards gibt, auf deren Grundlage Plattformen für das Cloud Computing überprüft und zertifiziert werden können. Gemeinsam mit seinen internationalen Partnern sowie Anbietern und Anwendern von Cloud-Lösungen arbeitet das BSI auch weiterhin mit Hochdruck daran, diese zu erstellen und weiterzuentwickeln.

BSI und GDV: Pilotprojekt Cloud-Zertifizierung

In einem Pilotprojekt entwickeln derzeit das BSI und der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) Zertifizierungskriterien für sichere Cloud Services. Der GDV betreibt seit vielen Jahren ein vom BSI zertifiziertes Branchennetz für den sicheren Datenaustausch der Branche mit ihren internen und externen Kommunikationspartnern. Dieses soll durch Nutzung von Cloud-Techniken auch zur Bereitstellung sicherer Services zu einer „Trusted German Insurance Cloud – TGIC“ weiterentwickelt werden. Hierzu wird vom GDV ein „Insurance Security Token Service“ (ISTS) entwickelt. Ziel des GDV ist es, den ISTS nach IT-Grundschutz unter Berücksichtigung der Cloud-spezifischen Bausteine zu zertifizieren sowie aufgrund des hohen Schutzbedarfes zusätzlich einer Common Criteria-Zertifizierung zu unterziehen.

Personenauthentisierung durch Biometrie: Finger oder Fake?

Prof. Markus Ullmann,
Leiter des Referats Technologische Grundlagen sicherer elektronischer Identitäten, Chipsicherheit

Der Fingerabdruck, die Iris im Auge oder die Anlage der Venen in der Hand: Sie alle sind bei jedem Menschen einzigartig und somit unverwechselbare biometrische Merkmale. Über sie lässt sich eine Person eindeutig identifizieren. Daher werden weltweit immer mehr biometrische Systeme gerade dort eingesetzt, wo es um die Authentisierung von Personen geht – beispielsweise beim Zugang zu Gebäuden oder Sicherheitsbereichen.

Die biometrischen Systeme stellen somit eine Alternative zu gängigen wissensbasierten Systemen dar, bei denen man zur Authentisierung etwa ein Passwort verwendet. In diesem Zusammenhang untersucht das BSI biometrische Systeme systematisch auf Schwachstellen und definiert entsprechende Sicherheitsniveaus sowie zugehörige Prüfschemata.

Forschung für die Praxis

In regelmäßigen Bedrohungsanalysen untersucht das BSI, welchem Bedrohungspotenzial aktuelle biometrische Systeme ausgesetzt sind. Hierzu werden u.a. unterschiedliche biometrische Nachbildungen von Gesichtern, Händen oder Fingern (sog. Fakes) erstellt, mit denen dann versucht wird, die biometrischen Systeme zu überwinden. Auf Basis der Testergebnisse werden technische Gegenmaßnahmen entwickelt und erprobt, um automatisch biometrische Fakes von echten menschlichen Merkmalen unterscheiden zu können.

Diese Erkenntnisse alleine erzielen noch keinen Mehrwert. Vielmehr müssen die Hersteller diese Gegenmaßnahmen auch in ihre biometrischen Erkennungssysteme integrieren, ohne dabei die biometrische Erkennungsleistung der Geräte einzuschränken.

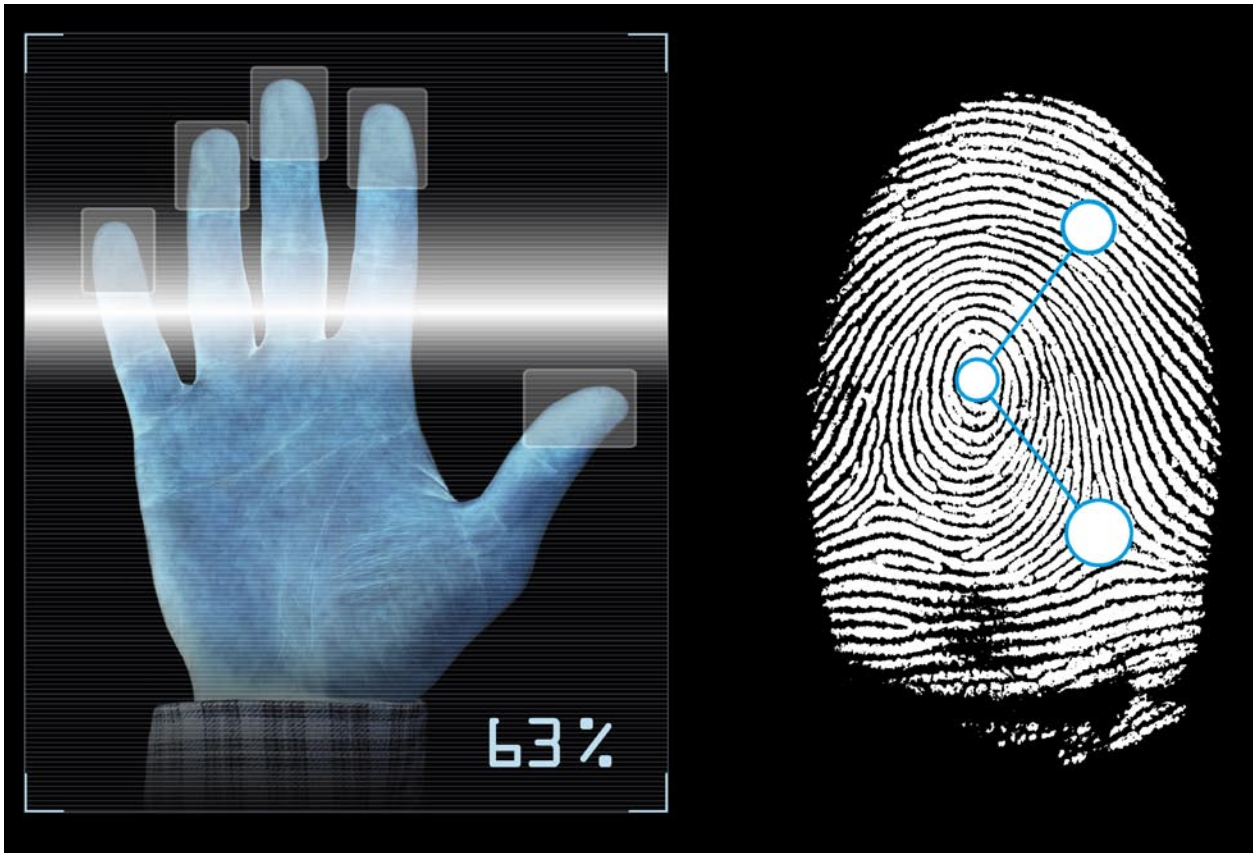
Um die Fake-Erkennungsleistung biometrischer Systeme objektiv ermitteln zu können, hat das BSI auf Basis der eigenen Bedrohungsanalysen und in Zusammenarbeit mit Prüflaboren verschiedene Sicherheitsniveaus definiert und Protection Profiles nach den Common Criteria (CC) entwickelt. Die Sicherheitsniveaus dienen Herstellern als Leitlinie bei der Entwicklung ihrer biometrischen Authentisierungssysteme. Die Prüfschemata ermöglichen eine objektive und unabhängige Evaluation und Zertifizierung der Überwindungssicherheit kommerzieller biometrischer Produkte. So hat das BSI das weltweit erste CC-Zertifizierungskonzept von Fake-Erkennungstechnologien für Fingerbiometrie entwickelt und veröffentlicht.

Fördern und fordern

Werden im hoheitlichen Bereich biometrische Systeme zur Authentisierung eingesetzt, so müssen diese Systeme auf Basis der Technischen Richtline BSI TR-03121 Biometrie in hoheitlichen Anwendungen geprüft werden. Durch die Etablierung dieses Prüfungsprozesses ist es gelungen, sowohl die Entwicklung von biometrischen Authentisierungssystemen mit integrierter Fake-Erkennung zu fördern als auch den Einsatz entsprechend geprüfter biometrischer Systeme zu fordern. Das BSI unterstützt und betreibt anwendungsorientierte Forschung, deren Ergebnisse unmittelbar in die Praxis überführt werden. Dieser Ansatz hat sich in den vergangenen Jahren bewährt.

Im Rahmen der Entwicklung und Weiterentwicklung der Sicherheitsanforderungen arbeitet das BSI eng mit nationalen und internationalen Forschungspartnern, Herstellern von biometrischen Systemen, Systemintegratoren und Anwendern zusammen. So ist das BSI etwa Mitgründer der BVAEG (Biometrics Vulnerability Assessment Expert Group), in der weltweit Institutionen wie das Biometrics Institute oder das National Institute of Standards and Technology ihre Erfahrungen im Bereich Überwindungssicherheit biometrischer Systeme austauschen und gemeinsame Standards schaffen. Darüber hinaus bietet das BSI auch Studierenden im Rahmen von Diplom-, Bachelor- und Masterarbeiten Mitwirkungsmöglichkeiten im Zukunftsfeld der Biometrie. Denn über den gegenwärtigen Schwerpunkt der Fake-Erkennung im Bereich der Fingerbiometrie hinaus weitet das BSI die dort gewonnenen Erfahrungen zukünftig auch auf andere biometrische Modalitäten aus.

Web:
www.bsi.bund.de/Biometrie



Weichen stellen – Zukunft planen

Studienförderung zur Fachkräftegewinnung macht sich bezahlt

Über die Betreuung von Abschlussarbeiten hinaus fördert das BSI inzwischen seit mehreren Jahren Studierende, die sich im Bereich Informatik ausbilden lassen wollen. Studenten, die an der BSI-Studienförderung teilgenommen haben, beginnen nach dem Abschluss eine Tätigkeit beim Bundesamt.

Der Arbeitsmarkt für IT-Fachkräfte ist weiterhin ein enger Markt. Wenige Fachkräfte stehen einer hohen Nachfrage nach sehr gut qualifizierten Informatikern gegenüber. Das BSI begegnet dieser Situation mit einer frühzeitigen Bindung von geeigneten Fachkräften. Durch die Betreuung von Abschlussarbeiten und mittels Studienförderung, bei der der BAföG-Höchstsatz sowie Studien- und Semestergebühren gezahlt werden, ist es bereits gelungen, erste Informatiker ins BSI zu holen.

Der erste Absolvent des Studienförderprogrammes, mit dem neben dem BSI auch das Bundesamt für Verfassungsschutz Nachwuchs rekrutieren möchte, ist Sebastian Cielewicz. Er arbeitet seit dem Abschluss seines Studiums zum Bachelor of Computer Science im BSI-Referat Analyse und Prognose in der Abteilung Cyber-Sicherheit.

Das Interesse an der BSI-Förderung ist jedenfalls hoch: 2012 bewarben sich 49 Studienanwärter für das Stipendium. „Studierende erhalten aktuelle und praxisrelevante Fragestellungen zur Bearbeitung sowie eine gute Betreuung durch BSI-Mitarbeiter. Dadurch tragen Studierende zu den Arbeitsergebnissen des BSI bei und erhalten zugleich Einblicke in die Arbeitsweise des Hauses. Das BSI lernt frühzeitig mögliche neue Mitarbeiter und ihre fachlichen und sozialen Kompetenzen im Rahmen der Bearbeitung von Abschlussarbeiten kennen“, erläutert Prof. Markus Ullmann die Win-win-Situation für das BSI und die Studierenden. Markus Ullmann ist Leiter des Referats Technologische Grundlagen sicherer elektronischer Identitäten, Chipsicherheit.

Auch zum Wintersemsester 2013/14 freuen sich wieder zwei Studierende über finanzielle Unterstützung und fachliche Einblicke.

Martin Reuter,
FH Bonn-Rhein-Sieg

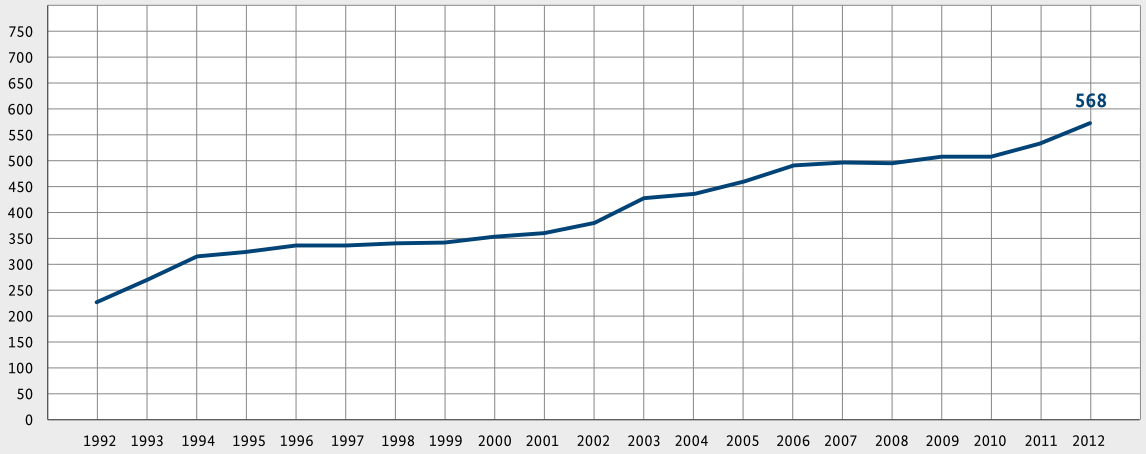
Ich bin bei der Recherche nach Studienmöglichkeiten auf der Internetpräsenz des BSI auf das Angebot der Studienförderung aufmerksam geworden. Besonders positiv an dem Programm ist, dass es nicht nur rein finanziell gestaltet ist, sondern auch Fachkollegen bei thematischen Fragen zur Verfügung stehen. Dies war auch einer der Aspekte, der die Studienförderung für mich sehr interessant gemacht hat. Auch das Praktikum hat mir wirklich sehr gut gefallen. Neben ersten Einblicken in Aufgaben und Tätigkeiten des BSI hatte ich zugleich die Möglichkeit, viele Kollegen kennenzulernen und erste Kontakte zu knüpfen. Gemeinsam mit Christoph Bläßer habe ich bereits im Praktikum ein Projekt bearbeiten dürfen. Es ist mein Wunsch, nach dem Studium im BSI zu arbeiten, da mein großes Interesse der IT-Sicherheit gilt. Das BSI stellt daher für mich den idealen Arbeitgeber dar. In der nächsten Zeit werde ich noch weitere Bereiche des BSI kennenlernen, daher kann ich mich jetzt noch nicht auf einen Bereich festlegen.

Ich bin bereits während meiner Weiterbildung zum staatlich geprüften Techniker auf das BSI aufmerksam geworden. Die Arbeit des Hauses hat mich schon zum damaligen Zeitpunkt interessiert. Im Bewerbungsprozess fand zunächst die Bewertung der Zeugnisse statt, im Anschluss ein Einstellungstest mit abschließendem Bewerbungsgespräch. In erster Linie umfasst die Förderung den finanziellen Aspekt. Darüber habe ich einen sehr guten Kontakt ins BSI, sodass ich bei Fragen direkt die Fachkollegen ansprechen kann. An der FH in Sankt Augustin lehren mit Prof. Markus Ullmann und Dr. Thomas Östreich auch zwei BSI-Mitarbeiter, der direkte Kontakt ist also immer gegeben. Ein Praktikum im Referat von Herrn Ullmann hat mir sehr gut gefallen, da ich mich dabei bereits mit dem Stoff des darauf folgenden Semesters auseinandersetzen konnte – was mir im Nachhinein das Verstehen erleichtert hat. Nach Abschluss des Studiums möchte ich gern im BSI arbeiten. Wo genau? Aufgrund der Vielzahl der Fachreferate bin ich da noch offen.

Christoph Bläßer,
FH Bonn-Rhein-Sieg

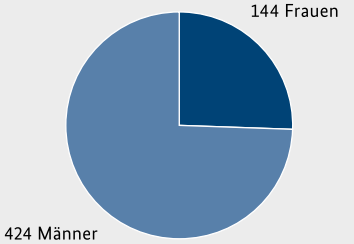
Mitarbeiterstatistik (Stand: 31.12.2012)

Entwicklung der Beschäftigungszahlen im BSI



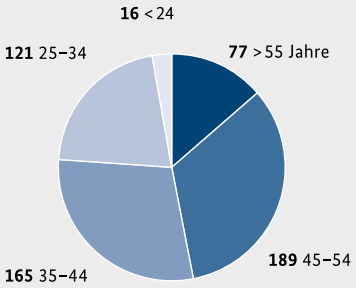
Mitarbeiter

(Stand Ende 2012)



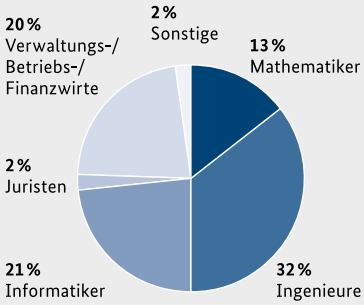
Mitarbeiter gesamt 568

Altersstruktur

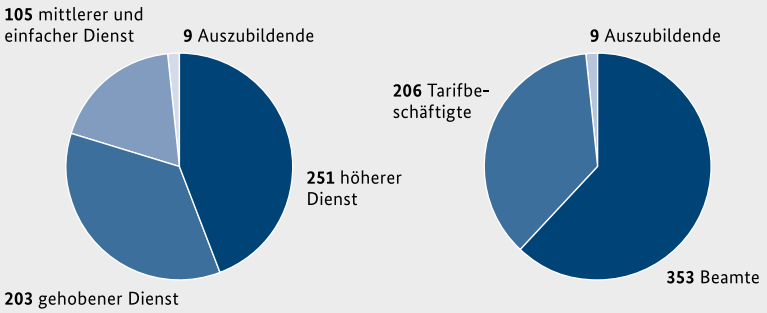


Beruflicher Hintergrund

(nur höherer und gehobener Dienst)



Laufbahnen



Das BSI ist beliebter Arbeitgeber bei IT-Absolventen

Auch im Jahr 2012 ist das BSI wieder unter Deutschlands beliebtesten Arbeitgebern im IT-Bereich. IT-Absolventen wählen das BSI zum wiederholten Mal auf Platz 12, gleich hinter namhaften Firmen wie Google, IBM, SAP und Microsoft.

trendence Graduate Barometer 2012 DEUTSCHLANDS 100 Top-Arbeitgeber IT

Kalender

2011

2012

Februar

8. Februar

BSI für Bürger

Der neu gestaltete Internetauftritt www.bsi-fuer-buerger.de geht online.

8. Februar

Safer Internet Day

Anlässlich des Safer Internet Days 2011 informiert das BSI Verbraucher zum Schwerpunktthema Smartphone-Sicherheit.

13.–18. Februar

RSA Conference 2011

Auf dem von TeleTrust organisierten Gemeinschaftsstand des Bundeswirtschaftsministeriums präsentiert das BSI seine Dienstleistungen und Projekte.

24.–25. Februar

COSADE 2011

In Darmstadt findet der zweite internationale Workshop zur konstruktiven Seitenkanalanalyse und sicherem Design, COSADE 2011, statt – organisiert von CASED und dem BSI.

April

1. April

Nationales Cyber-Abwehrzentrum

Das Nationale Cyber-Abwehrzentrum nimmt im BSI in Bonn seine Arbeit auf. Das Cyber-Abwehrzentrum ist ein Bestandteil der vom Bundesministerium des Innern erarbeiteten Cyber-Sicherheitsstrategie für Deutschland.

12.–13. April

a-i3-Symposium 2011

In Bochum findet das 6. interdisziplinäre Symposium der Arbeitsgruppe Identitätsschutz im Internet (a-i3) und des BSI statt. Im Rahmen der Tagung werden aktuelle Themen aus den Bereichen Infrastruktursicherheit, Identitätsmanagement und Datenschutz umfassend aus rechtlicher und technischer Perspektive beleuchtet.

14. April

Girls' Day 2011

Mädchen in IT-Berufen? Selbstverständlich! Das BSI öffnet in Bonn seine Pforten zum Mädchen-Zukunftstag.

Mai

3. Mai

De-Mail

Das De-Mail-Gesetz tritt in Kraft. Interessierte Anbieter können ab sofort beim BSI die Akkreditierung als De-Mail-Dienstanbieter („De-Mail-Provider") beantragen. Im Rahmen der Akkreditierung müssen alle künftigen De-Mail-Provider nachweisen, dass sie die durch das Gesetz geforderten hohen Anforderungen an die organisatorische und technische Sicherheit der angebotenen De-Mail-Dienste erfüllen.

10.–12. Mai

12. Deutscher IT-Sicherheitskongress

Im Rahmen von sechs Keynotes, 42 Fachvorträgen, einer Podiumsdiskussion zum Thema Cloud Computing sowie einer kongressbegleitenden Ausstellung mit 22 Ausstellern können sich die rund 550 Kongressbesucher aus Wirtschaft, Wissenschaft und Verwaltung in der Stadthalle Bonn-Bad Godesberg drei Tage lang über aktuelle Trends und Themen der Informations- und Datensicherheit informieren.

11.–14. Mai

Linuxtag 2011

Auf dem Linuxtag 2011 in Berlin zeigt das BSI seine aktuellen IT-Sicherheitslösungen auf Basis von Freier, Libre und OpenSource Software („FLOSS")

Kalender 2011

Juni

16. Juni

Nationales Cyber-Abwehrzentrum

Bundesinnenminister Dr. Hans-Peter Friedrich eröffnet das Nationale Cyber-Abwehrzentrum beim BSI in Bonn.

16. Juni

Lagebericht des BSI

Das BSI stellt den Bericht zur Lage der IT-Sicherheit in Deutschland 2011 vor. Auffällig ist die Differenz zwischen Angriffen auf die breite Masse der IT-Nutzer, für die vor allem Standardschwachstellen ausgenutzt werden, und gezielten Cyber-Attacken. Für diese werden bislang unentdeckte Schwachstellen eingesetzt, wie es etwa bei der Schadsoftware Stuxnet der Fall war.

Juli

11. Juli

Neuorganisation des BSI

Zur fachlichen und organisatorischen Fortentwicklung des BSI erfolgt eine Neuorganisation. Der Schwerpunkt liegt bei einer Aufgabengliederung in nunmehr vier Fachabteilungen mit neuen Bezeichnungen: Cyber-Sicherheit; Beratung und Koordination; Krypto-Technologie; Sichere elektronische Identitäten, Zertifizierung und Standardisierung.

August

20.–21. August

Einladung zum Staatsbesuch

Die Bundesregierung lädt unter dem Motto „Einladung zum Staatsbesuch“ in Berlin zum Tag der offenen Tür ein. Das BSI ist mit einem Informationsstand beim Bundesministerium des Innern vertreten. Dort können sich Interessierte über das Serviceangebot des BSI für private Computer- und Internetnutzer informieren. Dabei stehen Themen wie sicheres Surfen im Internet sowie die sichere Nutzung von sozialen Netzwerken im Mittelpunkt.

Kalender 2011

September

5. September

IT-Grundschutz-Überblickspapier

Das BSI veröffentlicht das erste IT-Grundschutz-Überblickspapier. Das Papier zum Thema Smartphones befasst sich mit typischen Gefährdungen der Informationssicherheit bei Smartphones sowie möglichen Gegenmaßnahmen. Mit den Überblickspapieren bietet das BSI ab sofort in loser Folge Lösungsansätze zu aktuellen Themen der Informationssicherheit an, die zu einem späteren Zeitpunkt auch in den IT-Grundschutz eingearbeitet werden.

29. September

12. ICCC

Die 12. ICCC findet in Kuala Lumpur/ Malaysia statt. Die ICCC ist die internationale Diskussionsplattform zu aktuellen Entwicklungen der Common Criteria für Hersteller, Prüfstellen, Anwender sowie Behörden und Zertifizierungsstellen im Common Criteria Anerkennungsabkommen (CCRA).

Oktober

it sa
Die IT-Security Messe und Kongress
The IT Security Expo and Congress

11.–13. Oktober

it-sa

Das BSI ist mit einem Stand auf der Leitmesse für IT-Sicherheit it-sa in Nürnberg vertreten.

12. Oktober

3. IT-Grundschutz-Tag 2011

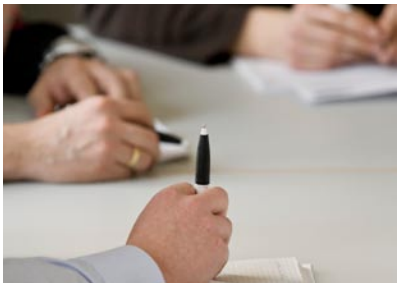
Der IT-Grundschutz-Tag im Rahmen der Sicherheitsmesse it-sa steht in Nürnberg ganz im Zeichen der Weiterentwicklungen des IT-Grundschutzes und vor allem des GSTOOLs.

14. Oktober

Tagung Smart Meter

Im Bundesministerium für Wirtschaft und Technologie findet die erste Tagung zur Entwicklung der Technischen Richtlinie für Smart Meter („Kommunikationseinheit eines intelligenten Messsystems“) statt. Bereits im Vorfeld der Veranstaltung stellte das BSI den Teilnehmern aus den Bereichen Telekommunikation, Energie, Informationstechnik, Wohnungswirtschaft und Verbraucherschutz die erste Fassung der Technischen Richtlinie für die Kommunikationseinheit eines Messsystems zur Verfügung.

November



23. November

5. IT-Grundschutztag 2011

170 IT-Grundschutz-Anwender treffen sich im Bundespresseamt in Berlin zum 5. IT-Grundschutz-Tag 2011, der unter dem Motto „IT-Grundschutz und seine Tools“ steht. Die Veranstaltung findet in Kooperation mit der Firma SerNet statt.

30. November bis 1.Dezember

LÜKEX 2011

Krisenstäbe in Bund, Ländern, Organisationen und Unternehmen üben bei der LÜKEX 2011 (Länderübergreifende Krisenmanagementübung (EXercise)) den Umgang mit IT-Sicherheitsvorfällen. Zusammen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) ist das BSI verantwortlich für die Planung, Vorbereitung, Steuerung und Auswertung der Übung, die 2011 bereits zum fünften Mal stattfindet.

8.–9. November

Moderner Staat 2011

Das BSI präsentiert sein Beratungs- und Produktangebot für Behörden auf der Messe Moderner Staat in Berlin.

Kalender 2011

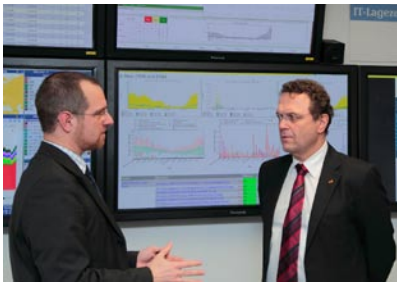
Januar

17.–19. Januar

Omnicard 2012

Das BSI informiert rund um das Thema Sicherheit elektronischer Identitäten auf dem Kongress Omnicard in Berlin.

Februar



3. Februar

BSI-Empfehlungen zur Cyber-Sicherheit

Im Rahmen der neuen Reihe „BSI-Empfehlungen zur Cyber-Sicherheit“ veröffentlicht das BSI ab sofort und in loser Folge zu unterschiedlichen Aspekten der Cyber-Sicherheit allgemeingültige Lösungsvorschläge sowie konkrete Handlungs- und Produktkonfigurationsempfehlungen.

7. Februar

Safer Internet Day

Anlässlich des europaweiten Safer Internet Days veröffentlicht das BSI Empfehlungen zur sicheren Konfiguration von Windows-PCs.

17. Februar

Bundesinnenminister besucht das Lagezentrum

Das IT-Lagezentrum des BSI wurde Ende 2011 modernisiert sowie strukturell und personell vergrößert. Am 17. Februar machte sich Bundesinnenminister Dr. Hans-Peter Friedrich in Bonn selbst ein Bild davon.

27. Februar bis 2. März

RSA Conference 2012

Auf dem von TeleTrust organisierten Gemeinschaftsstand des Bundeswirtschaftsministeriums auf der RSA in San Fransico präsentiert das BSI seine Dienstleistungen und Projekte.

März

2. März

Schwachstellenampel

Mit der Schwachstellenampel bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein neues Angebot im Rahmen seiner Informationsdienste zur Cyber-Sicherheit. Die Schwachstellenampel ist ein Indikator, der die aktuelle IT-Sicherheitslage in Bezug auf Schwachstellen in ausgewählter, gängiger Standardsoftware verdeutlicht.

6.–10. März

CeBIT 2012

Das BSI informiert mit eigenem Stand sowie Pressekonferenz, Vortragsveranstaltungen und Präsentationen auf der CeBIT in Hannover über aktuelle Themen und Entwicklungen in der Internet- und Informationssicherheit.

6. März

De-Mail-Diensteanbieter akkreditiert

Die ersten drei Anbieter von De-Mail-Diensten erhalten auf der CeBIT 2012 in Hannover ihre Akkreditierung durch das BSI. Mentana-Claimsoft GmbH, Telekom Deutschland GmbH und T-Systems International GmbH können nun ihre De-Mail-Dienste Unternehmen, Verwaltungen und Privatpersonen anbieten.

7. März

Allianz für Cyber-Sicherheit

Das BSI und der BITKOM initiieren die „Allianz für Cyber-Sicherheit“. Ziel der Allianz ist eine verbesserte Zusammenarbeit von Staat und Wirtschaft zur Stärkung der Cyber-Sicherheit in Deutschland.

Kalender 2012

April

16.–17. April

a-i3-Symposium 2012

In Bochum findet das 7. interdisziplinäre Symposium der Arbeitsgruppe Identitätsschutz im Internet (a-i3) und des BSI statt. Unter dem Oberthema „Perspektiven und Risiken der digitalen Gesellschaft – ID-Management und Datenschutz für Cloud Computing und IPv6“ werden aktuelle Themen aus den Bereichen Infrastruktursicherheit, Identitätsmanagement und Datenschutz umfassend aus rechtlicher und technischer Perspektive beleuchtet

26. April

Girls’ Day 2012

Beim Mädchen-Zukunftstag Girls’ Day besuchen 24 Schülerinnen das BSI, um Einblicke in technische Berufe und Tätigkeitsfelder zu bekommen. BSI-Experten aus verschiedenen Fachreferaten geben den Besucherinnen Einblicke in ihre Arbeitsbereiche. Neben einem Besuch im nationalen IT-Lagezentrum können die Teilnehmerinnen einen fiktiven Hackerangriff verfolgen und dabei ihre Fragen rund um das Thema IT-Sicherheit stellen.

Mai

15. Mai

Linuxtag 2012

Das BSI ist in Berlin als Aussteller auf dem LinuxTag 2012 vertreten und zeigt aktuelle IT-Sicherheitslösungen auf Basis von Freier, Libre und Open Source Software („FLOSS“). Zudem können sich Messebesucher am BSI-Stand über die Strategie der Behörde in Bezug auf Freie Software sowie über andere aktuelle Themen der IT- und Cyber-Sicherheit informieren.

31. Mai

Fachkonferenz Cyber-Sicherheit

Das BSI richtet in Bonn die Fachkonferenz Cyber-Sicherheit aus. Rund 250 Teilnehmer, darunter CIOs, CISOs, Geschäftsführer, IT-Leiter und IT-Sicherheitsbeauftragte aus Wirtschaft, Verwaltung und Forschung, informieren sich über aktuelle Trends und unterschiedliche Perspektiven der Cyber-Sicherheit. In den Vorträgen, u. a. von der Beauftragten der Bundesregierung für Informationstechnik, Staatssekretärin Cornelia Rogall-Grothe, oder BKA-Präsident Jörg Ziercke, steht die derzeitige Bedrohungslage im Fokus. Das Gleiche gilt für Kooperationsmodelle, aktuelle Lösungen und Best Practices im Bereich der Cyber-Sicherheit.

August

18.–19. August

Tag der offenen Tür der Bundesregierung

Unter dem Motto „Einladung zum Staatsbesuch“ lädt die Bundesregierung interessierte Bürgerinnen und Bürger zum Tag der offenen Tür. Auch in diesem Jahr ist das BSI bei der Veranstaltung in Berlin präsent und zeigte im BMI sein Service- und Informationsangebot für private PC-Anwender.

Kalender 2012

Oktober

16.–18. Oktober

it-sa 2012

Das BSI ist mit einem Stand auf der Leitmesse für IT-Sicherheit it-sa in Nürnberg vertreten. Am BSI-Stand informieren die Sicherheitsexperten des BSI zu zahlreichen Themen der IT- und Informationssicherheit. Das BSI unterstützt gemeinsam mit dem BITKOM die Messe als ideeller Träger.

29. Oktober

Citizen ID Award

Im Rahmen des 11. ID World International Congress wurde das BSI mit dem Citizen ID Award für die erfolgreiche Standardisierung, Implementierung und Zertifizierung des neuen Personalausweises ausgezeichnet.

November

8. November

Allianz für Cyber-Sicherheit

Die „Allianz für Cyber-Sicherheit“ startet als gemeinsame Initiative des BSI und des BITKOM. Sie soll aktuelle Informationen zur Cyber-Sicherheit in Deutschland bereitstellen sowie ein umfassenderes Bild der aktuellen Gefährdungslage ermöglichen. Die Initiative richtet sich an IT- und Sicherheitsverantwortliche in Unternehmen und Organisationen.

13. November

7. IT-Gipfel

In Essen findet der 7. Nationale IT-Gipfel statt. Er steht unter dem Motto „digitalisieren_vernetzen_gründen“. Schwerpunkte bildeten dabei die Themen „junge IT-Unternehmen“, „intelligente Netze“ und „mobile Sicherheit“.

29. November

4. Deutscher IT-Sicherheitspreis

In Darmstadt werden die Gewinner des 4. Deutschen IT-Sicherheitspreises ausgezeichnet. Mit dem alle zwei Jahre verliehenen Preis fördert die Horst Görtz Stiftung unter der Schirmherrschaft von BSI-Präsident Michael Hange die Position von IT-Sicherheit „Made in Germany“.

Dezember

17. Dezember

Schutzprofil in USA und Deutschland

Das BSI und die amerikanische National Information Assurance Partnership (NIAP) veröffentlichen ein gemeinsames Schutzprofil für Betriebssysteme.

4. Dezember

Zertifikat Penetrationstests

Das BSI erteilt das erste Zertifikat für einen IT-Sicherheitsdienstleister im Geltungsbereich Penetrationstests an die HiSolutions AG.

Kalender 2012

Bildnachweise

Titel: Burak Can OZTAS/Thinkstock; Seite 4, 10: Bildschön, Peter Lorenz; Seite 5, 12–14, 16, 18, 19, 21, 25, 29, 30, 32–34, 36, 37, 47, 50, 55, 58, 62, 63, 66–71: Bundesamt für Sicherheit in der Informatiostechnik; Seite 6: Peshkova/Shutterstock, Maksim Kabakou/Shutterstock; Seite 7: Joshua Haviv/Shutterstock, luchunyu/Shutterstock; Seite 8: Maksim Kabakou/Shutterstock; Seite 12: Vladimir Koletic/Shutterstock (oben); Seite 15, 38: robert_s/Shutterstock; Seite 21: Maksim Kabakou/Shutterstock (unten); Seite 22: Peshkova/Shutterstock; Seite 24: gyn9037/Shutterstock; Seite 24: REGIERUNGonline/Kugler; Seite 30: Anteromite/Shutterstock (oben); Seite 37: shironosov/Thinkstock (oben); Seite 40: violetkaipa/Shutterstock; Seite 42: alphaspirit/Shutterstock; Seite 43: Aaron Amat/Shutterstock; Seite 45: Naypong/Shutterstock; Seite 46: Sergey Nivens/Shutterstock (oben); Seite 48: luchunyu/Shutterstock; Seite 50: watcharakun/Shutterstock (oben); Seite 52: Dikiiy/Shutterstock; Seite 53: branislavpudar/Shutterstock; Seite 54: IdeaStepConceptStock/Shutterstock; Seite 56: ra2studio/Shutterstock; Seite 57: David Arts/Shutterstock; Seite 59: Slaven/Shutterstock; Seite 60: Joshua Haviv/Shutterstock

Bundesamt
für Sicherheit in der
Informationstechnik

Mit Sicherheit kein Job wie jeder andere

Wir suchen Sie!

www.bsi.bund.de/jobs

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
53175 Bonn

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Referat B23 – Öffentlichkeitsarbeit und Presse
Godesberger Allee 185–189
53175 Bonn
Telefon: +49 (0) 22899 9582-0
E-Mail: oeffentlichkeitsarbeit@bsi.bund.de
Internet: www.bsi.bund.de

Stand
Juli 2013

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Layout und Gestaltung
media consulta Corporate Publishing GmbH
Wassergasse 3
10179 Berlin

Artikelnummer
BSI-JB 13/603