Bundesamt
für Sicherheit in der
Informationstechnik

Mit Sicherheit

BSI-Magazin 2013/14

Informationssicherheit

für Staat, Wirtschaft und Bürger

ANGRIFFE

Wie gefährdet ist der Cyberraum?

NEUE INITIATIVEN

Das IT-Sicherheitsgesetz

Inhalt

Lehren des letzten Jahres

04 IT-Sicherheit erfordert Kompetenz und Vertrauen
Interview mit Dr. Thomas de Maizière, BMI

10 Digitale Autonomie

Cyber-Sicherheit

12 Wie bedroht ist Deutschlands Cyberraum?

14 Cyberkriminalität
Interview mit Dr. Günther Welsch, BSI
Interview mit Dr. Dirk Häger, BSI

18 SSL-Sicherheit auf Android

19 Allianz für Cyber-Sicherheit
Interview mit Deborah Klein, BDI
Interview mit Peter Rost, Rohde & Schwarz

Die sichere Informationsgesellschaft

22 Elektronische Identitäten

26 Verschlüsselte Gesundheitsdaten

30 Elektronisch bezahlen

32 Sicherheitsberatung

Rahmenbedingungen für IT-Sicherheit

34 Standardisierung

36 Smart Metering

40 Cloud-Computing

42 Industrial Control Systems

46 Kritische Infrastrukturen

Politische Entwicklungen

48 IT-Sicherheit im politischen Raum

51 Das IT-Sicherheitsgesetz

52 IT-Sicherheit und Datenschutz

Das BSI – Aufgaben und Ziele

54 Öffentlichkeitsarbeit im BSI

56 Kontakt zum Nachwuchs
Interview mit René Paegelow, BSI

58 Mitarbeiter des BSI

60 Rückblick 2013/2014

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

Projektleitung: Stephan Kohzer

Stand: Oktober 2014

Texte und Redaktion:
Bundesamt für Sicherheit in der Informationstechnik – BSI

Konzept, Redaktion und Gestaltung:
media consulta Corporate Publishing GmbH, Wassergasse 3, 10179 Berlin

Bildnachweis: Titel: WavebreakmediaMicro/Fotolia; S. 2: T. Linack/Fotolia (o.l.), BSI (u.), Immanuel Giel (o.r.); S. 3: BSI; S. 4: jesussanz/Fotolia; S. 6: Julien Eichinger/Fotolia; S. 8: jesussanz/Fotolia (l.), BDI (r.); S. 10/11: Julien Eichinger/Fotolia; S. 11: BSI; S. 12: vinzstudio/Fotolia; S. 14, 16: peshkova/Fotolia; S. 15: FKIE; S. 17: BSI; S. 18: Bespaliy/Shutterstock; S. 19: vege/Fotolia (o.), BDI (u.); S. 21: vege/Fotolia (u.), Rohde & Schwarz SIT (o., r.); S. 22/23: Julien Eichinger/Fotolia; S. 23: BSI; S. 24: Julien Eichinger/Fotolia (o.), BMI (u.); S. 26: adimas/Fotolia (o.), djama/Fotolia (u.); S. 28: Tomnamon/Fotolia (l.), lanlanlaaa/Fotolia (r.); S. 29: floral_set/Fotolia (o.), gematik (u.); S. 30: robu_s/Fotolia; S. 31: robu_s/Fotolia (o.), BSI (u.); S. 32: Coloures-pic/Fotolia; S. 33: BSI; S. 34/35: Daniel Coulmann/Fotolia; S. 35: BSI; S. 36: weseetheworld/Fotolia; S. 37, 38, 39: Mirscho/Fotolia; S. 38: BSI (u.); S. 39: Coloures-pic/Fotolia; S. 41: BSI; S. 43, 44: Kirill_M/Fotolia; S. 45: BSI (u.); S. 47: Thorsten Schier/Fotolia (o.), BSI (r.); S. 48: Bundesregierung/Bergmann, Guido; S. 50: BSI (l.), eyetronic/Fotolia (r.); S. 51: BSI (r.); S. 53: mapoli-photo/Fotolia, BfDI; S. 54: Wolkenkratzer; S. 55: BSI; S. 56: WavebreakMediaMicro/Fotolia; S. 57: BSI; S. 58/59: Bloomua/Shutterstock; S. 60: BSI (o., m.l., m.r.); S. 61: Sven Hoppe/Fotolia (o.); S. 62: qoqazian/Fotolia (o.), Deutscher Bundestag/Achim Melde (m.l.), Deutsche Messe (m.r.), Stefan Didam (u.l.); S. 63: lohner63/Fotolia

Druck: Druck- und Verlagshaus Zarbock GmbH & Co KG, Sontraer Str. 6, 63086 Frankfurt a.M., Internet: www.zarbock.de

Artikelnummer: BSI-Mag 14/701

Das Magazin ist Teil der Öffentlichkeitsarbeit des BSI.
Es wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

Editorial

Liebe Leserinnen und Leser,
IT-Sicherheitsvorfälle wie die millionenfachen Identitätsdiebstähle und nicht zuletzt die Enthüllungen von Edward Snowden haben das Bewusstsein für das Thema IT-Sicherheit geschärft. Vielen Anwendern in Unternehmen, Behörden und im privaten Bereich ist deutlich geworden, wie anfällig IT-Infrastrukturen sein können und wie sorgsam man mit sensitiven Informationen umgehen sollte.

Die zunehmende Digitalisierung und Vernetzung aller Lebens- und Arbeitsbereiche sowie eine oftmals unzureichend geschützte IT-Sicherheitsinfrastruktur bieten den Kriminellen ausreichend Angriffsmöglichkeiten. Es ist unumstritten, dass in Deutschland permanent Cyber-Attacken stattfinden, um informative oder finanzielle Vorteile zu erlangen. Sowohl staatliche Einrichtungen als auch Wirtschaftsunternehmen und Bürger sind betroffen.

Um dem entgegenzutreten, ist es wichtig, dass eben diese Gruppen sich ihrer Verantwortung bewusst werden. Wir brauchen Lösungen, die die Nutzung von Sicherheitsprodukten alltagstauglich und praktikabel machen. Der bewusste und vorsichtige Umgang mit Informationen muss geschult werden. Aber auch die Schaffung entsprechender Rahmenbedingungen, von der gemeinsamen Definition von Sicherheitsstandards bis hin zu einer möglichen IT-Sicherheitsgesetzgebung, spielt eine gewichtige Rolle.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit seinen derzeit rund 600 Mitarbeitern ist als unabhängige und neutrale Stelle für alle Fragen zur IT-Sicherheit in der Informationsgesellschaft an ebensolchen Prozessen und Gestaltungsmöglichkeiten maßgeblich beteiligt. Mit diesem Magazin möchten wir Ihnen einen Einblick in die vielfältigen Themen und Informationen zu ausgewählten Projekten des BSI geben.

Ich wünsche Ihnen bei der Lektüre viele Einblicke und Denkanstöße rund um das Thema IT-Sicherheit.

Bonn, im Oktober 2014

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Lehren aus den letzten Jahren

IT-Sicherheit erfordert Kompetenz und Vertrauen

Nach der Erschütterung des Vertrauens in die IT-Sicherheit sind neue Schutzmaßnahmen gefragt. Was kann die Politik erreichen? Wo ist jeder Einzelne gefordert?

Das Internet stand in seinen Anfängen einem überschaubaren Nutzerkreis zur Verfügung: Ende der 1960er Jahre bildete es noch einen Computerverbund der Universitäten und Forschungseinrichtungen. Die Förderung durch das US-Verteidigungsministerium brachte die Ausweitung in Schwung. Erst seit den 1990er Jahren kennen wir das Internet als weltumspannendes Netz. Heutzutage führt die IT-Durchdringung und Vernetzung auf vielen Ebenen zur Digitalisierung der Welt. Diese Entwicklung und die heutigen Einsatzszenarien waren ursprünglich nicht absehbar. Das Internet wurde hauptsächlich unter dem Aspekt hoher Verfügbarkeit geplant. IT-Security-by-Design, also der frühzeitige Einbau von vertraulichkeitsfördernden Maßnahmen, war nicht vorgesehen. Durch den weitgehenden Verzicht auf Kryptographie konnten und können Vertraulichkeit und Integrität damals wie heute nicht hinreichend gewährleistet werden. Diese Konstruktionsschwachpunkte stellen unsere Gesellschaft heute vor erhebliche Herausforderungen und liefern den methodischen Ansatzpunkt vieler Cyberangriffe. Der hohe Grad an Anonymität, die geringe Wahrscheinlichkeit, entdeckt zu werden, sowie das fehlende IT-Sicherheitsbewusstsein in der Gesellschaft spielen Cyberkriminellen in die Hände und fördern die Ausnutzung dieser Schwachstellen.

IT-Sicherheit, wo stehen wir?

Deutschland ist permanent Cyberattacken ausgesetzt – mit dem Ziel, einen informativen und finanziellen Vorteil zu erlangen. Betroffen sind alle – staatliche Einrichtungen, Wirtschaftsunternehmen sowie die Bürgerinnen und Bürger. Die Enthüllungen des ehemaligen ›

Geheimdienstmitarbeiters Edward Snowden im Jahr 2013 über die Methoden und Aktivitäten ausländischer Geheimdienste, aber auch weitere IT-Sicherheitsvorfälle wie die millionenfachen Identitätsdiebstähle zum Jahresbeginn 2014 haben dazu beigetragen, dass das Thema IT-Sicherheit verschärft wahrgenommen wird. Die Tatsache, dass staatliche Stellen die Kommunikation überwachen, ist nicht neu. Jedoch haben die Professionalität, das Ausmaß und die Dichte der Überwachungsmaßnahmen sowie der erhebliche Ressourcenaufwand, sowohl personell als auch finanziell, selbst Experten überrascht. Hintertüren in IT-Produkten sind dabei eine Möglichkeit, um in IT-Systeme einzudringen. Mit bekannten, noch nicht gepatchten Schwachstellen und erst recht mit Zero-Day-Exploits-Schwachstellen, die bislang unbekannt sind, lässt sich wirksam in IT-Systeme eindringen, wenn eine Sicherheitslücke nicht rechtzeitig geschlossen wird.

Angesichts dessen stellt sich die Frage, wie der Schutz der Privatsphäre und der Vertraulichkeit gewährleistet werden kann. Das Vertrauen in die eigene (Cyber-)Sicherheit, aber auch in IT-Unternehmen, die laut Snowden partiell mit den Geheimdiensten kooperieren, hat gelitten.

Hürden erhöhen

Die positive Nachricht ist, dass sich etwa 80–90 % der Cyberangriffe einer Kategorie zuordnen lassen, die hinsichtlich ihrer Qualität mit bekannten Standardsicherheitsmaßnahmen abgewehrt werden kann. Rein präventive Maßnahmen sind aber nur ein Baustein, um die Gefährdungslage in den Griff zu bekommen. Konsequente Strafverfolgung im kriminellen Bereich und eine Beobachtung der Aktivitäten fremder Nachrichtendienste sind ebenfalls von großer Bedeutung. Das Ganze muss flankiert werden durch die Schaffung von Rahmenbedingungen, die sich von der gemeinsamen Definition von Sicherheitsstandards bis hin zu einer möglichen IT-Sicherheitsgesetzgebung erstrecken. Im Spannungsfeld zwischen Privatheit und öffentlicher Sicherheit, zwischen der Schutzfunktion des Staates und der Eigenverantwortung des Einzelnen, zwischen staatlicher Regulierung und der Selbstregulierung durch den Markt ist dies eine große gesamtgesellschaftliche Herausforderung. Diese kann nicht von einer gesellschaftlichen Gruppe allein gelöst werden, sondern bedarf einer intensiven Zusammenarbeit auf allen Ebenen von Staat, Wirtschaft und Gesellschaft.

Wirtschaft und Bürger stehen zunächst selbst in der Verantwortung für ihre IT. Durch Angebote, Empfehlungen und Kooperationen leistet das BSI Hilfe zur Selbsthilfe. Ein gutes und erfolgreiches Beispiel ist die Allianz für Cyber-Sicherheit, die als nationale Kooperationsplattform ihren über 1.000 Unternehmen und Mitgliedern Empfehlungen, Good Practices und Lösungen bereitstellt, mit dem Ziel, die Cyber-Sicherheit in Deutschland zu verbessern.

Dort, wo Kooperation und Eigeninteresse nicht ausreichen, sind regulative Vorgaben zu prüfen, um ein ausreichendes Schutzniveau herzustellen. Dies gilt insbesondere für Einrichtungen, die für das Wohl der Gesellschaft unerlässlich sind, die Kritischen Infrastrukturen. Aus IT-sicherheitstechnischer Sicht hat das BSI eine Reihe von zentralen Maßnahmen definiert, die zur Verbesserung der Risikosituation im Cyberraum führen (siehe Darstellung Seite 7).

6-Punkte-Plan

Maßnahmen für alle Zielgruppen

1

Vertrauenswürdige Kryptotechnologie zur Anwendung bringen

Dazu gehört die Implementierung zugelassener Kryptoalgorithmen von vertrauenswürdigen Herstellern. Aber auch die Erhöhung der Nachfrage nach bereits zugelassenen Kryptoprodukten (beispielsweise Kryptohandys/-notebooks/-tablets).

2

Vertrauenswürdige Hersteller und Produkte identifizieren

Notwendig sind transparenzerzeugende Maßnahmen. Ansonsten wird es schwierig, die Einhaltung von Sicherheit, Vertraulichkeit, Integrität sowie Datensicherheit und Datenschutz zu überprüfen. Die Forderung nach Zertifizierung kann eine Maßnahme zu mehr Transparenz sein.

3

Technologische Souveränität

Technische Souveränität ist eine Säule der nationalen Souveränität im Cyberzeitalter. Regulative und sinnvolle Sicherheitsvorgaben sollen die Nachfrage nach Sicherheitsprodukten erhöhen, die Forschung fördern und – damit einhergehend – eine sich selbst erhaltende IT-Wirtschaft in Deutschland etablieren.

4

Den Bürger unterstützen

Der Bürger muss ausführlich und unmittelbar über die Möglichkeiten der sicheren Nutzung von Informations- und Telekommunikationstechnologien informiert und vor Risiken gewarnt werden. Kryptographische Vertrauensanker (z. B. der neue Personalausweis) müssen angeboten werden. IT-Mitarbeiter sind aufgefordert, mehr für die Sicherheit ihrer Kunden durch sichere Verschlüsselung und Authentisierung zu tun.

5

Zielgruppe Wirtschaft

Stärkung der kooperativen Zusammenarbeit (Allianz für Cyber-Sicherheit, UP Kritis), Erfahrungs- und Informationsaustausch, Empfehlungen zu Good Practices und Lösungen. Durch Zertifizierung von IT-Sicherheitsdienstleistern mehr Kompetenz in der Wirtschaft schaffen. Dort, wo keine kooperative Zusammenarbeit ausreicht, ist der Staat in seiner regulierenden Funktion gefordert (IT-Sicherheitsgesetz für KRITIS).

6

Standardisierung und Zertifizierung

Standardisierung ist ein herausragendes Instrument zur Festlegung von Interoperabilitäts- und Sicherheitsanforderungen an moderne IT-Systeme und IT-Dienstleistungen. Standards dienen der Vereinheitlichung und Durchsetzung von Zielen der Informations- und Cyber-Sicherheit. Zertifizierung ermöglicht es, den Bedarf an Dienstleistungen zum Schutz vor Angriffen abzudecken, indem beispielsweise IT-Sicherheitsdienstleister als vertrauenswürdige und kompetente Dienstleister zertifiziert werden.

Vertrauensanker schaffen

In der Zukunft wird es wichtig sein, dem gestiegenen Interesse an Sicherheitsthemen gerecht zu werden und ein umfangreiches Angebot an praktikablen, einfach zu bedienenden Sicherheitsprodukten sowie vertrauenswürdigen Informationsquellen zu schaffen. Vertrauen spielt dabei eine grundlegende Rolle. Unabdingbar dafür ist das Wissen um die funktionierende IT-Sicherheit von Systemen. Hierfür brauchen wir wiederum das Vertrauen in die Akteure – egal ob staatliche Stellen, Hersteller oder Dienstleister.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als unabhängige und neutrale Stelle für alle Fragen zur Sicherheit in der Informationsgesellschaft ist ein solcher Vertrauensanker. Mit der notwendigen fachlichen Kompetenz, der Neutralität im Wettbewerb und der Kooperation mit Wirtschaft und Wissenschaft arbeiten wir auch weiterhin daran, diesem Anspruch gerecht zu werden. Denn eines ist klar: IT-Sicherheit bzw. der Standortvorteil IT-Sicherheit in Deutschland ist keine Einzel-, sondern eine Gesamtleistung.

Schlussendlich haben die Sicherheitsvorfälle und die Enthüllungen von Edward Snowden eine Entwicklung gefördert und dazu beigetragen, die Gesellschaft für das Thema IT-Sicherheit zu sensibilisieren und IT-Sicherheit als wichtiges Gut in das Bewusstsein eines jeden zu rufen. Jeder kann und muss seinen Beitrag zur Erhöhung der Cyber-Sicherheit leisten. Das BSI unterstützt gerne dabei – auch in Zukunft.

Michael Hange,
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Dr. Thomas de Maizière,
Bundesinnenminister

„Sicherheit und Freiheit im Netz"

Herr Minister, Sie haben das Thema „IT-Sicherheit und Sicherheit im Netz" zu einem Kernthema Ihrer Arbeit gemacht. Wo sehen Sie die zentralen Chancen und Risiken der Digitalisierung und welche Rolle spielt Ihrer Meinung nach die IT-Sicherheit?

Der Koalitionsvertrag der großen Koalition greift die IT-Sicherheit und den Schutz der Bürgerinnen und Bürger im Netz prominent auf. Dabei geht es unter anderem um die Stärkung nationaler technologischer Kompetenzen auch im europäischen Verbund, die Beförderung einer vertrauenswürdigen IT- und Netzstruktur sowie auf europäischer Ebene um die Unterstützung eines europäischen Datenschutzrechts. Das Internet und die damit verbundenen Kommunikationstechnologien sind Schlüsseltechnologien der Informationsgesellschaft. Wie wir kommunizieren, Informationen verarbeiten und internationale Geschäfte ausführen, hat sich durch diese zentrale Infrastruktur maßgeblich verändert und verbessert. Die meisten Prozesse und Aufgaben in Unternehmen und der Verwaltung laufen heute IT-gestützt. Wir sind in hohem Maße von funktionierender Informationstechnik und sicheren Informationsinfrastrukturen abhängig. Die Gewährleistung von Sicherheit im Cyberraum und der Schutz der Kritischen Infrastrukturen erfordern daher ein hohes Engagement aller Beteiligten.

Im August 2014 hat das Bundeskabinett die Digitale Agenda verabschiedet. Auf welche Kernziele ist sie ausgerichtet? Und welche Ziele liegen Ihnen besonders am Herzen?

Drei Minister, der Bundesminister für Wirtschaft und Energie, der Bundesminister für Verkehr und digitale Infrastruktur und der Bundesminister des Innern, haben die Digitale Agenda vorgelegt. Das zeigt bereits, wie breit die Agenda angelegt ist. Gemeinsam mit allen gesellschaftlichen Gruppen sollen übergreifende Lösungen zu zahlreichen Fragen der Digitalisierung gefunden werden. Generell verfolgt die Digitale Agenda drei Kernziele. Zunächst soll das Innovationspotenzial unseres Landes für weiteres Wachstum und Beschäftigung stärker erschlossen werden. Zweitens soll der Aufbau flächendeckender Hochgeschwindigkeitsnetze und die Förderung digitaler Medienkompetenz für alle Generationen unterstützt werden, damit jeder einen Zugang erhalten und teilhaben kann. Drittens sollen die Sicherheit und der Schutz der IT-Systeme und Dienste verbessert werden, um Vertrauen und Sicherheit im Netz für Gesellschaft und Wirtschaft stärker zu gewährleisten. Für mich sind Sicherheit und Freiheit im Netz zwei Seiten einer Medaille. In einem breiten Dialog möchte ich ausloten, wie beide Aspekte unter den Bedingungen der zunehmenden Digitalisierung unseres Lebens in Einklang gebracht werden können.

Als eine der ersten Maßnahmen zur Umsetzung der Digitalen Agenda liegt der Entwurf für ein IT-Sicherheitsgesetz vor, der u. a. den Schutz Kritischer Infrastrukturen thematisiert. Was ist Ihre Motivation für den Gesetzentwurf?

Angriffe auf IT-Systeme erfolgen zunehmend zielgerichtet und werden technologisch immer komplexer. Gleichzeitig stellen wir fest, dass ein wirksamer Schutz der IT-Systeme vor Angriffen heute noch nicht in allen Bereichen, die für das Funktionieren unseres Gemeinwesens zentral sind, gleichermaßen gewährleistet ist. Auf Grund des hohen Grades der Vernetzung zwischen den Betreibern Kritischer Infrastrukturen ist dieser Zustand nicht länger hinnehmbar. Hier setzen wir mit dem IT-Sicherheitsgesetz an, das neben einer Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle auch die Einführung verbindlicher Mindeststandards für die IT-Sicherheit Kritischer Infrastrukturen vorsieht. Dem BSI wird eine zentrale Rolle bei der Entwicklung und Anerkennung dieser Mindeststandards zukommen. Außerdem soll das BSI die Betreiber Kritischer Infrastrukturen künftig über Angriffe informieren und sie bei der Sicherung ihrer IT-Systeme beraten. Aber auch in anderen Bereichen wird das BSI mit dem IT-Sicherheitsgesetz neue Aufgaben bekommen.

Der Bürger hat es oftmals schwer, sich gegen immer professioneller agierende Angreifer und die Gefährdungen im Internet zu schützen. Wie kann das BMI und auch die Politik den Bürger unterstützen?

Persönliche Daten bedürfen einer sicheren Verschlüsselung. Dadurch kann sie nur derjenige lesen, für den die Daten bestimmt sind. In der Digitalen Agenda hat sich die Bundesregierung ganz konkret zum Ziel gesetzt, die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden zu lassen. Mit De-Mail haben wir hier ein gutes und sicheres System für die elektronische Kommunikation bereits verfügbar. Hier sind die Anbieter – die „De-Mail-Provider" – verantwortlich für die Sicherheit und sorgen für Verschlüsselung, die verlässliche Identität der Kommunikationspartner und dafür, dass nachgewiesen werden kann, dass die Unterlagen auch unverändert und fristgerecht beim Empfänger angekommen sind. Das BSI prüft regelmäßig die Einhaltung der hohen Sicherheitsstandards der De-Mail. Eine gemeinsame Arbeitsgruppe mit der Wirtschaft soll eine flächendeckende Einführung von De-Mail beschleunigen.

Wichtig ist es auch, anstelle unsicherer Passwortverfahren sichere Authentifizierungsmechanismen zu verwenden, etwa die eID-Funktion des Personalausweises. Behörden und Unternehmen, die eine Nutzung der eID ermöglichen, signalisieren, dass sie größten Wert auf vertrauenswürdige elektronische Dienste legen und dass sie die Daten der Bürger schützen. Je mehr Anwendungsmöglichkeiten es für die eID-Funktion gibt, desto öfter können die Bürger von diesem Schutz profitieren. Deshalb setzen wir uns für den Ausbau des eID-Angebotes ein. Zugleich vereinfachen wir die Nutzung der eID mit einer neuen nutzerfreundlichen Software für den Online-Ausweis.

Neben den staatlichen Schritten, die wir im Rahmen der Digitalen Agenda beschreiten werden, und der Weiterentwicklung der Informationstechnik durch Wirtschaft und Wissenschaft muss aber auch die Überzeugung von der Notwendigkeit und die Aufklärung über die vorhandenen Schutzmöglichkeiten bei jedem Einzelnen einen festen Platz einnehmen.

Der Verein Deutschland Sicher im Netz e. V. (DsiN) leistet hierzu sehr wertvolle Arbeit durch Projekte in Zusammenarbeit mit seinen Zielgruppen – den Bürgerinnen und Bürgern, klein- und mittelständischen Unternehmen sowie Multiplikatoren.

Zum Abschluss: Wo sehen Sie das BSI in fünf Jahren?

Die Entwicklung des BSI wird durch die Umsetzung des IT-Sicherheitsgesetzes einen neuen Schub bekommen. Das BSI soll als internationale Zentralstelle für die Sicherheit in der Informationstechnik und als zentrale Stelle für die Sicherheit der Informationstechnik Kritischer Infrastrukturen etabliert werden. Das BSI wird die Befugnisse bekommen, alle auf dem Markt befindlichen Produkte im Hinblick auf die Sicherheit untersuchen und bewerten und die Ergebnisse veröffentlichen zu können. Das BSI wird in den nächsten Jahren die zentrale Instanz für die Sicherheit in der Informationstechnik in Deutschland.

Digitale Autonomie

Informationen im Netz sichern

Im Netz unbeobachtet und unabhängig bleiben – wie lässt sich dieser Wunsch nach einer „Digitalen Autonomie“ umsetzen?

Mit der Digitalisierung unterschiedlichster Bereiche des menschlichen Handelns und Wirtschaftens, von der Schrift und der Sprache über Automobil-, Maschinen- und Energietechnik bis hin zur Medizintechnik, werden essenzielle Handlungen des Privatlebens zum Gegenstand technologischer Entwicklung. Zusammen mit der umfassenden Vernetzung der zugrunde liegenden IT-Technik entsteht so das oft zitierte „Internet der Dinge“.

Gleichzeitig wird in diesem Netz aber jegliches digitalisierte Datum in einer völlig neuen Art und Weise exponiert: Dort, wo früher ein Brief über wenige Postämter (!) befördert oder Kommunikation über eine eindeutig definierte Folge von Vermittlungsämtern (!) geführt wurde, wird heute eine aus Anwendersicht weitgehend unübersichtliche Netzinfrastruktur genutzt. Diese Exposition gilt spätestens seit dem Siegeszug des Smartphones auch für meinen Aufenthaltsort und jeden Aspekt meines digitalisierten und vernetzten Lebens. Wie in diesem Jahresbericht vielfach dargestellt, wirken auf dieses Netz verschiedene nachrichtendienstliche und kriminelle Gefährdungen. Allen Gefährdungen ist aber gemein, dass sie letztlich auf die Vertraulichkeit und Verfügbarkeit der Daten und der Kommunikation, auf die Überwindung der Schutzmechanismen der verwendeten IT-Systeme und – das ist im Bewusstsein vieler die neue Erkenntnis nach Snowden – auf die persönliche Präsenz im Netz zielen.

Unabhängig und unbeobachtet

Die Konsequenz aus dieser Erkenntnis sind die vielfältigen Forderungen nach „Unabhängigkeit und Unbeobachtbarkeit“ im Netz: Ende-zu-Ende-Verschlüsselung, Anonymisierung, Schengen-Routing, technologische Souveränität. Alle Ideen streben nach einer klaren Kontrolle von Ort, Besitz und Schutz von Daten und Kommunikation sowie einem umfassenden Wissen über die genutzten Infrastrukturen, IT-Produkte und IT-Dienstleistungen sowie über ihre Informationssicherheit. Diesen angestrebten Zustand möchte ich als „Digitale Autonomie“ bezeichnen.

Zielkonflikte

Einer „Digitalen Autonomie“ in diesem weit gefassten Sinn ist von vornherein eine ganze Reihe von Zielkonflikten inhärent: Hier nur wenige Beispiele:

- Nutzer exponieren in vielen Fällen ihre Daten freiwillig (z. B. Google-Suche, Facebook) und „zahlen“ mit ihren Daten für die angebotenen Dienste,
- verschlüsselte Kanäle schützen ggf. die durch sie transportierte Schadsoftware und so illegales Handeln im Netz,
- starker Schutz geht bei aktuellen Produkten mit unhandlicher Nutzung einher.

Die Realisierung der „Digitalen Autonomie“ erfordert die Lösung anspruchsvoller technischer Herausforderungen: Starke Kryptographie ist zwar zum Schutz der Vertraulichkeit verfügbar, das Ziel muss aber eine transparente Nutzbarkeit und eine weite Verbreitung in einer geeigneten Vertrauensinfrastruktur sein. Auch Cyber-Sicherheitsmechanismen stehen zur Verfügung, angesichts der immensen Zahl von Schwachstellen von Hard- und Software sowie der hohen Erfolgsrate von Angriffen müssen aber Security by Design und Security by Default erst zum Standard heranwachsen.

Die größte Herausforderung stellt der Schutz der „Präsenz im Netz“ dar: Grundsätzliche, strukturelle Änderungen in der heutigen Netz- und IT-Architektur sind gefordert, um durchgreifende Verbesserungen der Sicherheitslage zu erreichen. Hier können nur internationale Anstrengungen in Forschung, Entwicklung und Standardisierung Fortschritte bewirken. Bis dahin bleiben für den Schutz des Bürgers Sensibilisierung und Bildung vorrangig.

Was unternimmt das BSI?

Die Aufgabe des Staates und seiner Institutionen ist die Herstellung von Vertrauen durch Transparenz. Dies geschieht vor allem durch

- die Bereitstellung öffentlicher und standardisierter Krypto- und Cybermechanismen,
- die Förderung und Kennzeichnung vertrauenswürdiger Hersteller, Produkte und Dienstleistungen, die Beförderung der internationalen Anstrengungen für eine sichere globale Netzinfrastruktur sowie vor allem durch
- die Moderation eines öffentlichen Diskurses zur Diskussion der gesellschaftlichen Zielkonflikte einer „Digitalen Autonomie“. □

Andreas Könen,
Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik

Wie bedroht ist Deutschlands Cyberraum?

Täglich werden
2.000–3.000
Angriffe auf die Netze des Bundes registriert, darunter 3–5 gezielte.

1,7 Mio.
neue mobile Malware auf Android (2013) – jeden Monat kommen 250.000 hinzu.

Werkzeuge
für Cyberangriffe
kosten nur
5 USD
pro Stunde.

Jede 40. Website ist infiziert

Manipulierte Werbebanner verbreiten Drive-by-Exploits – täglich 500.000 weltweit. Allein durch den Besuch einer solchen Website kann der Rechner infiziert werden.

BSI

100.000 Abonnenten beziehen Informationen vom Bürger-CERT.

Der Warn- und Informationsdienst des BSI erteilt monatlich
100 Empfehlungen und
200 Kurzinformationen.

Gezielte Cyber-Spionage (Advanced Persistant Threats) wird im Schnitt nach
243 Tagen
entdeckt.

Cyberkriminalität

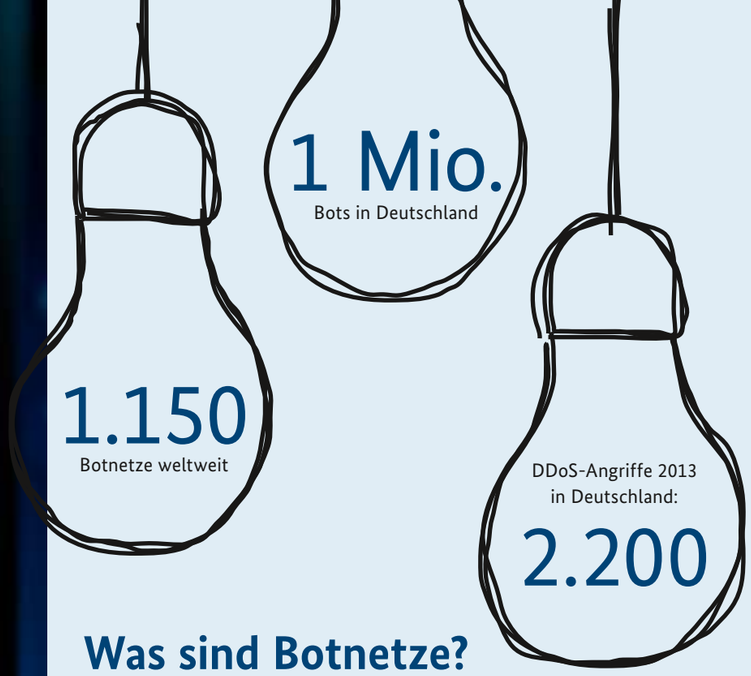
Licht ins Dunkel bringen

In den letzten Jahren hat sich Cyberkriminalität zu einem signifikanten Problem entwickelt. Wie groß ist die Gefahr? Und wie kann Forschung helfen?

Wegen der großen Dunkelziffer sind die tatsächlichen Ausmaße von Cyberkriminalität zwar unbekannt, doch lassen publik gewordene Einzelfälle die enorme Größenordnung der Schäden erahnen. Insgesamt gestaltet sich die Aufklärung und Strafverfolgung von Cyberangreifern als äußerst schwierig. Neben der technischen Komplexität tragen auch die Multinationalität des Phänomens und die unterschiedlichen Rechtssysteme betroffener Länder zur Komplexität der Problematik bei. Im Rahmen der BOTMAN®-Aktivitäten (BOTnet & Malware ANalysis) entwickeln Forscher des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) Prozesse und technische Lösungen, um dem Phänomen Cyberkriminalität begegnen zu können. Dazu wurden Prozesse definiert, um mit ganzen Projektteams kooperativ Schadsoftware analysieren und kriminelle Infrastrukturen aufklären zu können. Passend zu diesen Prozessen sind technische Werkzeuge zur effizienten Analyse von Schadsoftware, zur Konzeption und zum Test von Gegenmaßnahmen, der Warnung von Betroffenen und der Ermittlung durchgeführter Straftaten sowie zur Erfassung von Täterhinweisen entstanden. □

Prof. Dr. Peter Martini, Leiter Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE)

Dr. Elmar Gerhards-Padilla, Leiter Forschungsgruppe Cyber Analysis (FKIE)



Was sind Botnetze?

Botnetze sind Netzwerke aus infizierten Systemen (Bots), die von Cyberkriminellen ferngesteuert werden können. Informationsdiebstahl, Spamversand, Distributed-Denial-of-Service-Angriffe (DDoS), Bitcoin Mining oder gezieltes Ausbringen weiterer Schadsoftware auf den Bots sind nur einige der Zwecke, für die Botnetze von Kriminellen eingesetzt werden.

Weitere Bestandteile solcher kriminellen Infrastrukturen sind häufig spezielle Server für die Auslieferung von Schadsoftware, Systeme für die Anonymisierung der Täter sowie Systeme für die Verwaltung von Mittätern und Geldflüssen. Insbesondere bei der Anonymisierung wird meist eine ganze Kette von Systemen durch die Kriminellen eingesetzt, um die Ermittlung von Identitäten möglichst zu erschweren.

Schäden durch Cyberangriffe

500 Mio.
USD Schaden (für Privatpersonen) durch Online-Banking-Trojaner Citadel im Jahr 2013 weltweit (Quelle: Microsoft)

1,1 Mio.
USD jährliche Einnahmen für Betreiber des weltweit aktiven Schadnetzwerks Bamital zwischen 2009 und 2013 (Quelle: Symantec)

42,5 Mio.
EUR* Gesamtschaden im Jahr 2012 durch Cybercrime in Deutschland (Quelle: BKA)

* nicht alle Delikte erfasst, große Dunkelziffer

INTERVIEW

„GEGEN DIE KRÄMER SEELE IN UNS“

Wie hat sich seit den Veröffentlichungen Snowdens die Wahrnehmung von Sicherheitsthemen verändert?

Firmen, Organisationen und Behörden fragen kritischer nach und sind auch bereit, ihr bisheriges Handeln unter IT-Sicherheitskriterien zu reflektieren. Beispielsweise bezieht das BMI zukünftig IT-Dienstleistungen verstärkt von vertrauenswürdigen Anbietern. Die Bürger sollten verinnerlichen, dass sie sehr wohl einiges für die eigene IT-Sicherheit und den Schutz ihrer Daten tun können. Denn jede Sicherheitsmaßnahme erschwert Internet-Kriminellen den missbräuchlichen Zugriff auf IT-Systeme und Daten.

Welche Entwicklungen sehen Sie auf die Menschen zukommen?

Die Vernetzung nimmt mittlerweile lawinenartig zu. Die Digitalen Infrastrukturen von heute waren vor 30 Jahren nur als Utopien denkbar. Das Internet der Dinge, die „Fabrik der Zukunft“ und die schrankenlose Vernetzung von Informationen und Systemen in allen Lebensbereichen werden unsere Begleiter in der voll digitalisierten Welt. Wir stehen somit vor einer gewaltigen Transformation unserer industriellen Wirtschaft und der Zivilgesellschaft.

Und in wirtschaftlicher Hinsicht?

Ein neues globales Wettrennen hat begonnen, bei dem es nun darum geht, wer am besten die konventionellen Wirtschafts- und Industriebereiche digitalisiert. Hier entscheidet sich auch die Zukunft Deutschlands. In klassischen Industriebereichen sind wir stark. Aber IT-Unternehmen drängen mit großer wirtschaftlicher und innovativer Kraft in unsere Kernkompetenzen ein. Durch die Digitalisierung entstehen neue dynamische Geschäftsmodelle, und klassische Industrieprodukte differenzieren sich in Zukunft über Mehrwerte, die durch Vernetzung und Digitalisierung entstehen. Wollen wir im Wettbewerb mithalten, geht es darum, jetzt die Cyber-Technologien schnell, funktionell überzeugend und insbesondere mit guter IT-Sicherheit zu integrieren. Deutschland ist ein starkes Ingenieurland mit großem Know-how in der IT-Sicherheit. Dies müssen wir zu unserem Vorteil ummünzen.

Welches sind für Sie die zentralen Themen, die es in den nächsten Jahren anzugehen gilt?

Wir müssen IT-Systeme und IT-Geschäftsmodelle im Internet fordern, die eine größere inhärente IT-Sicherheit aufweisen. Es wird darum gehen, wie die Nachfrage besser organisiert werden kann. Nur wenn IT-Sicherheit als differenzierendes Element im Wettbewerb wahrgenommen wird, kann man mit einer deutlichen Verbesserung rechnen. Solange aber die Krämerseele in uns lieber das günstigere Gerät bevorzugt, statt das zu wählen, das mehr Sicherheit bietet, aber auch teurer und weniger ergonomisch ist, wird der Markt sich nicht ändern. Dem BSI kommt hier auch die Aufgabe zu, für Bewusstsein zu sorgen und gemeinsam mit interessierten Unternehmen nachzuweisen, dass Produkte mit guter Funktionalität auch sicher sein können.

Dr. Günther Welsch,
Fachbereichsleiter
„Koordination und Steuerung“

„VERANTWORTUNG FÜR ALLE“

Wer trägt welche Verantwortung im Kampf gegen Cybergefahren?

Als Gesellschaft müssen wir Kindern, Jugendlichen und Erwachsenen Medienkompetenz vermitteln. Ein jeder hat eine eigene Verantwortung und Pflicht, sich im Rahmen seiner Möglichkeiten technisch zu schützen. Dies gilt umso mehr für Betreiber von wichtigen IT-Infrastrukturen und für Hersteller von IT-Systemen. In Zukunft muss es gelingen, IT-Systeme mit deutlich weniger Schwachstellen und Verwundbarkeiten zu entwickeln, denn diese sind der Quell für die meisten schadhaften Aktivitäten im Internet. Der Staat muss ein Mindestmaß an IT-Sicherheit durchsetzen, wenn das normale Marktgeschehen nicht für ausreichende Sicherheit sorgt, und er muss kriminelle Aktivitäten konsequent verfolgen. Im Zeitalter der Globalisierung ist das natürlich eine Herausforderung im internationalen Umfeld.

Wie sollten Privatpersonen ihre Privatsphäre schützen?

Jeder sollte sehr sparsam sein mit der Preisgabe von persönlichen Daten im Internet. Insbesondere bei angebotenen Vergünstigungen (Rabatten) im Gegenzug zur Preisgabe von persönlichen Informationen ist Vorsicht geboten.

Welche Aufgaben sehen Sie in Zukunft auf das BSI zukommen?

Das BSI genießt eine große Reputation in Fragen der IT-Sicherheit in Deutschland und darüber hinaus. Was das BSI empfiehlt und wovor es warnt, hat in der Öffentlichkeit und Fachöffentlichkeit Bedeutung. Diesen Ruf müssen wir erhalten und ausbauen. Das heißt auch, die richtigen Schwerpunkte zu setzen, denn auch die Ressourcen des BSI lassen nur die Bearbeitung der prioritären Herausforderungen der IT-Welt zu.

Dr. Dirk Häger,
Fachbereichsleiter
„Operative Netzabwehr“

SSL-Sicherheit auf Android

Probleme aufgedeckt

Nutzer, Administratoren und Entwickler stolpern über die SSL-Verschlüsselung – das belegen Untersuchungen am Fraunhofer FKIE.

Mit einem Marktanteil von über 80% ist Android das meistgenutzte Betriebssystem für Smartphones. Die Mehrheit aller Android-Apps hat einen legitimen Grund, Daten mit dem Internet auszutauschen. Allerdings sind diese Apps damit auch für den Schutz von sensiblen Nutzerdaten verantwortlich. Der Secure Sockets Layer (SSL) und sein Nachfolger, die Transport Layer Security (TLS), sind Verschlüsselungsprotokolle, die zum Schutz der Netzwerkkommunikation vor Abhören und Manipulation eingeführt wurden. Forscher am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) haben zahlreiche und gravierende Probleme in der praktischen Umsetzung aufgedeckt, und zwar sowohl bei Entwicklern und Administratoren als auch bei Benutzern. Entwickler sind etwa bei der Programmierung der SSL-Bibliotheken häufig überfordert. In einer Studie zu 13.500 Android-Apps wurden zahlreiche Apps mit unsicheren SSL-Verbindungen gefunden. Fast 20% der untersuchten Apps mit SSL enthalten potenziell unsicheren Code, darunter Anbieter wie American Express, Diners Club, Paypal, Facebook, Twitter, Microsoft Live ID, Remote-Server, Bankkonten und Mailaccounts. Insgesamt lag die Anzahl der Installationen dieser Stichprobe nach Angaben des Google Play Markets schon zwischen 39,5 und 185 Millionen Nutzern. Wenige Entwickler gefährden somit Millionen von Nutzern.

Aber auch Administratoren haben Probleme mit SSL: Forscher des FKIE haben für eine weitere Studie über 8.000 Administratoren von Webseiten mit fehlerhaften SSL-Zertifikaten kontaktiert. Die in der Folge befragten 755 Teilnehmer begründeten die Fehler vor allem mit der Komplexität der Konfiguration, mit Kosten und mit mangelndem Vertrauen in Certification Authorities.

In einer weiteren Studie wurde untersucht, ob Benutzer eine reguläre HTTP- überhaupt von einer HTTPS-Verbindung auf Android unterscheiden können und ob sie eine SSL-Warnung wahrnehmen. Die Mehrheit der Teilnehmer (darunter 57,6% Nichtexperten und 52,3% IT-Experten) gab an, noch nie eine Android-Zertifikats-Warnung gesehen zu haben. 24,0% der Teilnehmer lasen die Warnung nur teilweise und 4,5% gar nicht. Bezüglich der Sicherheit der SSL-Verbindung zeigten die Ergebnisse, dass 47,5% der Nichtexperten glaubten, eine sichere Verbindung zu nutzen, obwohl die Befragung über HTTP durchgeführt wurde. Darüber hinaus gaben sogar 34,7% der Teilnehmer mit IT-Expertise an, einen sicheren Kanal zu nutzen, obwohl dies gar nicht der Fall war. Nur 58,9% der Experten und 44,3% der Nichtexperten identifizierten die Verbindung korrekterweise als sicher bzw. unsicher.

Insgesamt sollte das gesamte SSL-Ökosystem überdacht werden, um es transparenter und menschengerechter zu gestalten. Forscher in der Usable Security & Privacy Group am FKIE haben bereits erste Lösungsvorschläge entwickelt, aber es ist noch viel Arbeit erforderlich, um menschengerechte Sicherheitslösungen zu entwickeln und am Markt zu etablieren. □

Prof. Dr. Matthew Smith,
Fraunhofer FKIE

Prof. Dr. Peter Martini,
Leiter Fraunhofer FKIE

Allianz für Cyber-Sicherheit

Gemeinsam gegen Angriffe

Seit der Gründung der „Allianz für Cyber-Sicherheit“ im Jahr 2012 durch das BSI und BITKOM steigt ihre Bedeutung stetig.

Inzwischen hat die Allianz mehr als 1.000 Teilnehmer mit steigender Tendenz. Täglich kommen weitere Institutionen, Verbände und Unternehmen hinzu – darunter sind sowohl DAX-Unternehmen als auch KMU. Die Allianz bietet den Unternehmen ein umfangreiches Informationsangebot mit Empfehlungen, Analysen und monatlichen Lageeinschätzungen zur Cyber-Sicherheit sowie vielfältigen Möglichkeiten zum Erfahrungsaustausch. Unternehmen können IT-Sicherheitsvorfälle anonym und unbürokratisch der Meldestelle der Allianz mitteilen. □

INTERVIEW

„AUFMERKSAMKEIT STÄRKEN“

Wie beurteilen Sie die Gefahr von Cyberangriffen auf die Industrie?

Die digitale Vernetzung ist ein Wettbewerbsfaktor für die deutsche Industrie. Neben den zahlreichen Chancen sind damit aber auch Risiken verbunden. Das Aufbrechen der Firmengrenzen, die Verflechtung mit Zulieferern und Dienstleistern sowie die starke Nutzung drahtloser Kommunikation erleichtern Angriffe auf IT-Systeme in den Unternehmen. Der potenzielle Schaden von Cyberangriffen ist enorm. Zeitlich unabhängig voneinander und grenzüberschreitend greifen kriminelle Organisationen und ausländische Nachrichtendienste zigtausendfach deutsche IT-Strukturen an. Daten werden oftmals unentdeckt entwendet, manipuliert oder ausgespäht und technische Systeme sabotiert. Die Ausfälle bei den Unternehmen aufgrund von Cyberangriffen haben weitreichende Folgen: Die jährlichen Schäden für unsere Unternehmen schätzen Sicherheitsexperten auf einen zweistelligen Milliardenbetrag. Die Dunkelziffer ist dabei um einiges höher.

Deborah Klein,
Referentin IT-Sicherheit in der Abteilung „Sicherheit und Rohstoffe“ beim Spitzenverband BDI

Welche Tendenzen beobachten Sie bei den Angreifern?

Neben der steigenden Zahl der Cyberangriffe ändern sich vor allem die Art und Weise, wie Unternehmen Angriffen ausgesetzt sind, und die Geschwindigkeit, mit der neue Viren entstehen und verbreitet werden: Alle zwei

INTERVIEW

Sekunden wird ein neues Schadprogramm entwickelt. Angriffe werden heute gezielt durchgeführt und richten sich auf Unternehmen, Staaten oder das Militär. Betroffen sind verstärkt mittelständische Unternehmen.

Wo sehen Sie den größten Handlungsbedarf?

Besonders mittelständische Unternehmen müssen für das Thema Cyber-Sicherheit weiter sensibilisiert werden. Auch bei der technischen und personellen Ausstattung der kleinen und mittleren Unternehmen (KMU) im Bereich Cyber-Sicherheit besteht noch Handlungsbedarf.

Welche Maßnahmen empfehlen Sie?

Zwar gibt es keine absolute Sicherheit, wir können aber die Hürden für Angreifer höher legen. Mit präventiven Maßnahmen und nicht zuletzt mit zuverlässigen IT-Sicherheitstechnologien können die Unternehmen ein hohes Maß an Sicherheit erreichen. Nur wer rechtzeitig über die Gefahrenpotenziale informiert ist, kann geeignete Gegenmaßnahmen einleiten. Dazu gehört, die Aufmerksamkeit der Unternehmen für mögliche Gefahren im Bereich Cyber-Sicherheit zu stärken und rechtzeitig über Gefahrenpotenziale zu informieren, um geeignete Maßnahmen zu ergreifen. Freiwillige Initiativen wie die „Allianz für Cyber-Sicherheit“ leisten einen wichtigen Beitrag.

Welche Bedeutung hat in diesem Zusammenhang die „Allianz für Cyber-Sicherheit“?

*Cyber-Sicherheit ist eine gesamtgesellschaftliche Aufgabe. Die nachhaltige Stärkung der IT-Sicherheit von Infrastrukturen muss ein gemeinsames Ziel von Industrie, Politik und Gesellschaft sein. Ein sehr gutes Beispiel dafür, wie eine solche Zusammenarbeit erfolgreich funktioniert, ist die „Allianz für Cyber-Sicherheit“. Politik und Industrie arbeiten Hand in Hand beim Schutz vor Cyberangriffen. In konkreten Fällen kann so schnell und effizient ein breites Netzwerk aktiviert werden. Die Unternehmen wünschen sich eine aktive Informationspolitik des BSI in Form von praktischen Erfahrungen bei der Prävention oder der Abwehr von IT-Sicherheitsvorfällen. Dies macht die aktuelle Studie „IT-Sicherheit in Deutschland. Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes“ (**www.bdi.eu/Sicherheit.htm**) deutlich. Diese hat der BDI gemeinsam mit seinen Mitgliedsverbänden BDLI, BDSV, BITKOM und ZVEI bei KPMG in Auftrag gegeben.*

Wie steht der BDI zur Allianz?

Der BDI unterstützt die Arbeit der Allianz seit Beginn an. Das Ziel der Allianz, die Zusammenarbeit und den Informationsaustausch zwischen Unternehmen und Behörden auf freiwilliger Basis zu fördern, hält der BDI für richtig. Als Multiplikator möchte der BDI Unternehmen und Mitgliedsverbände auf die Arbeit der Allianz aufmerksam machen. Aktuell unterstützt der BDI die „Cyber-Sicherheits-Umfrage der Allianz“. Im Beirat vertritt der BDI die Interessen der deutschen Industrie hochrangig innerhalb der Allianz. Der BDI ist außerdem überzeugt, dass der Grundsatz der Freiwilligkeit der richtige Ansatz ist.

www.bdi.eu/IT-und-Cybersicherheit.htm

Allianz für Cyber-Sicherheit

Die Allianz in Zahlen

1.004
teilnehmende Unternehmen (Stand Oktober 2014)

1.605
teilnehmende Mitarbeiter (Stand Oktober 2014)

30
Veranstaltungen zum Thema Cyber-Sicherheit im 1. Halbjahr 2014

161.322
Besucher auf der Website www.allianz-fuer-cybersicherheit.de im 1. Halbjahr 2014

Die minimale Latenzzeit und die Multipunkt-Verschlüsselung des Netzwerkverschlüsselers des Herstellers Rohde & Schwarz gehen auf Anregungen von Allianz-Teilnehmern zurück.

„IDEE ZUR RECHTEN ZEIT“

Welchen Vorteil ziehen Sie ganz konkret aus der Allianz für Cyber-Sicherheit?

Für uns war die Möglichkeit attraktiv, uns nicht nur mit den Sicherheitsbehörden und der IT-Sicherheitsforschung auszutauschen, sondern verstärkt auch mit privatwirtschaftlichen Anwendern über konkret benötigte technische Lösungen und deren Anforderungen aus dem täglichen Betrieb. Der Erfahrungsaustausch mit den Allianz-Teilnehmern erleichtert es uns, Verschlüsselungslösungen so zu gestalten, dass sie den operativen Netzwerk- und Produktionsbetrieb der Anwender nicht merkbar beeinträchtigen und dennoch deren Schutzniveau deutlich erhöhen. Auf den Teilnehmertagen der Allianz für Cyber-Sicherheit fanden wir neben inspirierenden Referaten immer gute Gelegenheiten, Ideen und Erfahrungen auszutauschen.

Peter Rost
Rohde & Schwarz SIT, langjähriger Lieferant von Verschlüsselungstechnik für den hoheitlichen Einsatz

Konnten Sie auch selbst einen Beitrag leisten?

Schon seit Mitte 2012 begleiten wir die Initiative mit dem Ziel, als Partner unseren Beitrag zur Verbesserung der Cyber-Sicherheit unter den Teilnehmern der Allianz zu leisten. Wir haben z. B. im Herbst 2013 eine „Checkliste Netzwerksicherheit“ als Partnerbeitrag erstellt. Zum gleichen Thema, also zur sicheren und effizienten Vernetzung von Standorten sowie zur abgestuften Sicherheit durch die Einrichtung von Netzwerk-Zonen, haben wir auch Tagesseminare veranstaltet.

Wie bewerten Sie den Stellenwert der Allianz für Cyber-Sicherheit?

Die Allianz für Cyber-Sicherheit hat in den vergangenen zwei Jahren eine beeindruckende Erfolgsstory hingelegt: Steil wachsende Teilnehmerzahlen und insbesondere das zunehmende Multiplikatoren-Netzwerk sprechen eine deutliche Sprache. Die Idee, in Deutschland eine Plattform für den vertraulichen Austausch über praktische Aspekte der Cyber-Sicherheit zu schaffen, kam zur rechten Zeit. Die Allianz für Cyber-Sicherheit ist ein wesentlicher Baustein zur Verbesserung des IT-Schutzniveaus in Deutschland. Wir sind gerne darin Partner und freuen uns auf die nächsten gemeinsamen Schritte.

Elektronische Identitäten

Werkzeuge fürs Netz

De-Mail und der Personalausweis mit seiner Online-Ausweisfunktion sind Schwerpunkte der E-Government-Initiative des BMI und wesentliche Aufgabenbereiche beim BSI.

Grundlage für unser Handeln im Internet sind elektronische Identitäten, nicht nur im Bereich des E-Governments, sondern auch im E-Commerce. Unsere Aufgaben als zentraler Dienstleister für Informationssicherheit in Deutschland sind einerseits die Entwicklung und Bereitstellung, andererseits die Analyse und Bewertung sicherer eID-Technologien (d. h. Technologien für die Gewährleistung elektronischer Identitäten) in enger Kooperation mit Verwaltung, Wirtschaft und Forschung, um vertrauenswürdiges, authentisches und rechtsverbindliches Handeln im Internet zu ermöglichen und Identitätsdiebstahl abzuwehren. Als Verantwortlicher für die Gesamtinfrastruktur hoheitlicher Dokumente koordiniert das BSI die korrekte Umsetzung aller gesetzten Anforderungen.

Das am 25. Juli 2013 verabschiedete Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz, EGovG) definiert die gesetzliche Grundlage und damit das Handwerkszeug, mit dem der Staat wesentliche Schritte in die digitale Verwaltung unternehmen soll. So enthält das EGovG als wesentliche Änderung für das Verwaltungsverfahren neben der qualifizierten elektronischen Signatur die Einführung von zwei weiteren technischen Möglichkeiten, um die Schriftform in der elektronischen Kommunikation zu ersetzen: den Einsatz der Online-Ausweisfunktion des Personalausweises sowie De-Mail. De-Mail wird zudem nach dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 als sicherer Übermittlungsweg für elektronische Schriftsätze zum Gericht anerkannt.

Wesentliche Effekte wird die Umsetzung dieser Regelungen auch im Hinblick auf den Bürger haben: „Verwaltung“ wird durch das zunehmende Angebot digitaler Dienstleistungen bürgernäher – mehr und mehr Behördengänge können online erledigt werden. Durch die Effizienzsteigerung der internen Verwaltungsvorgänge und den damit verbundenen Bürokratieabbau wird sich ein messbarer Kosten-Nutzen-Effekt für Verwaltung und Bürger ergeben.

Was regelt das EGovG?

- Ersatz der Schriftform durch Online-Ausweisfunktion und De-Mail
- elektronischer Zugang zur Verwaltung
- elektronische Aktenführung
- elektronisches Bezahlen
- Gestaltung von Datenformaten
- Barrierefreiheit der digitalen Angebote der Verwaltung

Dr. Astrid Schumacher,
Referatsleiterin „Sicherheit in eID-Anwendungen“

1. Online-Ausweisfunktion

Die eID-Funktion des neuen Personalausweises ermöglicht eine sichere Authentifizierung des Bürgers mittels sogenannter Zwei-Faktor-Authentisierung zum Schutz vor Identitätsdiebstahl. Um diese Funktion nutzen zu können, benötigt der Bürger eine Softwareanwendung auf seinem heimischen Computer. Dies kann die zentral bereitgestellte Ausweis-App sein, deren Weiterentwicklung maßgeblich vom BSI betreut wird, oder auch eine marktverfügbare Alternative. Anbieter von Online-Diensten binden im Gegenzug die Online-Ausweisfunktion als Identitätsprüfung in ihre Prozesse ein, um sicher zu sein, wer ihr Partner in der elektronischen Kommunikation ist.

www.personalausweisportal.de

2. Vertrauenswürdige Verwaltung und Schriftformersatz

Um die Verwaltung bei der Konzeption von E-Government-Verwaltungsdienstleistungen zu unterstützen, hat das BSI 2013 mit der Entwicklung einer Technischen Richtlinie begonnen (BSI-TR 03107 „Elektronische Identitäten und Vertrauensdienste im E-Government“), die in Teil 2 die Verknüpfung sicherer Formulare mit der Nutzung der Online-Ausweisfunktion des elektronischen Personalausweises beinhaltet.

Teil 1 ist ein wesentlicher Beitrag zum sicheren Identitätsmanagement, indem dort verschiedene Vertrauensniveaus sowie Bewertungsmaßstäbe aufgearbeitet werden, die die Behörden in die Lage versetzen, ihre Dienstleistungen entsprechend sicher und datenschutzgerecht zu gestalten. ›

De-Mail

De-Mail ermöglicht den verbindlichen und vertraulichen Versand elektronischer Dokumente und Nachrichten. Das De-Mail-Gesetz, das am 3. Mai 2011 in Kraft trat, sorgt dafür, dass alle De-Mail-Anbieter nach den gleichen Kriterien in einem transparenten Verfahren geprüft und akkreditiert werden. Dadurch wird De-Mail deutschlandweit von allen De-Mail-Anbietern auf einem einheitlichen Sicherheitsniveau angeboten.

Der Unterschied zu herkömmlichen E-Mails: De-Mails werden auf verschlüsselten Transportwegen versendet. Zudem kann die Identität der Kommunikationspartner ebenso wie der Versand und Eingang von De-Mails nachgewiesen werden. Dadurch können viele Vorgänge auch elektronisch abgewickelt werden, für die bisher nur der Postweg infrage kam.

Akkreditierte De-Mail-Dienstleister

- 1&1 De-Mail GmbH
- Mentana-Claimsoft GmbH
- T-Systems International GmbH
- Telekom Deutschland GmbH

Diese Entwicklungen gehen sowohl in die eID-Strategie des IT-Planungsrates ein als auch in die Umsetzung der EU-Verordnung zu elektronischen Identitäten und Vertrauensdiensten.

3. De-Mail

Nach § 2 EGovG ist jede Bundesbehörde grundsätzlich verpflichtet, neben der eID-Funktion auch einen Zugang für die Übermittlung elektronischer Dokumente über De-Mail anzubieten. Zudem kann nach § 3a Absatz 2 Satz 4 Nr. 2VwVfG die Schriftform auch durch eine De-Mail ersetzt werden, wenn der Nutzer sich „sicher“ an seinem De-Mail-Konto angemeldet hat, also etwa mit der Online-Ausweisfunktion des Personalausweises. Das BSI übernimmt als zuständige Behörde die Akkreditierung von De-Mail-Diensteanbietern. So erhielt die 1&1 De-Mail GmbH im Rahmen der CeBIT 2013 in Hannover ihre Akkreditierung vom BSI als Anbieterin von De-Mail-Diensten. Als Grundlage hierfür waren u. a. das ISO 27001-Zertifikat auf Basis des IT-Grundschutzes für den Informationsverbund der 1&1 De-Mail GmbH nötig, ein Testat nach Technischen Richtlinien für De-Mail-Dienste sowie ein Datenschutzzertifikat der BfDI.

Vertrauenswürdig, authentisch und rechtsverbindlich

4. Elektronische Aktenführung und -archivierung

Ein weiteres wesentliches Ziel des EGovG sind medienbruchfreie Prozesse vom Antrag bis zur Archivierung. Das BSI hat für den Bereich der elektronischen Akte in den vergangenen Jahren Technische Richtlinien entwickelt, die mit ihren strukturierten Anforderungen pragmatische Orientierungshilfen für Verwaltung und Wirtschaft zur Einhaltung ordnungsgemäßer Prozesse bieten.

So wurde 2013 die BSI-TR 03138 „ResiScan“ zum ersetzenden Scannen veröffentlicht. Die TR hat zum Ziel, Anwendern in Verwaltung, Justiz und Wirtschaft als Handlungsleitfaden und Entscheidungshilfe zu dienen, wenn es darum geht, Papierdokumente unter Gewährleistung der Informationssicherheit einzuscannen und auf die anschließende Aufbewahrung des Originals unter größtmöglicher Beweissicherheit zu verzichten. Die BSI-TR 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ wurde 2013 weiterentwickelt. Mit dieser stellt das BSI einen Leitfaden zur Verfügung, der beschreibt, wie elektronisch signierte Daten und Dokumente über lange Zeiträume – bis zum Ende der Aufbewahrungsfristen – unter Wahrung des Beweiswertes vertrauenswürdig gespeichert werden können. Das BSI hat bereits erste Zertifikate mit der Konformitätsbestätigung nach diesen Richtlinien erteilt. □

„SICHERHEITSGEWINN FÜR DIE BÜRGER“

Cornelia Rogall-Grothe,
Staatssekretärin im Bundesministerium des Innern und Beauftragte der Bundesregierung für Informationstechnik

INTERVIEW

Frau Cornelia Rogall-Grothe ist seit 1977 als Juristin im Bundesministerium des Innern (BMI) tätig. 2010 wurde sie Staatssekretärin im BMI und zugleich zur Beauftragten der Bundesregierung für Informationstechnik ernannt. Im Gespräch erläutert sie die E-Government-Initiative des BMI.

Frau Rogall-Grothe, das Bundesministerium des Innern hat im März 2012 eine E-Government-Initiative für De-Mail und den Personalausweis ins Leben gerufen. Worin lag die Motivation, die Initiative zu starten?

Uns liegt viel daran, dass De-Mail und die Online-Ausweisfunktion des Personalausweises und des elektronischen Aufenthaltstitels bundesweit genutzt werden, weil sie persönliche Daten über verschlüsselte Kanäle und ausschließlich an zuvor zuverlässig identifizierte Kommunikationspartner übertragen. Über diesen Sicherheitsgewinn für die Bürger im Internet hinaus ermöglichen die beiden staatlich geregelten Infrastrukturen durchgängig elektronische und dadurch effiziente und nutzerfreundliche Verwaltungsdienste, die von den Bürgern einfach und bequem am PC erledigt und von der Verwaltung ohne Medienbrüche bearbeitet werden können. Wir haben die E-Government-Initiative gestartet, um diese Vorzüge für die Bürger und die öffentliche Verwaltung zu erschließen. Behörden aller Verwaltungsebenen sollten dazu angeregt werden, neue, für die Bürger attraktive Anwendungen für De-Mail und die eID-Funktion zu entwickeln. Zugleich kann das von unterstützten Behörden erworbene Wissen dokumentiert und anderen Behörden für eigene Vorhaben zur Verfügung gestellt werden.

Im Juli 2014 endete die zweite Unterstützungsphase der E-Government-Initiative. Welche Ergebnisse konnten erreicht werden?

Insgesamt erhielten 53 Behörden von Bund, Ländern und Kommunen Beratungsleistungen zur Umsetzung von 71 Vorhaben, mit denen attraktive eID- und De-Mail-Anwendungen entwickelt werden sollten. 14 von der Initiative unterstützte eID-Anwendungen waren im Mai 2014 online, vier Behörden hatten ihren De-Mail-Zugang eröffnet. Die restlichen Behörden arbeiten an der Fertigstellung ihrer Vorhaben. Auf www.personalausweisportal.de und www.de-mail.de finden Sie inzwischen über 60 Ergebnisdokumente, z. B. Architektur- und Fachkonzepte, Potenzialanalysen, Machbarkeitsstudien sowie Wirtschaftlichkeitsbetrachtungen. Es werden im Laufe dieses Jahres noch deutlich mehr werden. Wir konnten also binnen zwei Jahren neue, attraktive Nutzungsmöglichkeiten auf allen Verwaltungsebenen für beide Infrastrukturen erschließen und eine breite Wissensbasis zu vielen Implementierungsaspekten aufbauen, die allen interessierten Behörden zur Nachnutzung offensteht. Damit haben wir eine gute Grundlage für die weitere Etablierung von De-Mail und der eID-Funktion im deutschen E-Government gelegt.

Verschlüsselte Gesundheitsdaten

Umfangreiche Maßnahmen sorgen dafür, dass die Patientendaten der elektronischen Gesundheitskarte geschützt sind. Doch welche Techniken stecken dahinter?

Wie unterstützt das BSI die Sicherheit von Patientendaten?

Die Zugriffsbeschränkung auf medizinische Daten wird in der Telematikinfrastruktur (TI) generell auf Basis technischer Verfahren durchgesetzt. Die Sicherheit dieser Verfahren wird maßgeblich durch die kontinuierliche Begleitung des BSI bei der Entwicklung der fachspezifischen Sicherheitskonzepte, die Entwicklung von CC-Schutzprofilen und Technischen Richtlinien für die sicherheitsrelevanten Komponenten der Telematikinfrastruktur (TI) durch das BSI sowie den konsequenten Einsatz von entsprechend zertifizierten Produkten erreicht.

Die elektronische Gesundheitskarte soll vor allem medizinische Fachanwendungen, wie etwa die Prüfung der Arzneimitteltherapiesicherheit, ermöglichen – jedoch ruft die Speicherung solch sensibler gesundheitsrelevanter Daten auch Sorgen und Ängste hervor. Umso mehr muss das Projekt „Telematikinfrastruktur (TI) des deutschen Gesundheitswesens“ und der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) sich der Frage stellen, wie sich der nach § 291b SGB V formulierte Sicherstellungsauftrag erfüllen lässt. Er beinhaltet Folgendes: „die Interessen von Patientinnen und Patienten zu wahren“, „die Einhaltung der Vorschriften zum Schutz personenbezogener Daten sicherzustellen“ und „das notwendige Sicherheitsniveau der Telematikinfrastruktur (TI) zu gewährleisten“.

Das Zwei-Schlüssel-Prinzip

Durch das Zwei-Schlüssel-Prinzip ist sichergestellt, dass der Zugriff auf medizinische Daten sowohl die Anwesenheit der eGK als auch die eines Heilberufsausweises (HBA) erfordert. Erst wenn die eGK durch eine erfolgreiche Card-2-Card-Authentisierung festgestellt hat, dass sie sich einem gültigen HBA im erhöhten Sicherheitszustand (also nach PIN-Eingabe) gegenübersieht und auch der Versicherte seine PIN eingegeben hat, ist der Zugriff auf die medizinischen Daten oder die Nutzung des privaten Schlüsselmaterials auf der eGK möglich (siehe Grafik Seite 28).

Eine Ausnahme von der PIN-Erfordernis bildet der Zugriff auf medizinische Notfalldaten (freiwillige Anwendung) im tatsächlichen Notfall. Hier kann, aus offensichtlichen Gründen, die Mitwirkung des Versicherten unterbleiben. Allerdings ist der Zugriff auf die Notfalldaten durch einen HBA ohne PIN-Eingabe des Patienten auf bestimmte Typen von Heilberufsausweisen beschränkt. Maßgeblich ist hier das Bit 18 der Flagliste im CV-Zertifikat des Heilberufsausweises, welches nur bei Ausweisen von Ärzten und deren medizinischen Mitarbeitern sowie Rettungsassistenten gesetzt ist. Die technische Umsetzung des Zugriffsschutzes erfolgt dabei direkt durch das Kartenbetriebssystem der eGK, welche damit die Rechte der Versicherten durchsetzt. Die Definition der Zugriffsprinzipien auf medizinische Daten leitet sich im Übrigen immer aus den Vorgaben für die jeweiligen Zugriffsrechte ab, wie sie im § 291a SGB V geregelt sind.

Dezentrale Speicherung

Derzeit gibt es keine medizinische Fachanwendung in der Telematik (TI), welche einen zentralen Speicherdienst betreibt. Alle bisher spezifizierten Anwendungen nutzen für die Speicherung von personenbezogenen medizinischen Daten einzig die eGK, sofern sie nicht gänzlich beim Leistungserbringer verbleiben, also bei Ärzten, Zahnärzten und Apothekern sowie deren berufsmäßigen Gehilfen und Psychotherapeuten. Für zukünftige Anwendungen, wie z. B. das Projekt „Arzneimitteltherapiesicherheit“, die auch eine Online-Speicherung in einem Fachdienst vorsehen, gilt in jedem Fall der unabdingbare Grundsatz der patientenindividuellen Datenverschlüsselung mit der eGK. Eine Entschlüsselung der Daten durch den Betreiber des Datenspeichers ist damit technisch ausgeschlossen. Auf diese Weise sind medizinische Daten auch bei einer Online-Speicherung nur dezentral im Klartext vorhanden.

Die Gesundheitskarte muss sicher sein.

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik)

Geschlossenes Netz

Das Zentrale Netz der Telematikinfrastruktur (TI) ist ein in sich geschlossenes Netz. Zugangsmöglichkeiten ›

bestehen nur über sichere zentrale Zugangspunkte, die nur entsprechend den konkreten Anforderungen der Fachdienste durch den Gesamtbetriebsverantwortlichen (die gematik) freigeschaltet werden. Die Anbindung an die TI-Plattform ist dabei an die Voraussetzung geknüpft, dass der jeweilige Dienst ein Zulassungs- oder ein Bestätigungsverfahren bei der gematik durchläuft. Leistungserbringerinstitutionen werden nur über einen vom BSI zertifizierten Konnektor und einen VPN-Zugangsdienst an die Telematikinfrastruktur (TI) angeschlossen.

Verschlüsselt übertragen

Medizinische Daten oder andere personenbezogene Daten des Versicherten werden vor einem etwaigen Transport aus der Umgebung der Leistungserbringer heraus verschlüsselt. Darüber hinaus sind alle Kommunikationsverbindungen in der Telematikinfrastruktur (TI) zusätzlich Ende-zu-Ende verschlüsselt. Innerhalb der IPsec-Verbindung des Konnektors mit dem VPN-Zugangsdienst wird dafür ein TLS-Kanal (mindestens TLS v1.1) bis zum entsprechenden Fachdienst aufgebaut. Dies bedeutet, dass auch der Betreiber des zentralen Netzes der Telematikinfrastruktur (TI) in keinem Fall mit den Daten der Fachdienste im Klartext in Berührung kommen kann. In der Abbildung wird anhand des Versichertenstammdatenupdates verdeutlicht, dass hier zusätzlich auch die eGK des Patienten einen verschlüsselten Kanal zum Kartenmanagementsystem des Kartenherausgebers aufbaut.

Grundsätzlich wird hierfür die bestehende IPsec-Verbindung vom Konnektor in das zentrale Netz der Telematikinfrastruktur (TI) genutzt. Darüber hinaus werden zwischen Kartenterminal und Konnektor, Konnektor und Intermediär sowie zwischen Intermediär und dem Card Management System der Krankenkasse (CMS) jeweils TLS- Kanäle aufgebaut. Die Kommunikation zwischen CMS und eGK findet über Secure Messaging statt. Die Sitzungsschlüssel für Verschlüsselung bzw. MAC-Bildung werden dabei unter Nutzung eines dem CMS und der eGK bekannten Shared Secret sitzungsindividuell abgeleitet.

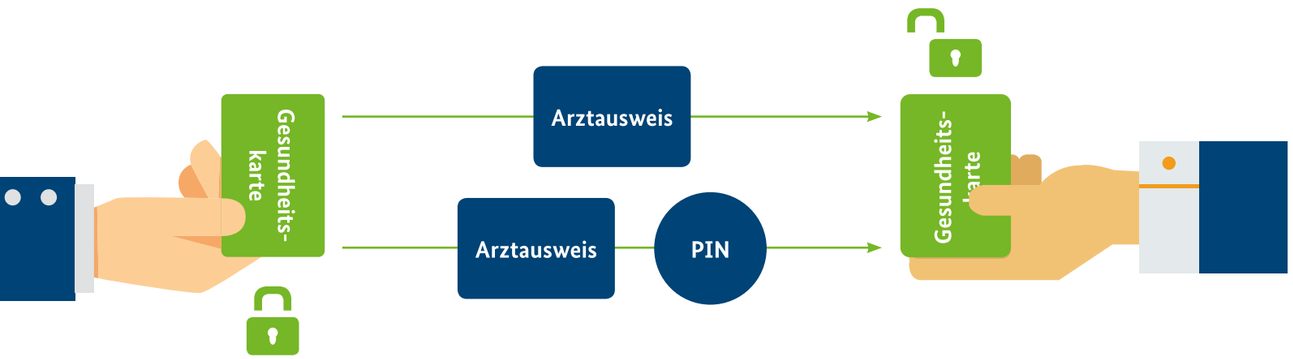
Vermeidung von Profilbildung

Über einen Intermediär wird die Identität der Leistungserbringer gegenüber den Kostenträgern (Krankenkassen) verschleiert, um die Bildung von Bewegungsprofilen des Versicherten zu verhindern. Er ist ein Dienst der zentralen Telematikinfrastruktur (TI) und liegt somit in der Verantwortung der gematik.

Evaluiert und zertifiziert

Grundsätzlich sind sämtliche kryptographische Verfahren, die in der Telematikinfrastruktur (TI) zur Anwendung kommen dürfen, in der Technischen Richtlinie TR-03116-1 verankert und für die gematik verbindlich. Die hier aufgeführten Verfahren und Mindest-Schlüssellängen gelten international als sicher und umfassen ausschließlich öffentliche und standardisierte Algorithmen. Zudem sind die Vorgaben der TR-03116-1 jeweils zeitlich befristet. In der aktuellen Fassung wird die Wirksamkeit der spezifizierten Kryptographie bis zum Jahr 2020 angenommen. Die Komponenten der TI-Plattform mit den höchsten Sicherheitsanforderungen (z. B. die Chipkarten, die Kartenterminals oder der Konnektor) müssen zusätzlich durch eine Zertifizierung nach Common Criteria (CC) bestätigen, dass sie die notwendige Kryptographie korrekt

Zwei-Schlüssel-Prinzip



Die gematik wird aufgrund ihrer Gesamtbetriebsverantwortung für die Telematikinfrastruktur (TI) als Kritische Infrastruktur in Deutschland geführt und ist Teilnehmer im Umsetzungsplan KRITIS (UP KRITIS).

umgesetzt haben und auch die restlichen Sicherheitsanforderungen der zugrunde liegenden Schutzprofile erfüllen. Hierfür beauftragen die Hersteller vom BSI akkreditierte Prüfstellen mit der Evaluierung ihrer Geräte und lassen diese anschließend vom BSI zertifizieren. Diese Zertifizierung ist, neben den technischen Prüfungen durch die gematik, Voraussetzung für eine Zulassung der Komponenten.

Sicherheit im operativen Betrieb

Der Aufbau und Betrieb eines Information Security Management Systems (ISMS) nach ISO 27001, mit speziellen Ausprägungen für die Telematikinfrastruktur (TI), ist für alle Betreiber von zentralen Diensten der TI verbindlich und muss für die Zulassung alle drei Jahre durch unabhängige Sicherheitsgutachten nachgewiesen werden. Die technische und organisatorische Umsetzung der Anforderungen des Anhangs A der ISO 27001 muss dabei mindestens auf dem Niveau der korrespondierenden Grundschutzanforderungen erfolgen, sofern die individuellen Sicherheitsanforderungen nicht noch höherwertigere Maßnahmen erfordern. Darüber hinaus werden alle Betreiber von zentralen Diensten der Telematikinfrastruktur in das koordinierende Informationssicherheits- und Datenschutzmanagementsystem der gematik eingebunden.

Nicht zuletzt wird die gematik, aufgrund ihrer Gesamtbetriebsverantwortung für die Telematikinfrastruktur (TI), als Kritische Infrastruktur in Deutschland geführt und ist Teilnehmer im Umsetzungsplan KRITIS (UP KRITIS). Auf diese Weise kann die gematik das hohe Sicherheitsniveau auch im laufenden Betrieb aufrechterhalten. □

Holm Diening,
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik)

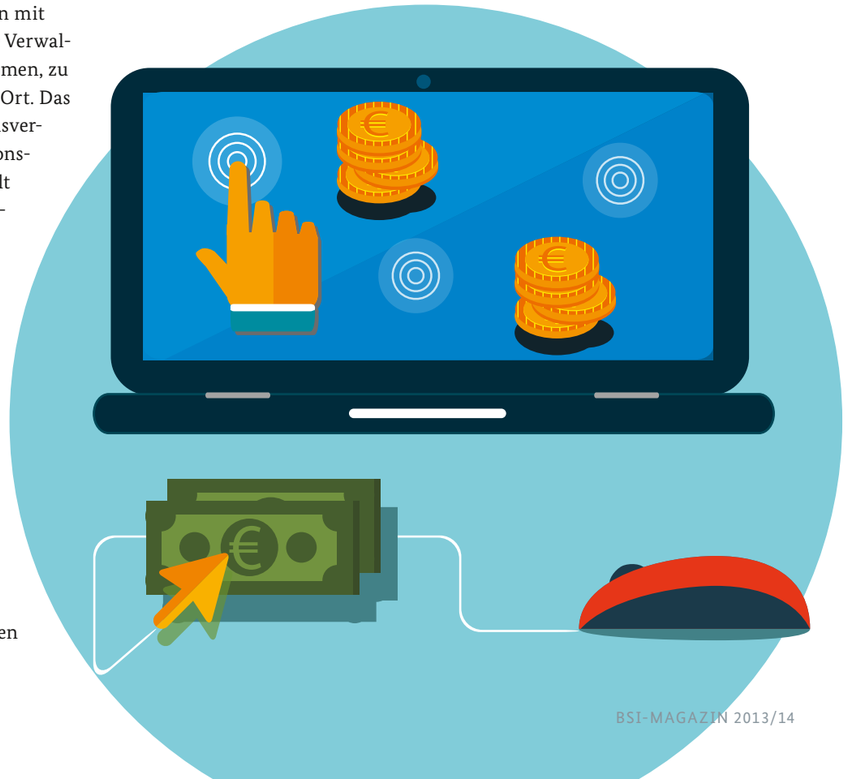
Elektronisch bezahlen – aber sicher?

Begriffe wie E-Money, Cyber-Wallets und kontaktloses Bezahlen sind das Münzklingeln der Zukunft. Als Plattform für Internet-Zahlungen der Verwaltung gilt ePayBL. Was steckt dahinter?

Wenn auch manche Bürger und Unternehmen glauben, dass sie Gebühren und Kostenbescheide nur mittels der guten alten Überweisung oder an der Kasse bezahlen können, so hat die Zukunft der Bezahlsysteme in der Verwaltung schon längst begonnen. Bürger können mit ePayBL Zahlungen an die Verwaltung elektronisch vornehmen, zu ihrer Zeit und von jedem Ort. Das Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT) entwickelt seit 2002 die Zahlungsverkehrsplattform ePayBL zusammen mit den Bundesländern Bayern, Baden-Württemberg, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland und Sachsen.

Externe Finanzdienstleister wickeln die Zahlungen ab. Die Kernkomponente von ePayBL verknüpft die Schnittstellen der Finanzdienstleister mit den verschiedenen Fachverfahren und den Haushaltssystemen der Behörden in Bund und Ländern.

Seit 2006 betreibt das ZIVIT in ihrem Bonner Rechenzentrum die mittlerweile in der Version 2.1 angekommene Kernkomponente der Zahlungsverkehrsplattform. ePayBL ermöglicht damit die seit 2013 vom § 4 EGovG geforderten durchgängigen elektronischen Verwaltungsprozesse von der Gebührenerhebung über die Rechnungslegung bis hin zur Abwicklung und Verbuchung der Zahlung in das Haushaltssystem der Behörde. Das BSI und das ZIVIT wollen daher initiativ die Informationssicherheit der Plattform prüfen und bei ihrer Weiterentwicklung stärken.



ePayBL ist ein Webservice, der einen Teil seiner Funktionen von externen Stellen bezieht. Daher legen das ZIVIT und das BSI im ersten Schritt ein Augenmerk auf die Anwendung von Sicherheitsrichtlinien und -empfehlungen schon während der Entwicklung des Webservice. Das betrifft beispielsweise die Festlegung der Zugriffsrechte der Entwickler auf die Software, um die Einschleusung schädlicher Funktionen zu verhindern. Auch die korrekte Anwendung der Elemente einer Programmiersprache ist zu betrachten, z. B. die Überprüfung extern zugeführter Zeichenketten auf schadhafte Anweisungen.

Prüfen und fortentwickeln

Softwaretests sind, gemessen an der Wichtigkeit der Plattform für ihre nutzenden Behörden, eher extensiv als reaktiv anzugehen. Die Gesamtarchitektur von ePayBL einschließlich seiner zahlreichen Schnittstellen zu den externen Fachverfahren und Benutzern aus Bund und Ländern ist Gegenstand dieses Tests auch während der Fortentwicklung. Das BSI stützt sich als Berater in dieser Kooperation auf seine Empfehlungen und Vorgaben aus den Leitfäden zur Entwicklung sicherer Web-Anwendungen, den IT-Grundschutz und seine weitreichende Expertise aus der Zertifizierung nach Common Criteria. Mittelfristig werden BSI und ZIVIT die Plattform ePayBL im Betrieb überprüfen. Das Angebot des BSI reicht hier von Tests auf Schwachstellen in den IT-Systemen, der Anwendungen und der Betriebsorganisation bis hin zu einer Zertifizierung nach IT-Grundschutz. Auch die Sicherheit der Zahlungsdaten bei ihrer Übertragung über unsichere Netze, die Stärke der Verschlüsselungsverfahren und die Organisation bei der Verteilung des Verschlüsselungsmaterials eröffnen ein weites Prüffeld. BSI und ZIVIT zielen bei ihrer Kooperation nicht nur auf geprüfte Informationssicherheit ab, sondern geben auch ein positives Beispiel für ein ausgezeichnetes Sicherheitsniveau bei gleichzeitiger Benutzbarkeit der Plattform. □

Elektronische Geldbörsen sind keine E-Mail-Konten.

Elektronisches Bezahlen ist tief in Verwaltungsprozesse integriert.

Sicherheitsmanager müssen sich daher intensiv mit allen Systemteilen befassen.

Dietmar Bremser,
Referent „Mindeststandards und Produktsicherheit“

Sicherheitsberatung

Wissen weitergeben

Bei der Sicherheitsberatung arbeitet das BSI eng mit den Kunden zusammen. Bindeglied sind die „IT-Sicherheitsbeauftragten“.

Die Sicherheitsberatung ist im BSI die ausgewiesene Ansprechstelle, der „Point of Contact“ (PoC), für die Kunden. Anfragen an das BSI werden durch Behördenkoordinatoren in der Sicherheitsberatung zentral gemanagt. Ziel dieser zentralen Organisation ist die Optimierung der Kommunikation zwischen Kunden und den Dienstleistungen des BSI. Von hier werden die Anfragen zur Beratung und Unterstützung entweder eigenständig oder unter Einbindung der Fachkompetenz zuständiger Referate beantwortet. In Einzelfällen erfolgt die fachliche Unterstützung durch Mitarbeit in Projekt- oder Arbeitsgruppen. Wahlweise wird die Beratung in Form begleitender Unterstützung oder individuell zu konkreten Lösungen sicherheitstechnischer Probleme durchgeführt.

Das PDCA-Modell

Informationssicherheit
... planen (plan)
... einrichten (do)
... prüfen (check)
... optimieren (act)

Günther Ennen,
Referatsleiter „Informationssicherheitsberatung für Behörden“

Fortbildung für mehr Kompetenz

In der Zusammenarbeit mit Behörden nimmt der IT-Sicherheitsbeauftragte den PoC auf Seiten der Kunden ein. Diese bilaterale PoC-Struktur ist Garant für die arbeitsökonomische Zusammenarbeit. Das BSI bietet in Kooperation mit der Bundesakademie für öffentliche Verwaltung (BAköV) die Fortbildungen zum zertifizierten IT-Sicherheitsbeauftragten an. Die Sicherheitsberatung verantwortet Inhalt und Struktur der Lehr- und Lerninhalte, unterstützt die IT-Sicherheitsbeauftragten innerhalb der Fortbildung, genehmigt und wertet die Projektarbeiten und ist in der Prüfungskommission vertreten. Dabei wird das Arbeitsfeld eines IT-Sicherheitsteams vertieft behandelt. Außerdem werden die Zuständigkeiten und Kompetenzen als IS-Manager vermittelt.

Elementar in der Zusammenarbeit zwischen dem BSI und den Kunden ist ein kundenseitig nach den Standards etabliertes Informationssicherheitsmanagementsystem (ISMS). Unter dieser Voraussetzung sind Rollen, Kompetenzen und die Verantwortung geregelt, Vereinbarungen sind leicht zu treffen, empfohlene Sicherheitsmaßnahmen werden umgesetzt, Beratung und Unterstützung fruchten.

Folgt zudem das ISMS dem etablierten PDCA-Model (Plan-Do-Check-Act) erfüllt es den geforderten Prozessgedanken einer stetigen Aktualisierung, Adaptierung und Reaktion auf neue Risiken der Informationssicherheit.

Zielgruppen der Beratung

Primäre Zielgruppe der Sicherheitsberatung als Kunden sind Bundesbehörden, darüber hinaus die Länder und Kommunen, sowie Hersteller, Vertreiber und Anwender in Fragen der Informationssicherheit. Die beratende und teils federführende Mitarbeit in Gremien und die Mitentwicklung von Studien ist Teil unserer Aufgaben zur Stärkung der IT-Sicherheit in Deutschland.

Unternehmen können auf das umfangreiche, im Internet frei verfügbare Informations- und Lösungsangebot des BSI zugreifen. Eine detaillierte individuelle Beratung findet zur Vermeidung einer Wettbewerbsverzerrung nur in besonderen Fällen statt. Spezielle Regelungen gelten für Unternehmen der kritischen Infrastrukturen, d.h. Institutionen mit hoheitlichen Aufgaben. Dies sind Aufgaben von besonderem öffentlichen oder politischen Interesse bzw. weitergehende Aufgaben der „Daseinsfürsorge“ des Staates.

Durch die Kommunikation der Kontaktstellen der IT-Sicherheitsbeauftragten in einer Behörde und die Sicherheitsberatung im BSI werden erfahrungsgemäß Arbeitsabläufe optimiert, in der Qualität gesichert und arbeitsökonomisch gestaltet. Auf der Homepage des BSI sind unter „Sicherheitsberatung“ die Informationen über Dienstleistungen und IT-Sicherheitsprodukte direkt erreichbar. Informationen für ausgewählte Zielgruppen sind in gesonderten und zugangsgeschützten internen Bereichen archiviert. Der Zugang ist allen IT-Sicherheitsbeauftragten und Geheimschutzbeauftragten möglich. □

Standardisierung

Der Einzelfall entscheidet

Das BSI engagiert sich national und international in der Normung. Dabei bewegt es sich im Spannungsfeld von gesetzlichen Vorgaben und Standards.

Standards im IT-Bereich definieren Qualitätsanforderungen für Produkte und bestimmen dadurch maßgeblich ihre IT-Sicherheitseigenschaften. Grund genug für das BSI, sich im Bereich der nationalen wie internationalen Standardisierung vielfach zu engagieren. Das BSI erstellt teilweise komplette technische Vorgaben. In anderen Fällen begleitet, beobachtet und kommentiert es Normungsprozesse. Soll das BSI laut einer gesetzlichen Vorgabe technische Standards bereitstellen, geschieht dies unter aktiver Beteiligung der jeweiligen Bedarfsträger und relevanter Normungsgremien, Hersteller oder Behörden. Grundlage der Entwicklung dieser Sicherheitsanforderungen für IT-Produkte sind in vielen Fällen die international anerkannten IT-Sicherheitskriterien (Common Criteria, CC) und zusätzlich bei Vorgaben für das IT-Sicherheitsmanagement der internationale Standard ISO 27001.

Verbindliche technische Vorgaben

Für die Kommunikationseinheit eines intelligenten Messsystems (Smart Meter Gateway) mit integriertem Sicherheitsmodul hat das BSI hohe sicherheitstechnische Vorgaben und funktionale Anforderungen zur Interoperabilität in Form von zwei Schutzprofilen (Protection Profiles, PP) und einer Technischen Richtlinie (TR) entwickelt. In der Technischen Richtlinie werden auch die Systemarchitektur, die Public-Key-Infrastruktur sowie Vorgaben zum sicheren technischen Betrieb des intelligenten Messsystems definiert. Aufgrund der spezialgesetzlichen Verankerung im Energiewirtschaftsgesetz (EnWG) und den dazugehörigen Rechtsverordnungen werden die technischen Vorgaben für intelligente Messsysteme und deren sicheren Betrieb für alle Marktakteure in Deutschland verbindlich. Weitere andere gesetzlich vorgegebene Standardisierungsvorhaben des BSI befinden sich im Bereich der hoheitlichen Dokumente, der Langzeitarchivierung, der Sicherheit von Erdfernerkundungssystemen (Satelliten) nach SatDSiG oder der Absicherung der Telematikinfrastruktur (TI) im Gesundheitswesen. Durch ein Zertifikat können hierbei die Hersteller Dritten gegenüber nachweisen, dass sie den Anforderungen der maßgeblichen Standards genügen.

In vielen Fällen gibt es keine gesetzliche Grundlage dafür, dass das BSI eigene technische Anforderungen entwickelt oder dass ein ganz bestimmter Standard erfüllt werden muss. Im unregulierten Bereich werden die Standards im Wesentlichen durch die Zusammenarbeit der Fachexperten der verschiedenen Hersteller selbst entwickelt. Dieser Prozess kann in ganz unterschiedlicher Form ablaufen und zu qualitativ sehr unterschiedlichen Ergebnissen führen. Das Spektrum reicht von De-facto-Standards durch einzelne Unternehmen über Standards aus Industriekonsortien bis hin zu Normen von offiziellen Organen wie des DIN oder der ISO/IEC.

Im derzeit wenig regulierten Bereich der Sicherheitschips verfügt Deutschland über starke international erfolgreiche Hersteller. Hier wirkt das BSI in Zusammenarbeit mit den Herstellern maßgeblich bei der Gestaltung von Standards mit. Bei den Steueranlagen für den Anlagen- und Maschinenbau – Stichwort „Industrie 4.0“ – verfügt Deutschland ebenfalls über eine starke Marktposition, allerdings ist dort die IT-Sicherheit noch nicht das treibende Thema. Die meisten anderen IKT-Bereiche wie z. B. Netzwerkausrüstung, mobile Geräte, Datenbanken, Betriebssysteme etc. werden vor allem durch US-amerikanische oder verstärkt asiatische Hersteller dominiert. Deutsche Gestaltungsmöglichkeiten sind hier nur in beschränktem Maße gegeben. Die aus der Mitarbeit in den verschiedenen Gremien gewonnenen Erkenntnisse und Einflussmöglichkeiten werden in Zukunft massiv an Bedeutung gewinnen. Vor dem Hintergrund der Verhandlungen auf EU-Ebene mit den USA zum TTIP (Transatlantic Trade and Investment Agreement), mit Kanada zum CETA (Comprehensive and Economic Trade Agreement) und mit 23 weiteren Staaten zum TISA (Trade in Services Agreement) werden sich die Verhandlungsparteien zusätzlich auf Standards einigen, nach denen ein Marktzugang für Produkte und Dienstleistungen auch im IT-Bereich sichergestellt sein wird. Hieraus ergeben sich wichtige Impulse für die nationalen Vorgaben an IT-Sicherheitsprodukte.

Kein Allheilmittel

Die Standardisierung ist ein wichtiges Element des BSI zur Förderung der IT-Sicherheit. Ein Allheilmittel für die Lösung jeglicher Sicherheitsprobleme ist sie jedoch nicht. Während in den gesetzlich regulierten Bereichen die IT-Sicherheitseigenschaften sehr direkt vorgegeben werden können, gibt es Marktbereiche, in denen eine Standardisierung kaum zu erreichen ist, weil z. B. der dominierende Anbieter eine Marktöffnung verhindern will. Da das Umfeld jedes einzelnen Standards anders gelagert ist, muss in jedem Einzelfall abgewogen werden, ob und ggf. wie das BSI in den Standardisierungsgremien mitwirkt. 2013 engagierte sich das BSI aktiv bzw. beobachtend in ca. 50 verschiedenen offiziellen Normungsgremien von DIN, DKE, CEN, Cenelec, ETSI, ISO/IEC und ITU-T. □

Tobias Mikolasch,
Referatsleiter
„Industriekooperation und Standardisierung“

www.bsi.bund.de

Smart Metering

Energieverbrauch intelligent gemessen

Deutschland nimmt bei sicheren intelligenten Messsystemen in Europa eine Vorreiterrolle ein. Angesichts sensibler Verbraucherdaten ergeben sich anspruchsvolle Aufgaben für das BSI.

Intelligente Netze stellen sicher, dass Energieerzeugung und -verbrauch effizient verknüpft und ausbalanciert sind. Kernbausteine eines solchen Netzes sind intelligente Messsysteme, auch „Smart Metering Systems“ genannt. Sie sollen für eine aktuelle Verbrauchstransparenz und eine sichere Übermittlung von Messdaten sorgen. Zudem steuern sie elektronische Verbrauchsgeräte und Erzeugungsanlagen so, dass ein besseres Last- und Einspeisemanagement im Verteilnetz 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. Das BSI entwickelt für diesen Bereich 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.

Schutzprofile und Richtlinien

Das BSI wurde im September 2010 vom Bundeswirtschaftsministerium beauftragt, zwei Schutzprofile (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 technologieunabhängig 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.

Sicherheitsstandards

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 der beiden Schutzprofile und der Technischen 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 zu den beiden Schutzprofilen 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 entgegengebracht wird.

Schutz der Privatsphäre

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 die damit einhergehende Ausforschung in Bezug auf die Lebensgewohnheiten des Endkunden zu verhindern. Hierzu können Auswertungsprofile im Smart Meter Gateway (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. ›

verbauen. In der Novellierung des EEG 2014 wurde sichergestellt, dass der mit der EnWG-Novelle erreichte Sicherheits- und Interoperabilitätsstandard perspektivisch auch für die nach § 9 EEG und § 34 EEG beschriebenen Anwendungsfälle Berücksichtigung finden muss.

Intelligent gesteuert

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 Last- und Einspeisemanagement wird ein hohes Potenzial von Smart Metering festgestellt, so dass 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.

Gesetzliche Pflicht

Das Energiewirtschaftsgesetz (EnWG) enthält neben umfangreichen Vorgaben zum bereichsspezifischen Datenschutz auch eine Kernvorschrift (§ 21e), in der für bestimmte Fälle ein verpflichtender Einbau eines zertifizierten Messsystems vorgeschrieben ist. 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 sieben Kilowatt zertifizierte Messsysteme

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 Konformitätsbewertung 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.

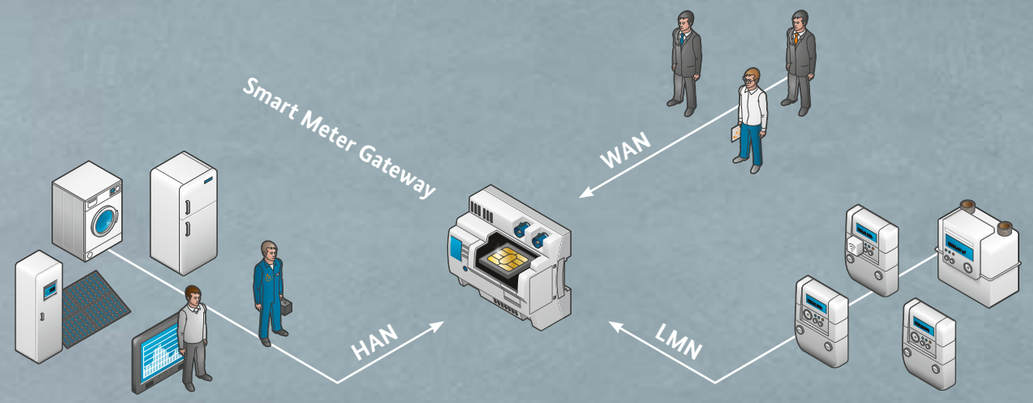
Der Referentenentwurf zur Verordnung über technische Mindestanforderungen an den Einsatz intelligenter Messsysteme (Messsystemverordnung – MsysV) nach § 21i EnWG hat am 23. September 2013 gemeinsam mit den beiden Schutzprofilen sowie der Technischen Richtlinie 03109 erfolgreich das europäische Notifizierungsverfahren 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. Eine Verabschiedung im nationalen Rechtsetzungsverfahren ist nach dem Koalitionsvertrag zwischen CDU, CSU und SPD im zweiten Halbjahr 2014 angedacht. □

Dennis Laupichler,
Referent „Industriekooperation und Standardisierung“

www.bsi.bund.de/SmartMeter

Smart Meter Gateway

Dreh- und Angelpunkt des intelligenten Messsystems

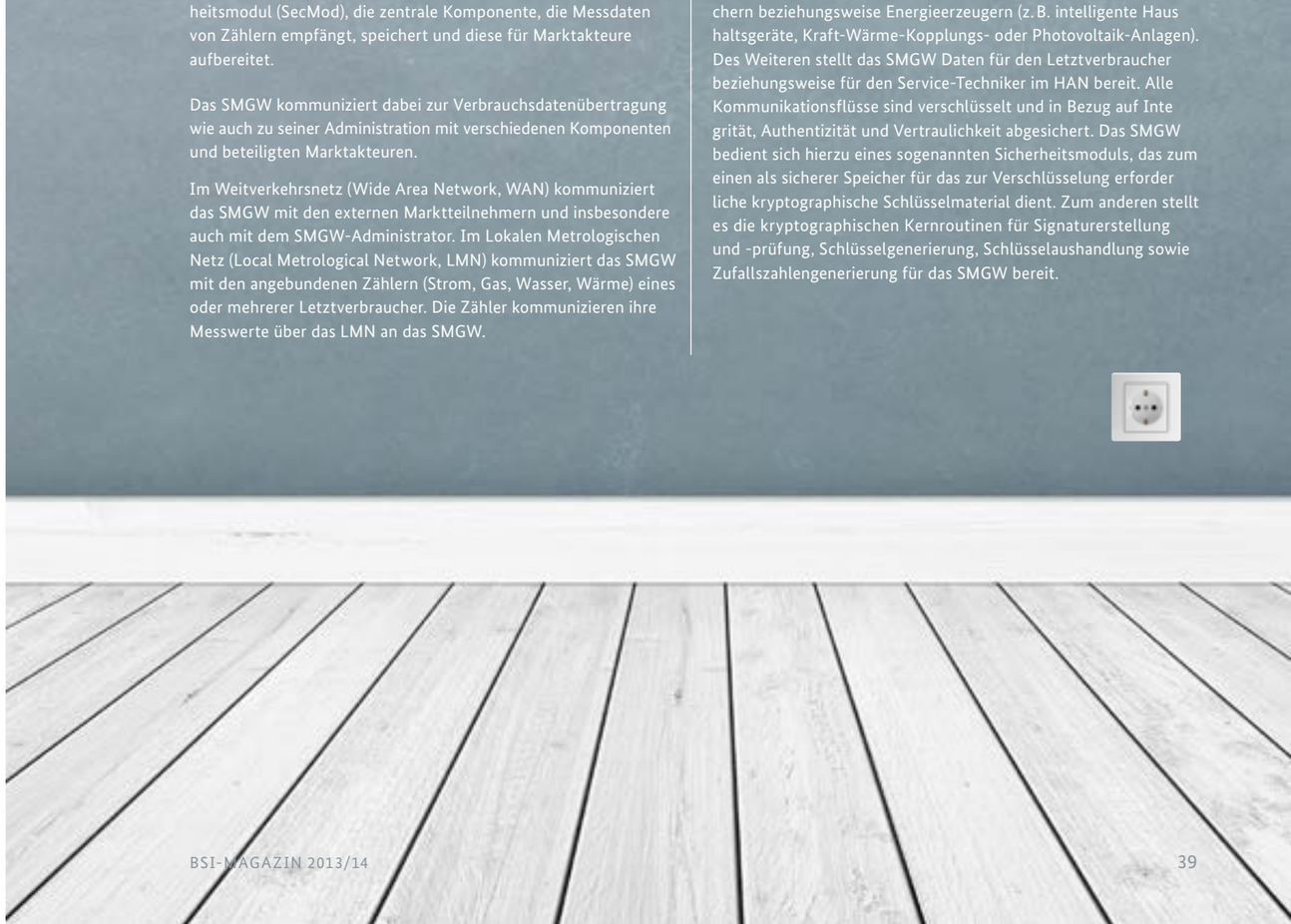


In einem intelligenten Messsystem bildet die Kommunikationseinheit, das Smart Meter Gateway (SMGW) mit integriertem Sicherheitsmodul (SecMod), die zentrale Komponente, die Messdaten von Zählern empfängt, speichert und diese für Marktakteure aufbereitet.

Das SMGW kommuniziert dabei zur Verbrauchsdatenübertragung wie auch zu seiner Administration mit verschiedenen Komponenten und beteiligten Marktakteuren.

Im Weitverkehrsnetz (Wide Area Network, WAN) kommuniziert das SMGW mit den externen Marktteilnehmern und insbesondere auch mit dem SMGW-Administrator. Im Lokalen Metrologischen Netz (Local Metrological Network, 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 Heimnetz (Home Area Network, HAN) des Letztverbrauchers kommuniziert das SMGW mit den steuerbaren Energieverbrauchern beziehungsweise Energieerzeugern (z. B. 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. Alle Kommunikationsflüsse sind verschlüsselt und in Bezug auf Integrität, Authentizität und Vertraulichkeit abgesichert. Das SMGW bedient sich hierzu eines sogenannten 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.



Cloud-Computing

Vertrauen in die Wolke

Dr. Patrick Grete,
Referent „Informationssicherheit und Digitalisierung“

Dr. Clemens Doubrava,
Referent „Informationssicherheit und Digitalisierung“

Transparenz soll neues Vertrauen in die Sicherheit des Cloud-Computings schaffen. Das BSI hat sechs Cloud-Bausteine für das Risikomanagement entwickelt.

Seit den Veröffentlichungen von Edward Snowden herrscht auch im Bereich Cloud-Computing tiefe Verunsicherung. Neues Vertrauen kann nur durch Transparenz entstehen. Für das sichere Cloud-Computing ergeben sich die folgenden drei Aspekte:

1 Risikotransparenz

Die Risiken für die Informationssicherheit müssen klar benannt und bewertet werden. Die jeweiligen Entscheidungen für oder gegen einen Cloud-Dienst muss das Risikomanagement der jeweiligen Institution treffen – das BSI unterstützt es darin. Da beim Cloud-Computing Prozesse, Daten und Akteure stark vereinheitlicht sind, können Risiken sehr systematisch analysiert werden.

2 Offene Standards

Die Effizienz von Cloud-Computing liegt in der hochgradigen Standardisierung der Dienste. Auch die Sicherheit profitiert davon. Dies führt zu Vertrauen, wenn die jeweiligen Standards offen sind und ebenso offen diskutiert und bewertet werden können. Vergleichbares gilt für die jeweilige Architektur der Cloud und entsprechende Sicherheitszertifikate.

3 Klare Aufteilung

Die Migration in die Cloud geht immer mit einer Verteilung der Verantwortung für die Informationssicherheit einher – die Letztverantwortung lässt sich nicht auslagern. Daher ist es wichtig, diese geteilte Verantwortung vertraglich genau zu regeln und so Klarheit zwischen Nutzern und Anwendern zu erreichen.

Sicherheit und Risiko

Aus diesen Punkten ist ersichtlich, dass das BSI beim Cloud-Computing einen risikobasierten Ansatz verfolgt: Risiken für die Informationssicherheit lassen sich in verteilten Infrastrukturen wie dem Cloud-Computing nicht ausschließen. Sie lassen sich nur reduzieren und müssen aktiv von einem Risikomanagement gesteuert werden. Das BSI adressiert beim Thema sicheres Cloud-Computing verschiedene Zielgruppen. So wurde der Webauftritt des Cloud-Computings (**www.bsi.bund.de/cloud**) neu gestaltet und hält für verschiedene Zielgruppen angepasste Informationen bereit. Seit der Veröffentlichung des Eckpunktepapieres „Mindestsicherheitsanforderungen für Cloud Computing Anbieter“ hat das BSI systematisch weitere Beiträge publiziert, um die obigen Ziele zu erreichen. Dazu zählen die insgesamt sechs Cloud-Bausteine (Virtualisierung, Web-Anwendungen, Cloud-Management, Webservices, Cloud-Storage und Cloud-Nutzung) für das Informationssicherheits-Managementsystem IT-Grundschutz. Sie beschreiben zu den jeweiligen Themen die wichtigsten Gefährdungen und Gegenmaßnahmen.

Die sechs Cloud-Bausteine sind auch für Nicht-IT-Grundschutz-Anwender äußerst hilfreich. Über die darin aufgelisteten Gefährdungen kann das Risikomanagement Risiken identifizieren und die zugeordneten Maßnahmen bilden eine Grundlage, um Sicherheitskonzepte zu ergänzen. Zu jedem Baustein gibt es die sogenannten Goldenen Regeln, die für die Managementebene die wichtigsten Anforderungen zusammenfassen. Für Vertragsverhandlungen stellen sie eine Checkliste dar, sodass der potenzielle Anbieter Auskunft zur Umsetzung der jeweiligen Sicherheitsanforderungen geben muss.

Damit sind diese Bausteine ein wichtiger Beitrag für die Risikotransparenz. Für mehr Transparenz sorgt auch, Risiken mit einer systematischen Methode zu identifizieren und angemessene Maßnahmen aus relevanten internationalen Standards und Rahmenwerken anzuwenden.

Sicherheitsprofil SaaS

Zur CeBIT 2014 wurde hierfür das Sicherheitsprofil für SaaS veröffentlicht. Es beschreibt für den Anwendungsfall des Kundenbeziehungsmanagements (engl. CRM) zunächst alle relevanten Akteure, Geschäftsprozesse und Daten sowie die betroffenen Komponenten einer Cloud-Architektur. Dort wirken die sechs Gefährdungen: Vortäuschen, Manipulation, Abstreitung, Vertraulichkeitsverlust, Verfügbarkeitsverlust und Rechteeskalation. Das Ergebnis dieser Verknüpfung sind alle möglichen Risiken, solange das Akteurs-, Daten- und Geschäftsprozessmodell vollständig ist. Unter allen Risiken sind 13 besonders relevante in Steckbriefen zusammengefasst. Diesen Risiken wird mit Maßnahmen begegnet, die aus verschiedenen Rahmenwerken und Standards stammen: dem Eckpunktepapier des BSI, der ISO/IEC 27001, der Cloud Control Matrix der CSA, dem NIST 800-53 und FedRAMP. Für den Anwendungsfall CRM sind zusätzlich konkrete Sicherheitsmaßnahmen formuliert. Eine Kreuz-Referenztabelle ordnet Maßnahmen den Gefährdungen zu. So ist ersichtlich, welche Risiken reduziert wurden und welche Restrisiken zu tragen sind. Das Sicherheitsprofil ist damit eine sinnvolle Blaupause für jedes Risikomanagement, um Risiken systematisch zu erfassen, angemessene Maßnahmen zu ergreifen und die Restrisiken zu überblicken. So können vom Anbieter begründete Entscheidungen getroffen werden, die bei Vertragsverhandlungen auch für den Anwender hilfreich sind.

Das Cloud-Security-Team im BSI arbeitet weiter an den oben genannten Zielen für Sicherheit im Cloud-Computing und freut sich über weitere Diskussionen oder Anregungen für konkrete zukünftige Themen. Es ist über **cloudsecurity@bsi.bund.de** zu erreichen. □

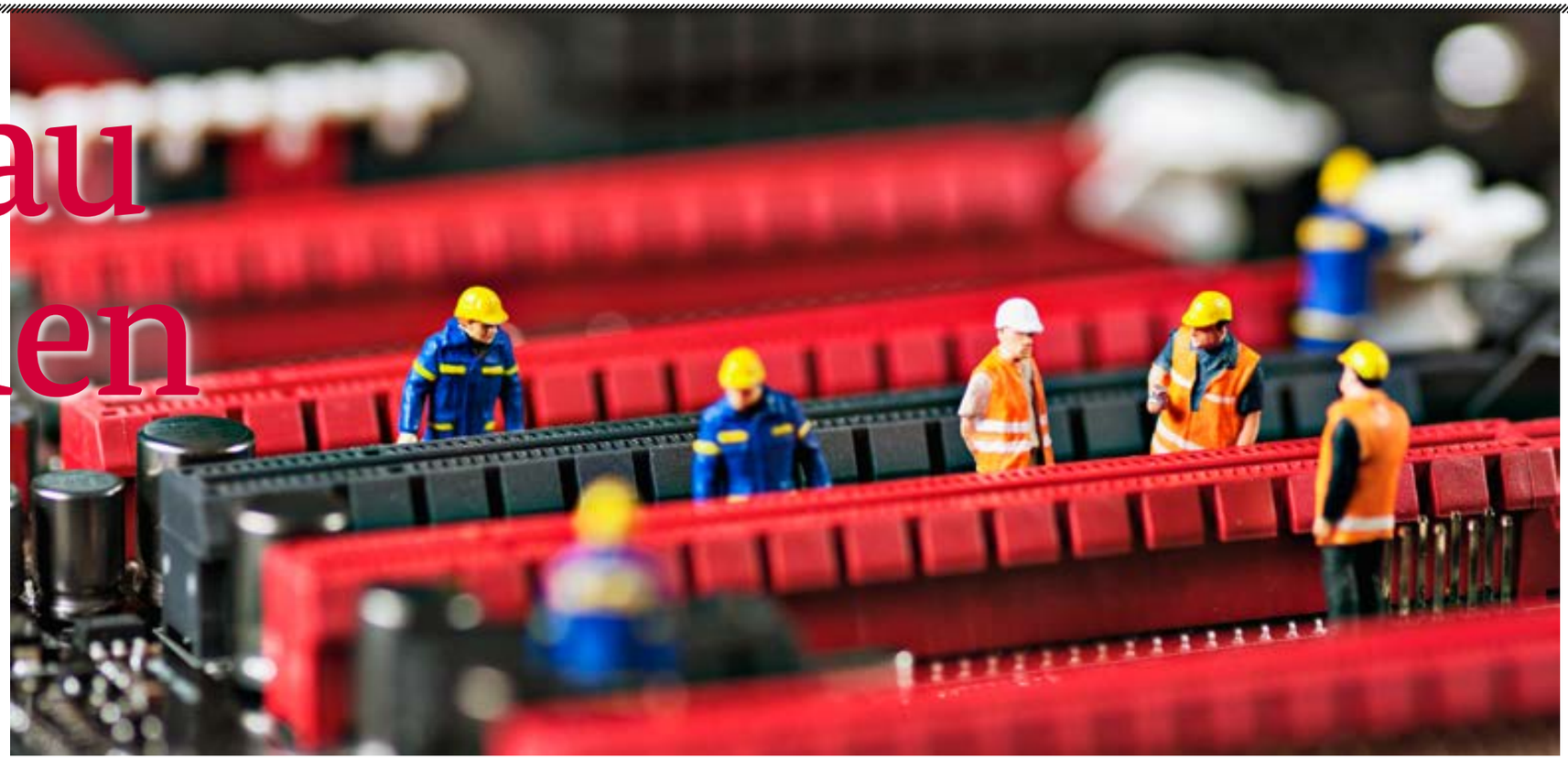
Sicheres Cloud-Computing im BSI

2014 Baustein Cloud-Nutzung
Aktualisierung Baustein Speichersysteme
Baustein Webservices
Sicherheitsprofil SaaS
2013 Baustein Cloud-Management
2012 Baustein Web-Anwendungen
2011 Baustein Virtualisierung, Eckpunktepapier
„Sicherheitsempfehlungen für Cloud Computing Anbieter“
2010 Vorabversion des Eckpunktepapieres
2009 Baustein Speichersysteme
2006 Erstes Auftreten des Begriffs Cloud-Computing

www.bsi.bund.de/cloud

Industrial Control Systems

Passgenau empfohlen



Angriffe auf industrielle Anlagen häufen sich. Das BSI schützt Betreiber und Hersteller mit passgenauen Empfehlungen.

Die Infrastrukturen der Fabrikautomation und Prozesssteuerung – subsummiert unter dem Begriff Industrial Control Systems (ICS) – waren in den vergangenen Jahren grundlegenden Änderungen unterworfen. Aus sicherheitsspezifischen Gesichtspunkten war dies insbesondere die massive Vernetzung im Produktionsnetz, im Unternehmensnetz und auch unternehmensübergreifend. Zudem ist der Einsatz von Standardkomponenten (commercial off-the-shelf) wie Betriebssystemen, Datenbanken und in der konventionellen IT etablierten Konzepten und Technologien heute Usus. Dies führt dazu, dass die heute zu beobachtenden Cyber-Bedrohungen auch für Industrial Control Systems eine hohe Kritikalität haben.

Die Sicherheitsvorfälle im Bereich Industrial Control Systems nehmen sukzessive zu. Insbesondere gezielte Angriffe sind immer häufiger zu beobachten. Während noch vor einigen Jahren nahezu ausschließlich Angriffe im Bereich Knowhow-Diebstahl zu beobachten waren, nimmt die Zahl der Angriffe auf die Verfügbarkeit der Anlagen immer mehr zu.

Das BSI hat vor drei Jahren mit dem Referat „Kommunikationssicherheit in kritischen IT-Systemen, Anwendungen und Architekturen“ eine Organisationseinheit geschaffen, die sich gezielt mit den Sicherheitsaspekten von ICS befasst.

In den vergangenen Jahren ist ein breites Portfolio an Empfehlungen und Hilfsmitteln entstanden, welches Hersteller industrieller Komponenten, Integratoren und Maschinenbauer sowie Anlagenbetreiber dabei unterstützt, ein hinreichendes Sicherheitsniveau der eigenen Produkte bzw. Anlagen zu erreichen. Da das Thema Cyber-Sicherheit in Bereichen wie Maschinenbau und Automatisierungstechnik vielerorts noch stiefmütterlich behandelt wird, musste hier ein Ansatz gewählt werden, der es ermöglicht, einen einfachen und leichtgewichtigen Einstieg in die Thematik zu finden und die dort erzielten Fortschritte sukzessive auszubauen.

Zielgruppe Betreiber

Für die meisten Betreiber bilden die **„ICS Top 10 Bedrohungen und Gegenmaßnahmen“** den optimalen Einstieg in das Thema ICS-Security. In diesem Dokument werden die kritischsten und am häufigsten ausgenutzten Schwachstellen dargestellt, mit denen ein Angreifer in Produktionssysteme eindringen kann. Die Erläuterungen erlauben eine erste Bewertung für den konkreten Anwendungsfall und zeigen geeignete Gegenmaßnahmen auf. Zudem enthält das Dokument einen kurzen Self Check bestehend aus 30 Fragen, die zur Durchführung einer ersten Positionsbestimmung im Unternehmen geeignet sind. Ergänzt werden diese „Top 10 Bedrohungen und Gegenmaßnahmen“ durch eine Reihe von Empfehlungen zu konkreten Themen wie Innentätern oder dem Umgang mit der Abkündigung von Windows XP im Produktionsumfeld.

Diese Dokumente eignen sich für den anlassbezogenen Einstieg in die ICS-Security und zielen darauf ab, mit möglichst geringem Aufwand bereits einen signifikanten Sicherheitsgewinn zu erzielen (Quick Wins). Da gerade die Sensibilisierung zur ICS-Security immer noch eine Herausforderung ist, gibt es zudem eine Sammlung von Fallbeispielen, die exemplarisch Sicherheitsvorfälle in Produktion und Automation aufzeigen.

Start small, keep on growing, and think big.

Motto des BSI im Bereich ICS

Nachdem Betreiber über diese Hilfsmittel den Einstieg in die ICS-Security geschafft haben, gibt es weiterführende Dokumente, die bei der Vertiefung und Fortführung der begonnenen Umsetzung von Cyber-Sicherheit helfen – allen voran das **„ICS Security Kompendium“** des BSI. Dieses Grundlagenwerk gibt sowohl IT-Experten bzw. IT-Sicherheitsexperten als auch Fachleuten aus Produktion und Automation einen Einstieg in das Thema ICS-Security. Schwerpunkt des „ICS Security Kompendiums“ ist eine Sammlung von Best Practices für Betreiber, die für die Absicherung von Bestandsanlagen sowie neuen Anlagen geeignet sind. Es werden verschiedene Umsetzungsmöglichkeiten dargestellt, die insbesondere den typischen Rahmenbedingungen ›

in der Fabrikautomation und Prozessleittechnik gerecht werden. Einzelne Themen wie beispielsweise die Durchführung von Security Audits werden in separaten Kapiteln noch einmal detaillierter betrachtet. Ergänzend zum „ICS Security Kompendium“ ist mit **„Light and Right Security“ (LARS)** ein ICS-spezifisches Tool verfügbar, welches bei der Erfassung der Systeme beim Betreiber und bei der Umsetzung der Maßnahmen aus dem „ICS Security Kompendium“ unterstützt. Kompendium und Tool greifen dabei nahtlos ineinander. Diese Software ist nicht nur kostenfrei, sondern auch unter Open-Source-Lizenz verfügbar, was u. a. eine einfache Anpassbarkeit gewährleistet.

Industrial Control Systems werden typischerweise nicht von Informatikern, sondern von Technikern und Ingenieuren betrieben. Diese sind häufig weniger IT-affin und insbesondere für das Thema Cyber-Sicherheit nicht hinreichend sensibilisiert. Ein weiteres Hilfsmittel des BSI ist daher das **„ICS Security Awareness Toolkit“**. Im Mittelpunkt steht dabei ein kurzer Leitfaden, der die wichtigsten Aspekte bei der Planung und Durchführung von Sensibilisierungskampagnen im Unternehmen aufzeigt. Ergänzt wird dieser Leitfaden durch eine multimediale Sammlung von Materialien wie Postern, Textbausteinen für Intranet und Newsletter, Videos, Flyern und Handouts. Ziel ist es, dieses Toolkit gemeinsam mit der Industrie sukzessive zu erweitern. Gerade kleine und mittelständische Unternehmen, die kein Budget für solche Awareness-Kampagnen aufbringen können, können damit ein geeignetes Programm aufbauen.

Zielgruppe Hersteller

Auch für Hersteller, Maschinenbauer und Integratoren folgt das BSI dem Motto „Start small, keep on growing, and think big“. Den Einstieg bilden hier beispielsweise Empfehlungen zur Handhabung von Schwachstellen oder eine Sammlung von Anforderungen an industrielle netzwerkfähige Komponenten. Während insbesondere nach Stuxnet einige Hersteller massiv ihre Bemühungen bezüglich der Sicherheit der eigenen Produkte intensiviert haben, besteht vielerorts noch Nachholbedarf auf dieser grundlegenden Ebene. Darauf aufbauend gibt ein Testleitfaden Herstellern und Integratoren die Möglichkeit, auf eine etablierte Basis eigene Testverfahren zur Sicherheit ihrer Produkte aufzusetzen. Bislang beschränken sich die Testverfahren bei den Herstellern oftmals auf die funktionalen Aspekte und ggf. die Mechanismen zur funktionalen Sicherheit (Safety). Angesichts der aktuellen Bedrohungen der Cyber-Sicherheit ist es jedoch erforderlich, die Produkte auf alle Schwachstellen zu testen, bevor diese auf den Markt gebracht werden. Ziel für Hersteller und Integratoren muss es sein, Sicherheit ganzheitlich und als integralen Bestandteil des Produktlebenszyklus zu betrachten.

Herausforderung Industrie 4.0

Im Kontext von Industrie 4.0 wird sich das Thema Security als einer der marktentscheidenden Aspekte erweisen. Die für Bestandsanlagen bewährten Lösungsmöglichkeiten halten jedoch nicht mit der massiven Zunahme der Komplexität Schritt, die diese Entwicklung mit sich bringen wird. Hier bedarf es innovativer Ansätze für Rollen- und Rechtemanagement, Vertrauensanker und sichere Plattformen. □

Betreiber

- Self Check
- ICS TOP 10 Bedrohungen
- ICS Security Kompendium
- ICS Security Awareness Toolkit
- Spezifische Empfehlungen
- LARS

Hersteller und Integratoren

- Handhabung von Schwachstellen
- Anforderungen an netzwerkfähige Industriekomponenten
- Testleitfaden
- ICS Security Kompendium

Die Sicherheitsvorfälle im Bereich Industrial Control Systems nehmen sukzessive zu

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

Kritische Infrastrukturen

Die branchenübergreifende Zusammenarbeit von Wirtschaft und Staat im Rahmen der Kooperation UP KRITIS hat sich zu einem Erfolgsmodell entwickelt. Die Kooperation passt sich stetig den geänderten Bedrohungsszenarien an.

In den letzten Jahren hat sich die Teilnehmerzahl des UP KRITIS deutlich erhöht. Vorübergehend konnten sogar keine neuen Organisationen mehr aufgenommen werden. Um auch in Zukunft weiterhin konstruktiv zusammenarbeiten und weitere Teilnehmer aufnehmen zu können, entstand im Jahr 2013 eine neue Organisationsstruktur mit einem zweistufigen Teilnahmemodell. Die Ziele der Kooperation wurden ebenfalls an die neuen Aufgaben und Herausforderungen angepasst. Die am UP KRITIS beteiligten Organisationen tauschen sich untereinander aus und lernen voneinander. Alle Teilnehmer werden – über ihre Notfallkontakte – an die Warn- und Meldestrukturen des BSI angeschlossen und stehen so mit dem BSI und insbesondere mit dem Nationalen IT-Lagezentrum in direktem Kontakt. Sie erhalten Lageinformationen und Warnmeldungen vom BSI und tragen durch eigene Beiträge zum gemeinsamen Lagebild bei. Die gemeinsame Einschätzung der Bedrohungs- und Risikosituation ist eine wesentliche Voraussetzung dafür, um auf IT-Vorfälle und (potenzielle) IT-Krisen gut vorbereitet zu sein. Mit einem gemeinsamen Verständnis der Bedrohungen und gut abgestimmten Krisenmanagementstrukturen können eingetretene Störungen oder gar Krisen gemeinsam und schnell bewältigt werden. In regelmäßig durchgeführten Übungen wird erprobt, ob die vereinbarten Kommunikationsbeziehungen aufgebaut und aufrechterhalten werden können und ob die Krisenmanagementstrukturen und -prozesse effizient und effektiv sind.

Bedrohungen verstehen

In verschiedenen Branchenarbeitskreisen zur IT-/Cyber-Sicherheit arbeitet das BSI mit KRITIS-Betreibern der jeweiligen Branche daran, Ausfälle oder Störungen der IT- und Informationsinfrastrukturen zu vermeiden. Hierzu tauschen sich die KRITIS-Betreiber und das BSI in den Arbeitskreisen regelmäßig über Cybergefährdungen in der jeweiligen Branche aus. Ziel ist es, ein gemeinsames Verständnis der IT-/Cyber-Bedrohungslage zu haben und dadurch geeignete Sicherheitsmaßnahmen zu treffen, Risiken einzudämmen, Vorfälle zu erkennen und ggf. aufgetretene (IT-)Krisen schnellstmöglich zu bewältigen. In den letzten Jahren hat dabei besonders das Thema Cyber-Sicherheit an Bedeutung gewonnen, da die Produktions- und Versorgungsprozesse der Kritischen Infrastrukturen – und damit letztlich die Versorgung der Bevölkerung – immer mehr vom ordnungsgemäßen Funktionieren von IT abhängen. Damit steigt das Risiko IT-bedingter Störungen oder Ausfälle der (kritischen) Versorgungsleistungen.

Am UP KRITIS teilnehmen können alle Organisationen mit Sitz in Deutschland, die hierzulande Kritische Infrastrukturen betreiben, nationale Fach- und Branchenverbände aus den KRITIS-Sektoren sowie die zuständigen Behörden. □

www.upkritis.de
www.kritis.bund.de

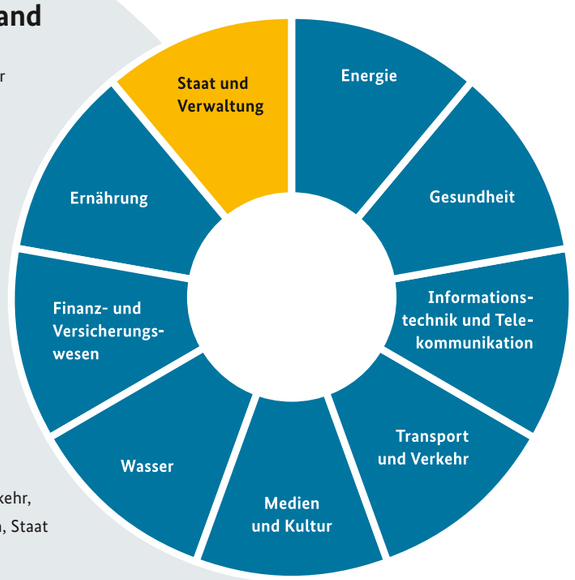
Störungen und Ausfälle beispielsweise in der Energieversorgung können weite Teile der Bevölkerung erheblich treffen.

Nora Apel,
Referentin „Schutz Kritischer Infrastrukturen“

Kritische Infrastrukturen in Deutschland

Kritische Infrastrukturen (KRITIS) sind die „Lebensadern“ unserer Gesellschaft. Sie stellen wichtige, teils lebenswichtige Güter und Dienstleistungen bereit, die für das staatliche Gemeinwesen, d. h. für Wirtschaft, Staat und Gesellschaft, unabdingbar sind. Die KRITIS-Strategie der Bundesregierung definiert Kritische Infrastrukturen als „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ (das Dokument ist abrufbar auf der Seite **www.kritis.bund.de** unter „Publikationen“).

Zu den Kritischen Infrastrukturen in Deutschland gehören Organisationen und Einrichtungen aus den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur.



IT-Sicherheit im politischen Raum

Im politischen Raum steigt die Aufmerksamkeit für das Thema IT-Sicherheit. Das BSI ist als kompetenter Ansprechpartner gefragt.

Vor dem Hintergrund der fortschreitenden Digitalisierung der Gesellschaft ist die politische Wahrnehmung des Themas IT-Sicherheit in den vergangenen Jahren kontinuierlich gestiegen. Durch verschiedene Entwicklungen in einem ereignisreichen Jahr 2013 wurde diese Aufmerksamkeit noch weiter erhöht. So erfolgte im Frühjahr 2013 die Vorstellung eines Entwurfs für ein IT-Sicherheitsgesetz. Einen Monat später wurden die Ergebnisse der Arbeiten der 2010 vom Deutschen Bundestag eingesetzten Enquete-Kommission „Internet und digitale Gesellschaft“ dem Bundestagsplenum vorgelegt. Infolge der Snowden-Veröffentlichungen stellte die Bundesregierung im Sommer 2013 zudem ein Acht-Punkte-Programm zum besseren Schutz der Privatsphäre vor, mit dem das Thema Informationssicherheit ein weiteres Mal in den politischen Fokus rückte. Zur gleichen Zeit setzte die entscheidende Phase im Bundestagswahlkampf ein, in dem sowohl zahlreiche Parteien als auch verschiedene politische Interessengruppen Positionen zu Fragen der IT-Sicherheit bezogen.

Die zunehmende Bedeutung von Fragen der IT-Sicherheit spiegelt sich auch in dem Ende November 2013 vorgestellten Koalitionsvertrag für die 18. Legislaturperiode wider, in dem die Digitalisierung zu den wichtigsten Herausforderungen gezählt wird und zahlreiche Maßnahmen zur Förderung der IT-Sicherheit enthalten sind. So enthält der Koalitionsvertrag u. a. die Ankündigung, in der neuen Legislaturperiode ein IT-Sicherheitsgesetz zu verabschieden und die „Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum“ zu stärken. Auch das BSI findet im Teilkapitel zur digitalen Sicherheit und zum Datenschutz explizit Erwähnung, da die Koalitionsparteien ankündigen, „die Kapazitäten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und auch des Cyber-Abwehrzentrums auszubauen“. Der Koalitionsvertrag greift zudem zahlreiche Fachthemen des BSI auf, da u. a. eine „Weiterentwicklung und Verbreitung von Chipkartenlesegeräten, Kryptographie, DE-Mail und sicheren Ende-zu-Ende-Verschlüsselungen“ und eine „Zertifizierung für Cloud-Infrastrukturen und andere sicherheitsrelevante Systeme und Dienste“ angestrebt werden. Auswirkungen auf die Arbeit des BSI ergeben sich darüber hinaus aus der Ankündigung einer ressortübergreifenden „Digitalen Agenda 2014–2017“, mit der die Schwerpunkte der Digitalpolitik der Bundesregierung festgelegt werden sollen. Als unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft ›

berät das BSI die Politik durch seine fachliche Expertise zu technischen Fragen der Informationssicherheit und Digitalisierung bei der Konzeption und Umsetzung politischer Maßnahmen zur Förderung der IT-Sicherheit. So wurde das BSI auch 2013 von politischen Gremien wie dem Innenausschuss, dem Parlamentarischen Kontrollgremium (PKGr) oder der IuK-Kommission des Ältestenrates des Deutschen Bundestages konsultiert und von zahlreichen politischen Stakeholdern zu Veranstaltungsvorträgen eingeladen. Da dem Thema IT-Sicherheit auch im transnationalen Raum verstärkt Aufmerksamkeit geschenkt wird, ist die Fachexpertise des BSI dabei nicht nur auf nationaler, sondern auch auf europäischer und internationaler Ebene gefragt.

Die steigende politische Relevanz von Themen der Informationssicherheit hat zugleich Auswirkungen auf die Arbeit im BSI, da technische Fragestellungen häufig nicht mehr losgelöst von den Erwartungen und Anforderungen der Akteure im politischen Raum betrachtet werden können. Vielmehr ist von zahlreichen Wechselwirkungen zwischen den Entwicklungen im politischen Raum und den Aufgaben des BSI als einer technischen Fachbehörde auszugehen, denen innerhalb des BSI u. a. durch eine regelmäßige Vorbereitung der Amtsleitung für Anhörungen in politischen Gremien oder einen regelmäßigen Dialog mit den politischen Stakeholdern des BSI Rechnung getragen werden muss.

Oliver Klein,
Referent „Informationssicherheit und Digitalisierung“

Diese Entwicklungen werden sich auch im Jahr 2014 fortsetzen, wie beispielsweise die laufende Erarbeitung der „Digitalen Agenda 2014–2017“ verdeutlicht. Durch den bereits im Frühjahr 2013 im Abschlussbericht der Enquete-Kommission „Internet und digitale Gesellschaft“ geforderten ständigen Bundestagsausschuss zu Themen der Netzpolitik, der im Februar 2014 als Ausschuss Digitale Agenda seine Arbeit aufgenommen hat, wird die Fachexpertise des BSI in Zukunft auch in einem weiteren Bundestagsausschuss gefragt sein. Hinzu kommen verschiedene neue Arbeitsgruppen und Initiativen, die in Reaktion auf die Digitalisierungsprozesse in Wirtschaft, Verwaltung und Gesellschaft Themen der Informationssicherheit aufgreifen. Da die Entwicklungsdynamik und die politische Relevanz der Digitalisierung somit weiter zunehmen werden, wird das BSI auch zukünftig die Entwicklungen auf der politischen Ebene begleiten und politischen Akteuren als kompetenter und vertrauenswürdiger Ansprechpartner für Fragen der Informationssicherheit zur Verfügung stehen. ◻

Stimmen aus der Politik

Es kann nicht sein, dass Bürger alleine für ihre Sicherheit verantwortlich sind, und es kann nicht sein, dass der Staat alleine für die Sicherheit der Bürger im Internet verantwortlich ist.

Bundesinnenminister Thomas de Maizière (CDU), Konferenz der Alfred-Herrhausen-Gesellschaft September 2014

IT-Sicherheit wird zu einer wesentlichen Voraussetzung zur Wahrung der Freiheitsrechte.

Aus dem Koalitionsvertrag zwischen CDU, CSU und SPD, 18. Legislaturperiode

Das IT-Sicherheitsgesetz

Für die ganze Gesellschaft

Das Thema IT-Sicherheit rückt immer stärker in die Wahrnehmung von Öffentlichkeit und Politik. Das neue IT-Sicherheitsgesetz soll Bürger und Wirtschaft schützen.

Mit großer Regelmäßigkeit kreisen die Nachrichten um Angriffe auf IT-Systeme oder Sicherheitslücken in gängigen Programmen und in häufig genutzten Geräten. Kein Wunder, dass sich die Anwender fragen, ob und wie sie die moderne Technik überhaupt noch sicher nutzen können. Daher haben auch die Regierungsparteien das Thema IT-Sicherheit im Koalitionsvertrag als eines der wichtigsten Handlungsfelder für die laufende Legislaturperiode definiert.

Auch der Bundesinnenminister widmet sich diesem Thema. Neben der organisatorischen Stärkung des Themas Cyber-Sicherheit innerhalb des BMI hat sich Dr. Thomas de Maizière öffentlich mehrfach für eine Stärkung des BSI ausgesprochen. Außerdem erklärte er kurz nach Amtsantritt, dass er das in der letzten Legislaturperiode nicht mehr zu Ende geführte Gesetzgebungsvorhaben für ein IT-Sicherheitsgesetz wieder aufgreifen werde. Wie auch immer die Regelungen genau aussehen werden, die der Bundestag letztlich verabschieden wird: Eine widerstandsfähige IT bei den Betreibern der Kritischen Infrastrukturen ist eine wichtige Grundlage für die Versorgung der Bevölkerung mit lebenswichtigen Gütern und Diensten. Wie anfällig industrielle Steuerungssysteme sein können, hat der Fall des Schadprogramms „Stuxnet“ auch einer breiteren Öffentlichkeit eindrucksvoll vor Augen geführt. Daher wird das Gesetz eine Verpflichtung der Betreiber Kritischer Infrastrukturen mit sich bringen, ihre IT-Systeme so zu schützen, dass keine Versorgungsengpässe durch Cyberangriffe entstehen. Auch die Einführung einer Meldepflicht bei erheblichen IT-Sicherheitsvorfällen ist wahrscheinlich. Auf dieser Basis wird das BSI ein fundierteres Lagebild erstellen und andere Betreiber über drohende Angriffe unterrichten, aber auch gezieltere Schutzmaßnahmen empfehlen können.

Ebenfalls sicher ist, dass das BSI mit dem IT-Sicherheitsgesetz eine neue Rolle einnimmt und sich von einem Sicherheitsdienstleister für die Bundesverwaltung zu einer Institution für die gesamte Gesellschaft wandelt. Damit wird der schon mit der letzten Novellierung des BSI-Gesetzes 2009 beschrittene Weg fortgesetzt. Bereits heute erwarten Bürger, Wirtschaft und Politik angesichts einer stetig komplexer werdenden digitalen Welt vom BSI, dass es Bürger und Wirtschaft verstärkt in Fragen der IT-Sicherheit unterstützt. Das BSI reagiert darauf mit dem Auf- und Ausbau seiner Angebote für die Bürger (u. a. BSI für Bürger) und für die Wirtschaft (u. a. Allianz für Cyber-Sicherheit). Der Gesetzgeber reagiert auf die gewandelte Rolle mit dem IT-Sicherheitsgesetz. ◻

Steve Ritter,
Referent „IT-Sicherheit und Recht“

IT-Sicherheit und Datenschutz

Vertrauliches schützen

IT-Sicherheit und Datenschutz brauchen ein gesetzgeberisches Gesamtkonzept.

In der IT-Sicherheit hat eine neue Zeitrechnung begonnen. Nach den Snowden-Enthüllungen, nach der Offenbarung von Millionen gehackter Accounts bei Ebay und nach vielen kleineren Skandalen ist eine der großen Fragen, die die IT-Sicherheitsbranche und damit letztendlich auch den Datenschutz beschäftigt: Wie können Behörden, Unternehmen und Privatleute vertraulich kommunizieren? Wie kann sichergestellt werden, dass die Geheimdienste, egal welcher Nation, dass Kriminelle, egal welcher Art, uns nicht überwachen, belauschen und ausspionieren können? Und wie schützen wir letztendlich unsere personenbezogenen Daten? Die Affären haben eines erreicht: Das Vertrauen in die Informationstechnik und in die IT-Sicherheit steht auf dem Prüfstand! Datenschutz wird zu einem aktuellen Thema. Ausgerechnet jetzt, in einer Zeit, in der Vernetzung die Welt näher zusammenbringt, müssen wir der Technik misstrauen, die dies gewährleistet, und wir zweifeln an der Sicherheit, die das Datenschutzrecht gewährleisten soll. Betroffen sind alle: Behörden, Unternehmen und Privatpersonen, Verbraucher und Produzenten, Jung und Alt.

Die ersten Vorschläge, die in die Diskussion einflossen, waren – technisch betrachtet – der umfassende Einsatz von Verschlüsselung und – rechtlich gesehen – ein Abkommen, das Spionage unterbinden könnte. Doch reicht das? Technisch sind Verschlüsselung der Kommunikation und Verschlüsselung von gespeicherten Daten sicherlich geeignete Maßnahmen, um sich vor neugierigen Blicken zu schützen. Ein „No-Spy"-Abkommen könnte diese vermutlich ergänzen. Aber ist das genug, um einen umfassenden Schutz vor staatlicher Spionage, Kriminellen und neugierigen Unternehmen zu gewährleisten? Und sind diese Maßnahmen auch nach weiteren technologischen Entwicklungen geeignet, den notwendigen Schutz zu bieten? Der Umstieg von der Papierwelt auf Elektronik ist nicht mehr aufzuhalten. Es ist daher geboten, IT-Sicherheit und Datenschutz auf eine breitere Basis zu stellen. Für Deutschland und Europa werden sich Sicherheits- und Datenschutztechnologien vermehrt zu einem nunmehr auch international beachteten Standortvorteil entwickeln. Technik wird zum entscheidenden Faktor und damit zum Bindeglied zwischen Anwendung und Nutzer. In die Technik müssen deshalb sowohl datenschutzrechtliche als auch IT-Anforderungen einfließen.

Die Bürger schützen

Eine Gesellschaft, die zunehmend auf elektronische Verfahren setzt, schafft damit neue Kritische Infrastrukturen, die nicht nur für Geheimdienste interessant sind, sondern auch andere Akteure auf den Plan rufen. Solche Kritischen Infrastrukturen zu sichern, wird in Zukunft eine Aufgabe sein, der sich der Staat annehmen muss, um seine Bürger zu schützen und deren Freiheit zu gewährleisten. Ohne diesen Schutz kann keine freiheitliche Gesellschaft auf Dauer funktionsfähig bleiben und bestehen. IT-Sicherheit und Datenschutz sind somit zwei Seiten der gleichen – kostbaren – Medaille.

Vor diesem Hintergrund ist es geboten, es nicht bei Einzelmaßnahmen zu belassen, sondern IT-Sicherheit und datenschutzrechtliche Anforderungen in ein Gesamtkonzept einzubinden, dass auch in Zukunft tragfähig ist. Auf der Basis eines IT-Sicherheitsgesetzes will die Bundesregierung das Sicherheitsniveau bei allen Kritischen Infrastrukturen in der Wirtschaft verbessern, mehr Transparenz hinsichtlich möglicher Gefahren oder Störungen herstellen und gleichzeitig Wissen und Know-how über die Bedrohungen aus den internationalen Netzwerken nutzen, um die Sicherheit insgesamt zu erhöhen. Auch der Datenschutz soll hier verstärkt berücksichtigt und zum zentralen Aspekt werden.

Spätestens der NSA-Skandal hat die Verletzlichkeit der digitalen Gesellschaft und die Dringlichkeit einer gesetzlichen Initiative aufgezeigt. IT-Sicherheit und Datenschutz sind wesentliche Voraussetzungen zur Wahrung der Freiheitsrechte. Ich unterstütze die Initiative der Bundesregierung mit Nachdruck. Denn letztendlich nützt sie auch dem Datenschutz. Die oft nur punktuelle Einführung von Verschlüsselung und neue Abkommen werden uns in Zukunft nicht schützen. Um die Kritischen Infrastrukturen abzusichern, brauchen wir eine solche disziplinübergreifende Initiative. ◻

Andrea Voßhoff,
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Öffentlichkeitsarbeit im BSI

IT-Sicherheit geht alle an

Newsletter, Social Media und Websites sind nur wenige der zahlreichen Kanäle, mit denen das BSI die Öffentlichkeit informiert.

Täglich erreicht das BSI eine Vielzahl von Anfragen rund um das Thema IT-Sicherheit. Die neutrale, produktunabhängige und kompetente Beratung kommt sehr gut an und zeigt, dass das BSI in den Köpfen der Nutzer als Ansprechpartner angekommen ist. Mit konkreten Hilfestellungen und nützlichen Tipps arbeiten wir täglich daran, das Bewusstsein der Bürgerinnen und Bürger für einen sicheren Umgang mit der Informationstechnik zu stärken.

Websites

Nur wer die Hilfestellungen und Tipps versteht, kann sie auch umsetzen. Daher bietet das BSI alle Informationen bedarfs- und zielgruppengerecht an. Auf der Website **www.BSI-fuer-buerger.de** finden sich deshalb komplexe Themen in einfacher und verständlicher Sprache wieder. Anhand konkreter Tipps und Checklisten kann hier jeder Nutzer lernen, was er selbst für die IT-Sicherheit seiner Geräte tun kann. Für IT-Experten hält die Website **www.bsi.bund.de** ein umfangreiches Angebot zu Themen wie Kritische Infrastrukturen, IT-Grundschutz oder Sicherheitsberatung bereit. Pressemitteilungen, aktuelle Studien oder Warnungen vor kritischen Sicherheitslücken erscheinen hier zuerst.

Newsletter

Der Newsletter „Sicher • Informiert“ des BSI-Bürger-CERTs meldet 14-tägig kostenfrei, schnell und kompetent Viren, Würmer und Sicherheitslücken in Computeranwendungen. Bereits über 100.000 Nutzer haben sich auf **www.buerger-cert.de** registriert.

Facebook

Seit August 2013 wird das BSI-Bürger-Portal durch eine Präsenz auf der Social-Media-Plattform Facebook ergänzt. Unter **www.facebook.com/BSI.fuer.buerger** postet das Redaktionsteam täglich (Mo–Fr) neben verschiedenen wiederkehrenden Formaten Sicherheitstipps sowie Multimedia- und Themenbeiträge aus dem Bereich IT-Sicherheit. Über die Kommentarfunktion und mittels privater Nachrichten können Fans und Besucher direkt mit dem BSI interagieren. Die mehr als 21.000 „Gefällt mir“-Angaben im ersten Jahr verdeutlichen, dass sich der Auftritt und die Interaktionsmöglichkeiten als Erfolgskonzept etabliert haben.

Informationen für Bürger

Newsletter „Sicher • Informiert“
26 (2013)
13 (bis Juli 2014)

Extraausgabe „Sicher • Informiert“
5 (2013)
6 (bis Juli 2014)

Technische Warnungen
109 (2013)
71 (bis Juli 2014)

INS INTERNET – MIT SICHERHEIT!
www.bsi-fuer-buerger.de
www.facebook.com/bsi.fuer.buerger

Das BSI Service-Center

Mit mehr als 2.500 Anrufen, E-Mails und Faxen pro Monat nimmt das BSI Service-Center einen wichtigen Platz im Bereich der Bürgerservices des BSI ein. Seit Anfang März 2014 ist das BSI Service-Center unter der kostenlosen Nummer 0800 274 1000 erreichbar.

Die neue Bürgerbroschüre des BSI

Pünktlich zum Safer-Internet Day 2014 hat das BSI sein Angebot um eine Cloud-Broschüre für Bürger erweitert. Viele IT-Anwender nutzen die Cloud bereits, ohne sich darüber bewusst zu sein. Die Bürgerbroschüre „In die Cloud – aber sicher!“ soll zu einem bewussteren Gebrauch anregen.

13. Deutscher IT-Sicherheitskongress

Unter dem Motto „Informationssicherheit stärken – Vertrauen in die Zukunft schaffen“ fand vom 14. bis 16. Mai 2013 der 13. Deutsche IT-Sicherheitskongress in Bonn statt. Drei Tage lang informierten sich die Teilnehmer aus Wirtschaft, Wissenschaft und Verwaltung über aktuelle Entwicklungen und Trends im Bereich der IT-Sicherheit.

Die Zeitschrift für Informations-Sicherheit

Das offizielle Verlautbarungsorgan des BSI ist das BSI-Forum in der <kes> Die Zeitschrift für Informations-Sicherheit. Sechs Mal im Jahr erscheint die Zeitschrift, in der BSI-Autorinnen und Autoren mit Beiträgen zu aktuellen Themen in der IT-Sicherheitsbranche informieren. Ergänzt wird der BSI-Beitrag durch die amtlichen Mitteilungen im Bereich Zertifizierung. Das BSI-Forum ist neben der Printausgabe in der <kes> auch elektronisch auf der Seite **www.bsi.bund.de/ForumKES** verfügbar.

Das BSI baut bereits früh Kontakte zu Studierenden auf – durch die Studienförderung, Hochschultage und Messen, Praktika sowie die Betreuung von Abschlussarbeiten.

Kontakt zum Nachwuchs

Im Bereich der IT besteht für sämtliche Arbeitgeber, ob freie Wirtschaft oder Öffentlicher Dienst, ein Fachkräftemangel. Die gut qualifizierten Fachkräfte stehen sofort nach dem Studium einem breiten Markt zur Verfügung. Insofern ist es notwendig, bereits während des Studiums Nachwuchskräfte auf sich aufmerksam zu machen und an sich zu binden.

Seit mehreren Jahren fördert das BSI Bachelor-Studierende bereits während des Informatik-Studiums und versucht sie so als spätere Mitarbeiterinnen und Mitarbeiter zu gewinnen. Das BSI nutzt zudem das Angebot der Hochschulen, um sich auf deren Hochschultagen als künftiger Arbeitgeber zu präsentieren (z. B. Unternehmenstag der Hochschule Bonn-Rhein-Sieg, ITS-Connect der Ruhruniversität Bochum etc.). Auch der Besuch von Messen (CeBIT, IKOM etc.) gehört zur frühzeitigen Kontaktaufnahme zu potenziellen Mitarbeiterinnen und Mitarbeitern. In den Studienordnungen verschiedener Studiengänge sind Praktika bzw. sogenannte Praxissemester vorgesehen. Während dieser studienpraktischen Zeit können Studierende die praktische Seite ihres Studiums kennenlernen. Für die in den Studienordnungen vorgesehene Dauer der Praktika wirken die Studierenden in verschiedenen Fach-/Sachgebieten des BSI mit und betreuen oftmals ein eigenes Projekt passend zu ihrem Studienschwerpunkt. Vielfach wird durch diese ersten Kontakte, die auch oftmals fach-/sachgebietsübergreifend sind, der Wunsch geweckt, auch die Bachelor- oder Masterthesis durch das BSI betreuen zu lassen. Halbjährlich werden aktuelle Themen über die Website des BSI publiziert und bieten Orientierung über mögliche Praktikums- und Abschlussarbeitsthemen.

Die Betreuung des Bachelorand/Masterand erfolgt durch erfahrene Mitarbeiterinnen und Mitarbeiter des BSI, die den Studierenden während der drei- bis sechsmonatigen Bearbeitungszeit beratend zur Seite stehen und im Prüfungsprozess die Rolle des Zweitbeurteilers wahrnehmen. □

Bettina Westhofen,
Referat „Personal“

„IDEALE IN DIE TAT UMSETZEN“

INTERVIEW

Herr Paegelow, 2011 kamen Sie als Diplomand der Fachrichtung Medieninformatik zum BSI. Heute sind Sie verbeamtet. Was hat Sie damals dazu bewegt, sich beim BSI zu bewerben?
Zur Zeit meines Studiums rückte das vielschichtige und interessante Thema Informationssicherheit auch außerhalb der Fachkreise in den allgemeinen Fokus der IT-Welt und ich verfolgte die Entwicklungen auf diesem Gebiet mit höchstem Interesse. Ich konnte glücklicherweise schon während des Studiums die Thematik Informationssicherheit bzw. IT-Sicherheit insbesondere durch zwei Wahlpflichtfach-Kurse vertiefen. Das war zu der Zeit an Hochschulen eine Seltenheit. Somit wurde ich natürlich auch auf das BSI und dessen vielseitige Aktivitäten im Bereich der Informationssicherheit aufmerksam.

René Paegelow,
Referat „Informationssicherheitsberatung für Behörden“

Gab es bestimmte Aspekte, die Sie besonders gereizt haben?
Insbesondere die in meinem Praxissemester durchgeführte IT-Grundschutzanalyse für eine mittlere Institution nach den vom BSI herausgegebenen Standards brachten mich sehr nahe an die Vielschichtigkeit der Informationssicherheit heran. Da ich das breite Spektrum der IT-Sicherheit und insbesondere den IT-Grundschutz auch nach meinem Praxissemester weiter verfolgen wollte, beschloss ich, mich beim BSI für meine Diplomarbeit zum Thema „IT-Grundschutz-Weiterentwicklung“ zu bewerben.

Und inwiefern führte Ihre Diplomarbeit zu Ihrer Bewerbung beim BSI?
Das Anfertigen meiner Diplomarbeit mit fachgebietsübergreifender Unterstützung der BSI-Mitarbeiter unter der allgemeinen BSI-Prämisse der eigenständigen qualitätsorientierten Arbeit und der Einbringung eigener Ideen mit dem Anspruch, dass meine Diplomarbeit und die Arbeit des BSI insgesamt auch der Allgemeinheit zugutekommt, gefiel mir sehr gut. Darum wollte ich auch nach dem Ende meines Studiums beim BSI arbeiten.

Was gefällt Ihnen beim BSI besonders gut?
Heute arbeite ich in der Sicherheitsberatung des BSI und wirke somit ganz nach meinem selbst gesteckten Anspruch einer nachhaltigen und qualitativen Unterstützung der Kunden, mit immer neuen und sehr interessanten Herausforderungen.

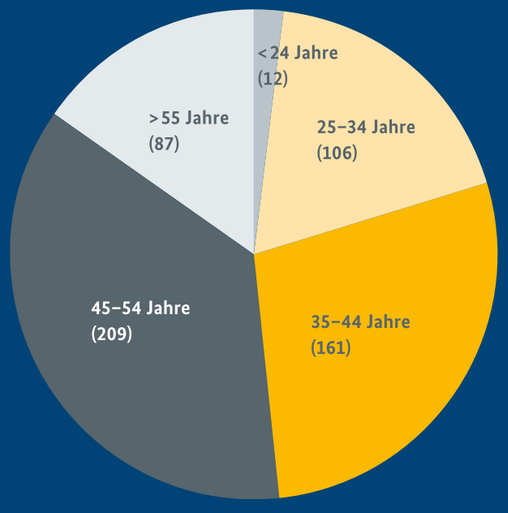
Mitarbeiter des BSI

Das Marketinginstitut trendence kürte das BSI 2014 zu Deutschlands beliebtesten 100 Arbeitgebern.

575 Mitarbeiter

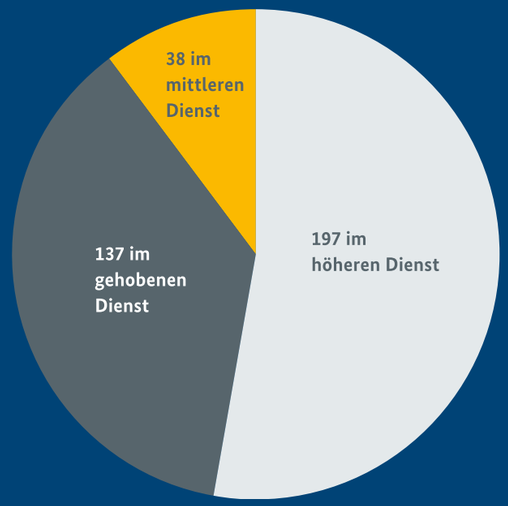
7 Auszubildende

Altersstruktur



143 Frauen (24,87 %)
432 Männer (75,13 %)

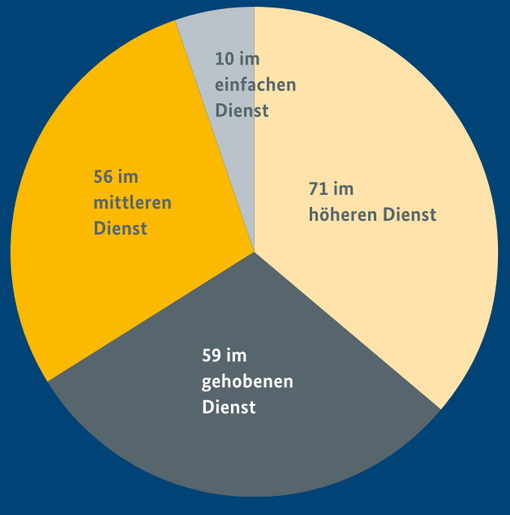
372 Beamte



Berufliche Hintergründe

- 31 % Ingenieure
- 22 % Informatiker
- 18 % Verwaltungs-/ Betriebswirtschafts-/ Finanzwirte
- 14 % Mathematiker
- 11 % Geologen, Biologen, Physiker
- 2 % Juristen
- 2 % Sonstige

196 Tarifbeschäftigte



Stand: 31.12.2013

2013

Das hat das BSI bewegt

Nicht nur Edward Snowdens Enthüllungen, sondern auch Messen, Kongresse und Mailtests markieren wichtige Etappen der vergangenen Monate.

05.03. – 09.03.2013

CeBIT

Die weltgrößte Computermesse CeBIT ist ein fester Bestandteil im BSI-Kalender. Mit einem neuen Standdesign und dem Fokusthema Cyber-Sicherheit sowie der von BSI und BITKOM initiierten Allianz für Cyber-Sicherheit.

08.04. – 12.04.2013

Hannover Messe

Premiere auf der Hannover Messe. Zusammen mit dem Zentralverband Elektrotechnik- und Elektronikindustrie e. V. (ZVEI) informiert das BSI zum Thema ICS und Industrial IT Security 4.0.

14.05. – 16.05.2013

IT-Sicherheitskongress

Heimspiel in Bonn. Beim Deutschen IT-Sicherheitskongress trifft sich alle zwei Jahre das Who's who der deutschen IT-Sicherheitsbranche.

Juni 2013

Snowden-Enthüllungen

Im Juni 2013 veröffentlichen der Guardian und die Washington Post geheime Dokumente, die sie vom früheren NSA-Mitarbeiter Edward Snowden erhalten haben. Snowden wird dafür in den USA wegen Spionage angeklagt.

Oktober 2013

European Cyber Security Month (ECSM)

Der ECSM ist eine Kampagne der EU zur Erhöhung des Bewusstseins für Cyber-Sicherheit. 2013 partizipiert das BSI zum ersten Mal mit durch Social Media begleiteten Aktionen zu den Themen soziale Netze, Online-Shopping sowie mobiles und sicheres Surfen.

15.11.2013

European Cloud Partnership (ECP)

Das ECP Steering Board beschäftigt sich mit strategischen Ansätzen, die sicherstellen, dass Cloud-Dienste in privaten und öffentlichen Angeboten ein nachhaltiges, innovatives und ökonomisches Wachstum ermöglichen. 2013 ist das BSI Ausrichter des jährlich stattfindenden Steering Boards.

2014


Cloud-Computing war eines der Top-Themen auf der CeBIT 2014.

Berliner Forum Cyber-Sicherheit

21.01.2014

Mailtest-Aktion

Aufgrund eines großflächigen Identitätsdiebstahls richtet das BSI eine Website ein, auf der Bürgerinnen und Bürger überprüfen können, ob sie von diesem Identitätsdiebstahl betroffen sind.

22.01.2014

Forum zur Cyber-Sicherheit

Mit der Bundesakademie für Sicherheitspolitik richtet das BSI das 1. Berliner Forum zur Cyber-Sicherheit in Berlin aus. Zahlreiche Vertreter aus Wirtschaft, Politik und Forschung folgen der Einladung und diskutieren gemeinsam über die Zukunftsperspektiven der IT-Sicherheit.

11.02.2014

Safer Internet Day

Das BSI gibt anlässlich des Safer Internet Days eine Cloud-Broschüre für Bürger heraus und beantwortet auf einer eigens dafür geschalteten Expertenhotline Fragen rund um das Thema Cloud-Computing.

10.03. – 14.03.2014

CeBIT

Die CeBIT 2014 zeigt sich in neuem Gewand mit einer B2B-Ausrichtung. Das tut dem Besucherstrom am BSI-Stand und bei den BSI-Vertretern im Public Sector Parc keinen Abbruch.

20.03.2014

NSA-Untersuchungsausschuss

Der Deutsche Bundestag setzt einen Untersuchungsausschuss zur NSA-Affäre ein. Das Gremium soll Ausmaß und Hintergründe der Ausspähungen durch ausländische Geheimdienste in Deutschland aufklären.

20.08.2014

Digitale Agenda

Das Bundeskabinett beschließt die „Digitale Agenda 2014–2017“.

23.09. – 26.09.2014

security essen

security essen ist die weltweit bedeutendste Messe für Sicherheit und Brandschutz. Das BSI ist mit den Bereichen materielle Sicherungstechnik und Informationssicherheitsberatung vertreten.

02.10. – 03.10.2014

Bürgerfest

Auf einem Bürgerfest am Tag der Deutschen Einheit in Hannover empfangen BMI, BSI und die Bundeszentrale für politische Bildung Besucher unter dem Motto „Deutschland gemeinsam im Netz – aber sicher!“.

www.bsi.bund.de