Bundesamt
für Sicherheit in der
Informationstechnik

# Mit Sicherheit

BSI-Magazin 2015

HILFE ZUR SELBSTHILFE

## Modernisierung des IT-Grundschutzes

SICHERE INFORMATIONSGESELLSCHAFT

## Das IT-Sicherheitsgesetz tritt in Kraft

# Inhaltsverzeichnis

**Cyber-Sicherheit**



**Sichere Informationsgesellschaft**



**IT-Sicherheit in der Praxis**



**Das BSI und seine Aufgaben**





# Editorial

**Liebe Leserinnen und Leser,**
das IT-Sicherheitsgesetz ist in Kraft getreten. Jetzt muss es sich in den Unternehmen und auch in der Gesellschaft etablieren. Das neue Gesetz räumt dem BSI zusätzliche Rechte und Pflichten ein. Wir werden sie aktiv nutzen, um diesen Etablierungsprozess zu unterstützen und die Robustheit unserer kritischen IT-Infrastrukturen zu verbessern.

Denn die  Infrastrukturen sind angreifbar wie nie zuvor. Immer mehr Geräte und Maschinen, immer mehr Lebens- und Produktionsbereiche sind heute mit dem Internet verbunden. Umfangreiche Risikoanalysen sind nötig, um die Gefahren richtig einschätzen und deren Eintrittswahrscheinlichkeiten gering halten zu können. Klare Richtlinien im IT-Sicherheitsbereich, wie sie durch das Gesetz definiert sind, helfen den Unternehmen, eine solide Grundlage zu schaffen, auf der sie aufbauen können.

Wir haben in den letzten Jahren eine rasante Steigerung von Angriffen beobachtet, wobei diese immer raffinierter wurden. Der Hackerangriff auf die IT-Systeme des deutschen Bundestags und die DDoS-Attacken auf die Webseiten der Bundeskanzlerin sind nur zwei Beispiele dafür.

Nicht nur die Quantität, sondern auch die Qualität von Cyber-Attacken verändert sich kontinuierlich und passt sich den aktuellen Gegebenheiten im Cyber-Raum an. Doch es gilt noch immer: Ein solider Grundschutz neutralisiert die gängigsten Angriffe und zwingt Angreifer zur Nutzung neuerer Methoden, die höhere Kosten verursachen und deshalb den Angreifer aus ökonomischer Sicht zur Aufgabe seiner Angriffsabsichten bewegen.

Die Themen IT-Sicherheit und Cyber-Sicherheit halten zunehmend Einkehr in unser alltägliches Leben. Wenn bisher Nutzerfreundlichkeit und einfache Bedienbarkeit im Vordergrund standen, nimmt heute merkbar auch das Bewusstsein für die Sicherheit zu. Nun gilt es, diese Thematik im Bewusstsein der Allgemeinheit weiter zu vertiefen.

Mit diesem Magazin geben wir Ihnen einen Einblick in ausgewählte Projekte, die genau dieses gewährleisten sollen. Ich wünsche Ihnen bei der Lektüre viele interessante Einsichten und Denkanstöße.
Bonn, im September 2015

*Michael Hange*
*Präsident des Bundesamtes für Sicherheit in der Informationstechnik*

# Alle Steine des Mosaiks

## Die aktuelle Bedrohungslage immer im Blick

Der BSI-Bericht „Die Lage der IT-Sicherheit in Deutschland“ gibt jedes Jahr Auskunft darüber, wie es hierzulande aktuell um die IT-Sicherheit bestellt ist. Die Veröffentlichung ist bestrebt, belastbare Antworten jenseits aller Spekulationen und Hysterie zu liefern – eine herausfordernde Aufgabe, an der zahlreiche Experten des BSI über Monate hinweg unzählige Mosaiksteine kontinuierlich zusammentragen, analysieren und auswerten, um eine aktualisierte und fundierte Antwort auf die Frage : „Wie ist die aktuelle Cyber-Sicherheitslage?“ zu liefern.

Am 17. Dezember 2014 hat Innenminister Dr. Thomas de Maizière gemeinsam mit BSI-Präsident Michael Hange den BSI-Bericht „Die Lage der IT-Sicherheit in Deutschland 2014“ vorgestellt. Ziel der Veröffentlichung ist es, die Erkenntnisse über die IT-Sicherheitslage in Deutschland und vor allem deren Bewertung durch das BSI einer breiten Öffentlichkeit zugänglich zu machen. Dabei geht es nicht nur darum, den Leser zu informieren und zu sensibilisieren, sondern vor allem auch darum, die Eigenverantwortung jedes Nutzers für IT-Sicherheit aufzuzeigen. An der Erstellung der vierzigseitigen Publikation hat ein großes Projektteam mit zahlreichen BSI-Experten mitgewirkt.



**Informationsquellen auswerten**
Primäre Quellen sind die Erkenntnisse des BSI-Lagezentrums, des Computer Emergency Response Teams (CERT) der Bundesverwaltung, des Cyber-Abwehrzentrums sowie Informationen aus dem täglichen Austausch in den Fachabteilungen. Hinzu kommen BSI-eigene Sensordaten, die zum Beispiel bei der Absicherung der Regierungsnetze anfallen. Einen ebenfalls nicht zu unterschätzenden Stellenwert haben Informationen von Dritten sowie die Auswertung einer Vielzahl öffentlicher Informationsquellen, die BSI-Experten vor allem im Bereich der Lagebeobachtung nutzen.

**Technische Parameter und organisatorische Rahmenbedingungen**
Der BSI-Lagebericht nimmt jedoch nicht nur zu technischen Parametern Stellung. Einen großen Einfluss auf die Lage haben die sich weiterentwickelnden Rahmenbedingungen, zum Beispiel wie Informationstechnologie heute im beruflichen oder privaten Kontext Verwendung findet. Dazu kommen Ursachen der aktuellen Gefährdungslage, die eher organisatorische als technische Hintergründe haben. Nach der Veröffentlichung des Berichts im Dezember 2014 wurde die Debatte um IT-Sicherheit, besonders im politischen Raum, beispielsweise um den Aspekt der „Digitalen Sorglosigkeit“ ergänzt. Hinter dem Begriff steht das alltägliche Spannungsverhältnis zwischen Verantwortung und Sorglosigkeit der Anwender im Umgang mit Informationstechnologie. Somit ist eine kontinuierliche Lageanalyse der technischen Parameter, das Wissen über organisatorische Einflüsse und die Berücksichtigung aktueller Rahmenbedingungen Grundlage für einen fundierten Jahresbericht zur IT-Sicherheitslage in Deutschland.


→ **Lage sondieren und Informationen zusammentragen**
Heute vergeht kein Tag mehr ohne Medienberichte über Cyber-Angriffe, neue Schwachstellen, Störungen von IT-Prozessen oder abgeflossenen Daten. Dabei ist jede Meldung, jeder Bericht und jede Statistik einer von vielen Mosaiksteinen, die immer wieder neu zu einem Lagebild zusammengesetzt werden müssen.

**Expertenanalyse**
Neben der Informationssammlung ist besonders für die Auswertung Expertenwissen gefragt. Nur ein Experte, der sich dauerhaft und intensiv mit einem Thema beschäftigt, kann Neues von Bekanntem oder Fakten von Spekulationen trennen sowie die Verlässlichkeit einer Informationsquelle richtig einordnen und so zu einer verlässlichen Einschätzung der Lage gelangen.

**Cyber-Sicherheitslagebild – Basis für den Lagebericht**
Den Grundstein für den BSI-Lagebericht in seinem aktuellen Format legt das Referat „Analyse und Prognose”, das sich in der Fachabteilung Cyber-Sicherheit befindet, mit dem Cyber-Sicherheitslagebild. Diese Auswertung wird seit dem Frühjahr 2014 regelmäßig zu aktuell neun unterschiedlichen Themen erstellt und dient als interne Basis für den Lagebericht. Ziel ist es, die Lageauswertung weiter zu verbessern. Dazu wurden Analyseprozesse stärker formalisiert, mehr Quellen kontinuierlich anstatt ad-hoc beobachtet und dadurch eine stets aktuelle Lagedarstellung zu zentralen Themen geschaffen. Neben der internen Weiterverwendung werden die Informationen aus dem Cyber-Sicherheitslagebild auch auf der Webseite der Allianz für Cyber-Sicherheit den Teilnehmern der Initiative im Mitgliederbereich zur Verfügung gestellt.

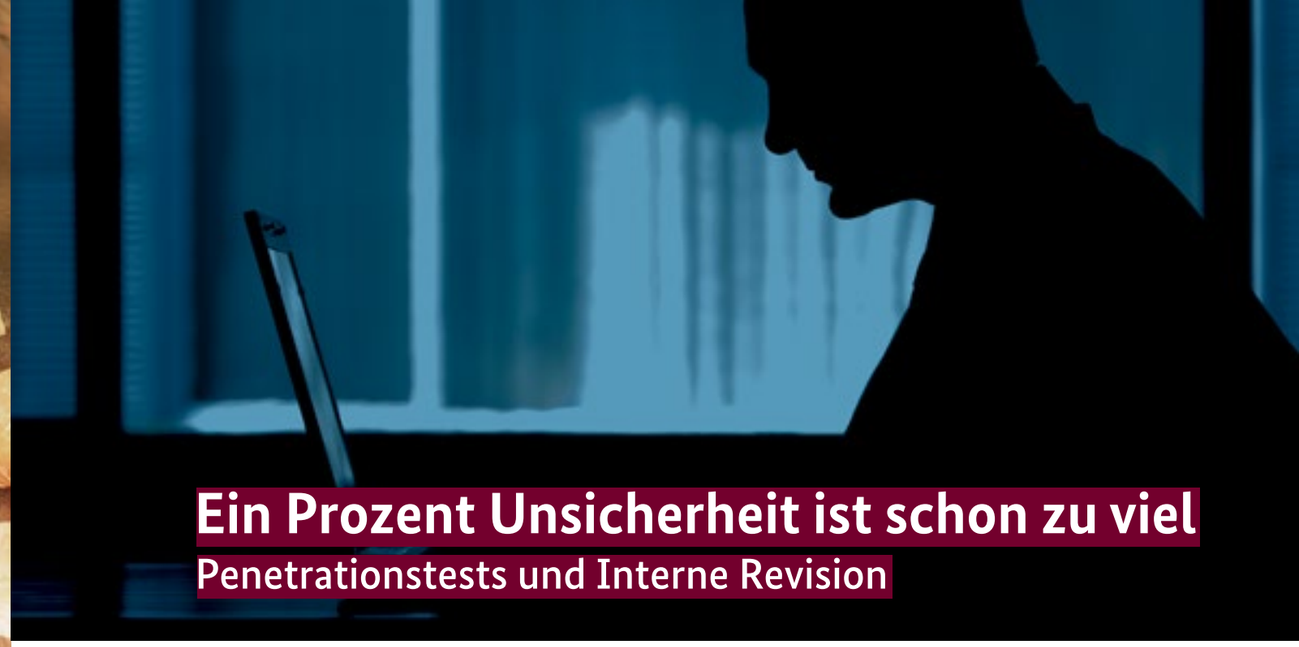
### Die Lage der IT-Sicherheit in Deutschland

Der BSI-Lagebericht 2015 wird im Herbst erscheinen und eine aktualisierte Antwort auf die Frage: „Wie ist die aktuelle Cyber-Sicherheitslage?“ liefern.
Danach liegt es an den Lesern, sich ihrer Eigenverantwortung bewusst zu werden und die gewonnenen Erkenntnisse in konkrete Handlungen zur Verbesserung der IT-Sicherheit umzusetzen. Denn das Wissen über die aktuelle Lage ist Voraussetzung, um adäquat darauf reagieren zu können.

*Daniel Mühlenberg, Referent "Analyse und Prognose"*

### Nach dem Lagebericht ist vor dem Lagebericht

Die Arbeiten für den BSI-Lagebericht 2015 sind bereits in vollem Gang. Wie im Vorjahr wird die aktuelle Lage anhand von Ursachen, Angriffsmitteln und -methoden sowie Angreifertypen dargestellt. Dazu kommen die Berichte über Vorfälle, von denen die Bundesverwaltung, KRITIS-Unternehmen oder die Wirtschaft allgemein sowie Privatnutzer im Jahr 2015 betroffen waren. Dabei lässt sich jetzt schon absehen, dass es wieder mehr relevante Vorfälle gibt, als im Bericht Platz finden werden. Im Hinblick auf das im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz wird voraussichtlich auch das Thema „Schutz Kritischer Infrastrukturen“ aufgegriffen werden. ■



# Ein Prozent Unsicherheit ist schon zu viel

## Penetrationstests und Interne Revision

**Von Sebastian Schreiber, Geschäftsführer SySS GmbH**

**Der Prüfung von IT und speziell der IT-Sicherheit kommt im Rahmen von Revisionsprüfungen eine noch immer untergeordnete, aber aus gutem Grund ständig wachsende Bedeutung zu. Schon lange setzen Unternehmen eine Vielzahl an Maßnahmen ein, um IT-Sicherheit zu gewährleisten: Diese reichen von diversen ISO- und BSI-Zertifizierungen bis hin zu Audits aller Art. Doch diese Maßnahmen reichen offensichtlich nicht aus, wie bereits ein erster Blick in die Presse zeigt: Immer wieder sorgen Berichte von IT-Security-Vorfällen in Organisationen, Unternehmen und Behörden für Schlagzeilen – zuletzt besonders prominent die Hackerangriffe auf das japanische Unternehmen Sony im Dezember 2014 und auf den Deutschen Bundestag im Juni 2015.**

Die IT-Sicherheitsvorfälle der jüngeren Vergangenheit zeigen eindrücklich, dass die IT-Systeme selbst bei internationalen Hightech-Unternehmen und obersten staatlichen Einrichtungen nicht hinreichend geschützt sind. Verbreitete Maßnahmen der IT-Qualitätssicherung – darunter Code-Reviews, Security Development Lifecycle oder Grundschutz- und ISO-Zertifizierungen – mögen ausreichen, um 99 Prozent der Systeme sicher zu gestalten. Entscheidend ist jedoch: Das daraus resultierende, verbleibende 1 Prozent Verwundbarkeit bietet ein Ziel für digitale Angriffe: Jede noch so kleine Lücke reicht aus, um eine ansonsten gut abgesicherte IT-Infrastruktur in ihrer Gesamtheit angreifbar zu machen.

*Diplom-Informatiker Sebastian Schreiber, geboren 1972, studierte Informatik, Physik, Mathematik und BWL an der Universität Tübingen. Von 1996 bis 1998 war er Mitarbeiter bei Hewlett-Packard. Noch während seines Studiums gründete er die SySS GmbH in Tübingen. Seit 2000 tritt Schreiber regelmäßig bei Messen und Kongressen im In- und Ausland als Live Hacker auf. Er ist gern gesehener IT-Sicherheitsexperte in Printmedien, Rundfunk und Fernsehen. Als langjähriges Mitglied engagiert er sich darüber hinaus im Verband für Sicherheit in der Wirtschaft Baden-Württemberg e.V. oder auch im Beirat der Zeitschrift "Datenschutz und Datensicherheit".*

*Penetrationstests waren in 1998 Anlass für die Gründung der SySS GmbH. Die Firma beschäftigt heute 70 Mitarbeiter und bezeichnet sich als Markt- und Technologieführer in Deutschland sowie Europa auf diesem Gebiet. Neben Sicherheitstests gehören Digitale Forensik, IT-Sicherheitsschulungen sowie Live-Hackings zum Portfolio der SySS GmbH.*

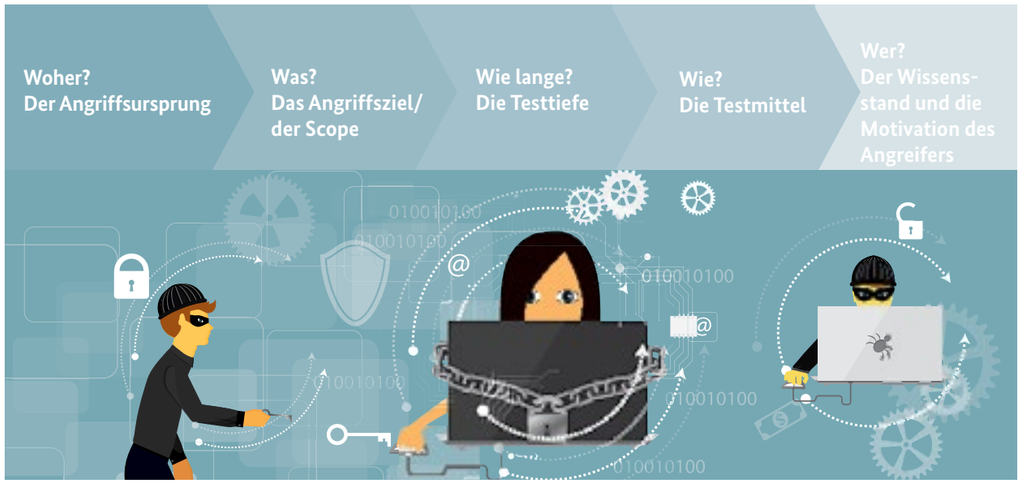
*Ein Penetrationstest ist die Simulation von Hackerattacken. Dabei nimmt der Tester die Rolle des Angreifers ein und deckt so Sicherheitslücken auf.*

*Penetrationstests legen schnell, kostengünstig und ohne großen Aufwand momentane Sicherheitslücken offen und bieten konkrete Lösungsansätze.*

→ **Regelmäßig Hackerangriffe simulieren**

Reale Angreifer verfügen über ein erfahrungsbasiertes Wissen, mit dem sie dieses eine Prozent Unsicherheit ausfindig machen und ausnutzen können. Und genau an dieser Stelle – oder besser gesagt davor – setzen Penetrationstester an: Einfach gesagt ist ein Penetrationstest die Simulation von Hackerattacken. Dabei nimmt der Tester die Perspektive derjenigen ein, die versuchen, ein Unternehmen anzugreifen und deckt so Sicherheitslücken auf, noch bevor diese für einen Angriff missbraucht werden können. Dabei sollte jedoch eines beachtet werden: Tagtäglich tauchen neue Sicherheitslücken in Softwareprodukten auf – und damit auch neue mögliche Einfallstore für Hacker. Penetrationstests sollten deshalb fest in die Prüfpläne von Revisionen integriert und entsprechend häufig in einem festen Rhythmus durchgeführt werden. Dies ermöglicht es, dass die Vielzahl an Hackerangriffen, von denen die betroffenen Unternehmen nicht einmal etwas wissen, keine reinen Zufallsentdeckungen mehr bleiben. Stattdessen werden gezielt Schwachstellen identifiziert und geschlossen, bevor sich beispielsweise ein Trojaner einnistet und über Jahre unentdeckt bleibt. Ein einzelner Penetrationstest untersucht dabei ein oder mehrere Angriffsszenarien, die vor Beginn eines Tests näher bestimmt werden müssen. Der Revisor bzw. Auftraggeber definiert dabei generell folgende Spezifika pro Szenario mit individuellem Bezug zum eigenen Unternehmen:

- Woher? Der Angriffsursprung
- Was? Angriffsziel/der Scope
- Wie lange? Die Testtiefe
- Wie? Die Testmittel
- Wer? Der Wissensstand und die Motivation des Angreifers




Wer Penetrationstests wirksam durchführen will, muss sein Spezialwissen ständig aktualisieren. Es ist deshalb nicht ratsam, derartige Untersuchungen allein von der eigenen Unternehmens-IT durchführen zu lassen: Die hauseigene IT-Fachabteilung hat meist nicht nur ein sehr breites Aufgabenspektrum, das einer gezielten Spezialisierung auf IT-Security entgegensteht, sondern läuft auch auf Dauer Gefahr, betriebsblind zu werden. Der in die regelmäßigen Revisionsprüfpläne integrierte Blick von außen durch einen externen Penetrationstester hilft dabei, „Blinde Flecken“ aufzudecken und Sicherheitslücken zu schließen – bevor es zu einem Vorfall kommt.

**Ein attraktives Prüfkonzept**

Aus Sicht der Internen Revision weisen Penetrationstests – abgesehen von ihrer nachweislich positiven Wirkung auf die IT-Sicherheit – einen weiteren praktischen Vorteil auf: Die Durchführung kann schnell erfolgen, ist kostengünstig und für den Revisor mit keinem großen Aufwand verbunden. Liegt dann der Prüfbericht vor, zeigt sich ein weiterer Vorzug: Das Ergebnis eines Penetrationstests ist meistens von bestechender Klarheit. Die gefundenen Schwachstellen und ihre Folgen lassen kaum Raum für Interpretationen und sind im Allgemeinen auch für Nicht-Informatiker gut verständlich: Weist ein Penetrationstester zum Beispiel nach, dass es ihm möglich ist, innerhalb weniger Stunden sämtliche Lieferantendaten aus der entsprechenden Datenbank auszulesen, wird wohl niemand mehr ein sachliches Gegenargument vorbringen können. Klar ist dann: Die IT-Sicherheit des Unternehmens weist an dieser Stelle offensichtlich ein Leck auf und sofortige Gegenmaßnahmen sind notwendig.

Auch was diese Maßnahmen angeht, erweist sich ein Penetrationstest für die Revision als konstruktiv. Am Ende einer jeden Prüfung steht immer ein Abschlussbericht, der nicht nur alle gefundenen Lücken ausführlich dokumentiert, sondern auch konkrete Vorschläge zu deren Behebung enthält. So kann der Revisor seiner Unternehmens-IT ein Pflichtenheft mit auf den Weg geben und zusätzlich mit relativ geringem Aufwand im Rahmen eines Nachtests überprüfen, ob die angemahnten Sicherheitsmängel erfolgreich beseitigt wurden. Der Revisor kann nun zunächst einmal wieder ruhig schlafen – zumindest vorübergehend. Denn ein entscheidender Unterschied zu anderen Prüfverfahren muss beim Penetrationstest immer beachtet werden: Die Systeme erhalten kein Prüfsiegel „Sichere IT“ mit einem definierten Gültigkeitszeitraum. Vielmehr ist es nicht auszuschließen, dass schon wenige Tage nach einem erfolgreich überstandenen Penetrationstest irgendwo in der Welt des Internets neue Sicherheitsschwachstellen gefunden werden, mit denen gerade noch sichere Systeme auf neue Art und Weise angreifbar werden. Gerade deshalb ist es so wichtig – je nach Komplexität und Schutzwürdigkeit der eigenen IT-Landschaft – Penetrationstest ganz systematisch in regelmäßige Prüfpläne zu integrieren. Denn die Kreativität eines Penetrationstesters besteht ja gerade darin, sich in einen Hacker mit böswilligen Absichten hineinzuversetzen und wie dieser „um die Ecke“ zu denken und dort Schwachstellen aufzudecken, die andere Prüfmethoden vielleicht nicht im Blick haben.

Wer die eigenen Maßnahmen für IT-Sicherheit auf diese Weise und immer wieder systematisch auf den Prüfstand stellt, der minimiert auch die Angriffsfläche für Hacker-Angriffe. ■

**Literaturempfehlung des Autors:**

*Aleksandra Sowa, Peter Duscha, Sebastian Schreiber: IT-Revision, IT-Audit und IT-Compliance. Praxis und Theorie der IT-Prüfung (Springer Vieweg 2015) Neuartige Instrumente und Methoden für die Arbeit innovativer IT-Revision stehen im Mittelpunkt dieses Fachbuchs. Ausgehend vom modernen, risikoorientierten Prüfungsansatz kommen auch „Hot-Topics“ wie Datenschutz, Cybersecurity, Penetrationstests und Investigationen nicht zu kurz: Eine Handreichung für Praktiker, die Prüfungen planen und durchführen.*

# Nationales Cyber-Abwehrzentrum

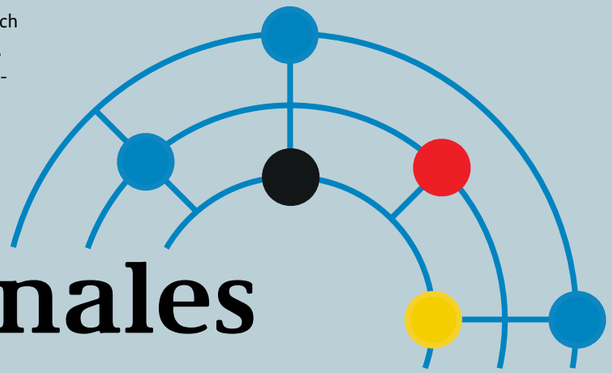
## IT-Sicherheit gemeinsam gestalten

**Die komplexen Gefahren für die IT-Sicherheit in der Bundesrepublik gehen über festgefügte Zuständigkeitsgrenzen deutscher Sicherheitsbehörden hinaus. Für sich allein kann daher weder das BSI noch eine andere Einrichtung optimal auf die dynamische Bedrohungslage reagieren. Umso wichtiger ist ein permanenter Informationsaustausch zwischen allen sicherheitsverantwortlichen Bundesbehörden als Basis für eine effektive Gefahrenabwehr und wirksame Prävention.**

Eben dies veranlasste die Bundesregierung vor vier Jahren, das Nationale Cyber-Abwehrzentrum, kurz Cyber-AZ, zu gründen. Das Zentrum ist ein Kernelement der 2011 ausformulierten Cyber-Sicherheitsstrategie (CSS), die den vorangegangenen „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ aus dem Jahr 2005 fortschrieb und gleichzeitig an die gewachsenen Herausforderungen des neuen Jahrzehnts anpasste. Unter Federführung des BSI, bei dem auch die Geschäftsstelle angesiedelt ist, beteiligen sich folgende Bundesbehörden am Cyber-AZ:

- Amt für den Militärischen Abschirmdienst
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
- Bundesamt für Sicherheit in der Informationstechnik
- Bundesamt für Verfassungsschutz
- Bundeskriminalamt
- Bundesnachrichtendienst
- Bundespolizei
- Bundeswehr
- Zollkriminalamt

Grundlage der Kooperation im Sinne höherer IT-Sicherheit sind spezielle Verwaltungsvereinbarungen zwischen den beteiligten Behörden – und zwar unter strikter Wahrung der gesetzlichen Aufgaben- und Befugnisverteilung aller mitwirkenden Stellen. Von Bedeutung sind insbesondere das Legalitätsprinzip sowie das Trennungsgebot zwischen Nachrichtendiensten und Polizei. Jede Behörde entsendet in Eigenverantwortung eine Verbindungsperson als ihren Mitarbeiter ins Cyber-AZ, wobei dessen Leitung dem BSI-Vertreter unterliegt. Der Präsident des BSI ist Sprecher des Cyber-AZ und somit dessen oberster Repräsentant.



# Nationales Cyber-Abwehrzentrum



*Besonders hilfreich sind die vielfältigen Synergien, die sich aus dem regelmäßigen Wissenstransfer im Cyber-Abwehrzentrum ergeben.*

**Ganzheitliches Lagebild, fundierte Handlungsempfehlungen**

Das zentrale Arbeitsinstrument des Cyber-AZ ist die tägliche Lagebesprechung: Hier kommen aktuelle Vorfälle und Erkenntnisse aus den beteiligten Behörden zur Sprache und werden je nach Brisanz zur vertiefenden Betrachtung an thematisch spezialisierte Expertenteams verwiesen. Die fachliche Analyse sicherheitsrelevanter Vorfälle bereichert einerseits das aktuelle Lagebild und erlaubt andererseits die Ableitung konkreter Handlungsempfehlungen, die sich an einschlägige politisch-operative Stellen oder aber auch an den Nationalen Cyber-Sicherheitsrat richten.

Um das Lagebild der IT-Sicherheit noch weiter zu vervollständigen, sieht die CSS künftig auch eine verstärkte Mitwirkung solcher Stellen vor, denen die Aufsicht sogenannter kritischer Infrastrukturen – kurz KRITIS – obliegt. Gemeint sind mit KRITIS Organisationen von herausragender Bedeutung für das Gemeinwesen wie etwa Wasser- oder Stromversorger. Besonders schutzbedürftig ist die IT solcher Einrichtungen, weil eine massive Funktionsbeeinträchtigung oder gar ein Ausfall im schlimmsten Fall Versorgungsengpässe oder erhebliche Störungen der öffentlichen Sicherheit nach sich ziehen könnte. Die Teilnahme von Vertretern KRITIS-beaufsichtigender Stellen am Cyber-AZ speist zusätzliche Informationen aus unterschiedlichen Sektoren in das Gesamtlagebild ein und ermöglicht so noch breitere und fundierte Empfehlungen.

Hervorzuheben bleibt, dass die beteiligten Behörden und Institutionen ungeachtet der engen Kooperation im Cyber-AZ alle operativen Aufgaben je nach Zuständigkeit weiterhin in Eigenverantwortung wahrnehmen. Hilfreich dafür sind jedoch die vielfältigen Synergien, die sich insbesondere aus dem regelmäßigen Wissenstransfer im Cyber-AZ ergeben.

In den vier Jahren seines Bestehens hat das Cyber-AZ sowohl seine organisatorische Struktur als auch seine Arbeitsschwerpunkte und Kooperationsmodelle kontinuierlich weiterentwickelt. Es vollzog dabei erfolgreich die Wandlung von einer reinen Informationsdrehscheibe hin zur zentralen Kooperationsplattform für Institutionen, die für die IT-Sicherheit in Deutschland Verantwortung tragen. ■


- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
- Bundesamt für Sicherheit in der Informationstechnik
- Amt für den Militärischen Abschirmdienst
- Bundesamt für Verfassungsschutz
- Bundesnachrichtendienst
- Bundeskriminalamt
- Zollkriminalamt
- Bundespolizei
- Bundeswehr

# Der Gipfel der Cyber-Sicherheit

## Ein Blick hinter die Kulissen der G7-Konferenz

**Für Anfang Juni hatte Bundeskanzlerin Angela Merkel sechs Staatschefs der G7 zum Gipfel nach Schloss Elmau in Bayern eingeladen – eine organisatorische Mammutaufgabe, die vor allem die Sicherheitsexperten vor immense Herausforderungen gestellt hat. Neben der physischen Absicherung musste die Konferenz auch vor Cyberbedrohungen geschützt werden. Letzten Endes trug die erfolgreiche Zusammenarbeit aller beteiligten Akteure dazu bei, dass Schloss Elmau für zwei Tage zu einem Cyber-Hochsicherheitstrakt wurde, in dem sich die Regierungschefs ungestört austauschen konnten.**

Die Bilder der Eskalation rund um die Eröffnung des EZB-Gebäudes in Frankfurt standen noch lebendig vor Augen – doch neben diesen physischen Bedrohungen spielte die Bedrohung der IT-Sicherheit bei dem G7-Gipfel im Juni eine zunehmende Rolle. Dabei galt es, vor Ort die Netze für die Delegationen, aber auch für die mehr als 5.000 angereisten Journalisten zu schützen sowie die verschiedenen Webauftritte, die über den Gipfel informierten, abzusichern. Hinzu kamen die Netze und Webauftritte der unterstützend am Gipfel beteiligten und weiteren Behörden der Bundesverwaltung, die für Cyber-Kriminelle potenzielle Gelegenheitsziele darstellen.

Ergänzend fand eine Abstimmung mit den Landesbehörden, sowohl den Polizeien, als auch im deutschen VerwaltungsCERT-Verbund mit den LänderCERTs, statt. Frühzeitig wurden Informationen über Bedrohungen und Schutzmaßnahmen ausgetauscht und diskutiert.



### Hochkritische Einschätzung

Nach verschiedenen größeren IT-Sicherheitsvorfällen im Vorfeld wurde die Cyber-Bedrohungslage als hoch eingestuft und floss auch so ins Bundeslagebild des Bundeskriminalamtes und des Bundesinnenministeriums ein. So gab es Anfang des Jahres 2015 Distributed Denial of Service (DDoS)-Angriffe, die die Webseiten der Bundesverwaltung im Zuge des Besuchs des ukrainischen Ministerpräsidenten lahmgelegt hatten. Zudem wurden nach den Anschlägen auf die Redaktion des französischen Satiremagazins „Charlie Hebdo“ und später auch in Deutschland Massendefacements mit islamistischen Hintergrund sowie schwere Verfügbarkeitsangriffe auf den Fernsehsender TV5 in Frankreich bekannt. Diese wahrscheinlich politisch motivierten Hacktivisten aus dem In- und Ausland wurden als Hauptbedrohung angesehen.

Über diese einmaligen Aktionen hinaus besteht aber auch dauerhaft die Gefahr der klassischen Spionage, um die Verhandlungspositionen der Delegationen und Sherpas oder die Abschlussdokumente frühzeitig zu erfahren. Kriminelle hätten den hohen Nachrichtenwert des Gipfels für Spam oder Phishing-Angriffe nutzen können. Politische Großereignisse sind zudem immer potenzielle Ziele für Terroristen, die durch Anschläge, auch im Cyber-Raum, Aufmerksamkeit gewinnen und Angst verbreiten wollen.

### Kooperative Abwehr

Deshalb wurden bereits im Vorfeld der Veranstaltung die Bundesverwaltung und viele Beteiligte für Schutzmaßnahmen insbesondere ihrer Außenschnittstellen sensibilisiert. Bei solchen Großereignissen gilt es vor allem, die Kommunikation zwischen den verschiedenen Beteiligten in den Behörden – IT-Sicherheitsbeauftragte, Öffentlichkeitsarbeit, Webseiten-Gestalter und -Hoster – zu verbessern. Hierfür hat sich ein Ansatz bewährt, bei dem die Akteure gemeinsam die verschiedenen Angriffsmöglichkeiten diskutieren. Wichtig ist, dass schon bei der Vertragsgestaltung und Beauftragung IT-Sicherheitsaspekte eingebracht werden. Spätestens im Betrieb muss die Sicherheit der Verfügbarkeit, aber auch die Integrität der Inhalte gegen Defacement oder Malware-Verteilung sichergestellt sein.

Für besonders gefährdete Webauftritte wurde durch das BSI ein Penetrationstest durchgeführt, um eventuelle Schwachstellen zu entdecken und schnellstmöglich abstellen zu lassen. Alle Behörden wurden aufgefordert, ihren DDoS-Schutz zu überprüfen und die notwendigen Absprachen mit den Hostern zu treffen. Nur dann kann im Angriffsfall schnell und geplant reagiert werden. In diesem Zusammenhang sollten auch Reaktionen für den Fall geplant werden, dass die üblichen Schutzmechanismen aufgrund der übergroßen Bandbreite nicht mehr ausreichen und in den höheren Netzebenen Maßnahmen ergriffen werden müssen.

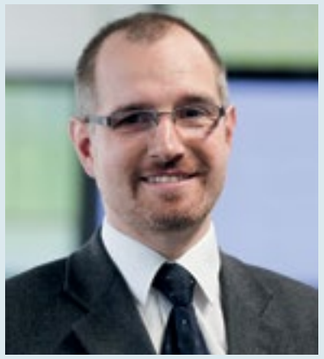
*Politische Großereignisse sind immer potenzielle Ziele, um Aufmerksamkeit zu gewinnen oder Angst zu verbreiten.*

### Lauschabwehr: Achtung, Feind hört mit

Einen besonderen Anteil an der Absicherung des Gipfels durch das BSI nahmen die Kollegen von der Lauschabwehr wahr. Sie prüften im Vorfeld die Räume auf versteckte Abhöreinrichtungen und überwachten während des Gipfels das Frequenzspektrum auf Anomalien, die auf Lauschangriffe hindeuten könnten. Auf die Hintergründe zu den Vorbereitungen und getroffenen Maßnahmen der Lauschabwehr beim Treffen der G7 in Elmau geht der nachfolgende Beitrag „Damit Vertrauliches vertraulich bleibt“ ein.

### Positives Fazit: keine besonderen Vorkommnisse

Die verschiedenen Vorveranstaltungen des Gipfels, die Treffen unterschiedlicher Ministerrunden blieben ereignislos für das BSI. Der Gipfel selbst konnte durch kleinere Angriffe nicht beeinträchtigt werden. Ein DDoS-Angriff gegen Gipfelwebseiten wurde abgewehrt, eine angriffsbedingte Störung in Teilen des Netzes für die Presse wurde nach kurzer Zeit behoben. Im Hintergrund hielt das BSI rund um die Uhr Kräfte bereit, die die IT-Infrastruktur des Bundes überwachten und verfügbar waren, um bei größeren Angriffen zu unterstützen. ■



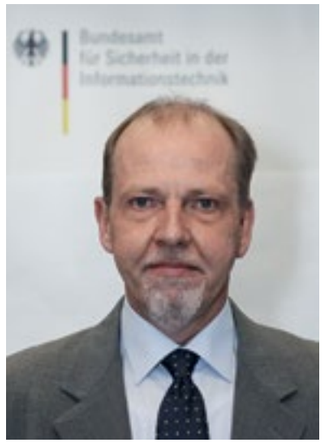
*Stefan Ritter, als Referatsleiter des Lagezentrums und CERT-Bunds für die IT-Absicherungsmaßnahmen durch das BSI verantwortlich*

# Damit Vertrauliches vertraulich bleibt

**Die Inhalte politischer Gespräche sind nichts für fremde Ohren. Gelangen Menschen mit kriminellen, gar terroristischen Absichten in den Besitz vertraulicher Informationen, kann dadurch unter Umständen die Sicherheit eines ganzen Landes bedroht sein. Daher genießt die Lauschabwehr bei Veranstaltungen wie dem G7-Gipfel höchste Priorität. Das BSI verfügt nicht nur über die erforderliche Technik, sondern bringt vor allem auch die notwendige Expertise mit, damit sich die Politiker austauschen können, ohne befürchten zu müssen, dass sie abgehört werden. Das Fazit: Es wurde kein illegaler Abhörangriff festgestellt.**

**Acht Fragen und Antworten zur BSI-Lauschabwehr beim Treffen der G7 in Elmau.**

**1. Warum ist eine Lauschabwehr bei einer Veranstaltung wie dem G7-Gipfel wichtig?**
Im Rahmen des deutschen G7-Vorsitzes fand in diesem Jahr der Gipfel im bayerischen Elmau statt. Ein wichtiger Aspekt solcher Treffen ist, dass die in vertraulichem Rahmen geführten Unterredungen auch vertraulich bleiben und Gesprächsinhalte nicht an Unbefugte gelangen. Die Lauschabwehr des BSI war deshalb in Elmau dabei, um die Abhörsicherheit der Veranstaltung zu gewährleisten.




*Volker Fricke, Referatsleiter "Lauschabwehr"*



**2. Welche Rolle spielte das BSI bei der Veranstaltung?**
Die Vorbereitungen hierfür begannen bereits einige Monate vorher, indem das Auswärtige Amt als Gipfel-Veranstalter durch das BSI beraten wurde, welche technischen und organisatorischen Maßnahmen für die Vertraulichkeit förderlich sind beziehungsweise welche eher vermieden werden sollten.

**3. Was sind die größten Schwachstellen für Lauschangriffe?**
Bei internationalen Veranstaltungen werden üblicherweise Dolmetscheranlagen aufgebaut, um die Gespräche in die Muttersprachen aller Teilnehmer zu übersetzen.Problematisch sind in diesem Zusammenhang Dolmetscheranlagen, die Gesprächsinhalte mittels unsichtbaren Infrarotlichts übertragen. Diese Infrarotstrahlung kann die Fenster der Konferenzräume fast ungedämpft durchdringen, sodass die Gespräche im Außenbereich auch aus weiter Entfernung mit

*Die GSM-Wanze bietet auf kleinstem Raum die Funktionalität eines Mobiltelefons, um Raumgespräche abzuhören.*

verhältnismäßig geringem Aufwand abhörbar sind. Deshalb wurde beim G7-Gipfel ausschließlich kabelgebundene Dolmetschertechnik eingesetzt.

**4. Welches Gefahrenpotenzial bergen mobile Endgeräte der Teilnehmer?**
Eine weitere Schwachstelle kann sein, dass Teilnehmer mobile Endgeräte (zum Beispiel Smartphones, Tablets) in die vertraulichen Besprechungen mitbringen, sofern nicht sicher ausgeschlossen werden kann, dass eine Schadsoftware Gesprächsinhalte aufzeichnet und an Unbefugte sendet. Das BSI bietet daher den Einsatz eines Mobilfunk-Detektionssystems an, mit dem unerwünscht eingebrachte Geräte erkannt und geortet werden können.

**5. Welche Aufgaben hat das BSI konkret vor Ort übernommen?**
Die Arbeit des Lauschabwehr-Teams „vor Ort“ bestand im Wesentlichen aus zwei Komponenten: der Überprüfung gefährdeter Räume auf versteckte Abhöreinrichtungen und einer kontinuierlichen Überwachung des Hochfrequenzspektrums hinsichtlich Anomalien, die auf aktive Abhörgeräte hinweisen.

**6. Wie werden die Räumlichkeiten vorab präpariert, damit sie abhörsicher sind?**
Die Raumüberprüfungen wurden unter anderem in den Konferenzräumen sowie in Bereichen durchgeführt, die für vertrauliche bilaterale Besprechungen vorgesehen waren. Sie begannen bereits gleichzeitig mit der Konferenzmöblierung, weil während dieser Arbeiten Hohlräume verschlossen werden mussten, die als Versteck für Abhörtechnik geeignet waren. Neben den visuellen Untersuchungen wurden die Räume auch mit speziellen Lauschabwehr-Prüfgeräten inspiziert. Dies schloss auch die technische Infrastruktur wie Beleuchtung und Verkabelung ein. Zeitgleich zur Möblierung der Konferenzräume wurden auch die Hochfrequenzempfänger und zugehörige Antennen eingebaut. Idealerweise geschieht das möglichst nahe am Konferenzgeschehen, um die Ortung verdächtiger Signale zu erleichtern.

**7. Wie ist es gelungen, die Schutztechnik so unauffällig zu installieren, dass sich die Gipfelteilnehmer dennoch in entspannter Atmosphäre unterhalten konnten?**
In Elmau wurden Besprechungstische mit einem großem Hohlraum im Fuß aufgebaut, der genügend Platz für die Technik bot. Die Steuerung der Empfänger erfolgt über ein schnelles IP-Rechnernetz, so dass eine vorhandene Netzwerk-Infrastruktur genutzt werden konnte. Eine Bedienung und Auswertung der Messergebnisse konnte deshalb von einer zentralen Stelle aus durchgeführt werden, nämlich dem Standort der Dolmetscher-Hauptregie und der Dolmetscherkabinen.


*Eine in der Uhr eingebaute Kamera zeichnet unbemerkt Bild und Ton der Umgebung auf.*

**8. Wie funktioniert die Technik im Hintergrund?**
Darüber hinaus wurde im Außenbereich, in unmittelbarer Nähe der Konferenzräume, ein Messfahrzeug des BSI abgestellt. In diesem Fahrzeug befinden sich ein weiterer Hochfrequenzempfänger und ein leistungsfähiges Peilsystem. Damit war es möglich, die im Vorfeld und während der Gespräche auftretenden ungewöhnlichen Hochfrequenzsignale, die auf einen illegalen Abhörangriff hindeuten könnten, mit den Ergebnissen aus den Konferenzräumen zu vergleichen und zu beurteilen, ob der Ursprung der Signale im Konferenzgebäude oder außerhalb liegt. ■

# Das IT-Sicherheitsgesetz

## Im Gespräch mit Steve Ritter und Dr. Timo Hauschild über die neuen Aufgaben des BSI

**Nach langen Vorarbeiten und vielen Diskussionen ist das IT-Sicherheitsgesetz im Juli in Kraft getreten. Was ändert sich jetzt?**

**Steve Ritter:** Mit dem IT-Sicherheitsgesetz ändert sich eine ganze Menge, sowohl für das BSI als auch für die Wirtschaft. Das BSI hat vom Gesetzgeber den klaren Auftrag erhalten, sich noch intensiver als bisher um die IT-Sicherheit der Bundesverwaltung zu kümmern. Es ist vorgesehen, dass das BSI vermehrt Mindeststandards erarbeitet, die alle Bundesbehörden umsetzen sollen bzw. nach Verbindlicherklärung durch das Bundesministerium des Innern sogar umsetzen müssen.

Aber auch außerhalb der Bundesverwaltung soll das BSI künftig eine größere Rolle spielen. Am deutlichsten wird das im Bereich der Kritischen Infrastrukturen. Diese soll das BSI künftig unterstützen – entweder selbst oder durch qualifizierte Dienstleister – und noch stärker als schon heute mit Informationen versorgen. Dadurch sollen die Betreiber in die Lage versetzt werden, ihre IT besser abzusichern. Nach dem Vorbild der zentralen Meldestelle für die Bundesverwaltung wird das BSI auch zur zentralen Meldestelle für IT-Sicherheit für Betreiber Kritischer Infrastrukturen. Die Betreiber Kritischer Infrastrukturen sollen einerseits Informationen von der Meldestelle im BSI erhalten, aber andererseits auch eigene erhebliche IT-Sicherheitsvorfälle an das BSI melden, damit andere Betreiber rechtzeitig vor Angriffen gewarnt werden können.

**Timo Hauschild:** Was aber noch viel wichtiger ist: Betreiber Kritischer Infrastrukturen müssen ihre relevante IT künftig nach dem Stand der Technik absichern und die Umsetzung der Sicherheitsmaßnahmen durch regelmäßige Prüfungen belegen. Grund hierfür ist, dass heutzutage fast alle Kritischen Infrastrukturen,



*Heutzutage müssen nicht mehr nur die Kritischen Infrastrukturen selbst, sondern auch die dafür nötigen IT-Systeme gesichert werden.*

*Steve Ritter, Referent „IT-Sicherheit und Recht"*

*Dr. Timo Hauschild, Referatsleiter „Schutz kritischer Infrastrukturen"*

also z. B. auch die Versorgung mit Wasser oder Lebensmitteln, von funktionierender IT abhängen. Daher müssen nicht mehr nur die Infrastrukturen selbst, sondern auch die dafür nötigen IT-Systeme abgesichert werden. Zumindest wenn wir nicht eines Tages alle auf dem Trockenen sitzen wollen, weil ein Hacker sich Zugriff auf die IT eines Wasserwerks verschafft hat.

Die Ausgestaltung der Absicherung bleibt größtenteils den Betreibern selbst überlassen. Lediglich für die Bereiche der Energienetze und -anlagen sowie der öffentlichen Telekommunikationsnetze werden konkrete Vorgaben durch die Bundesnetzagentur in Katalogen veröffentlicht – aufbauend auf Vorgaben, die es auch schon vor Inkrafttreten des IT-Sicherheitsgesetzes gab.

**Verpflichtungen für Webseitenbetreiber und Hoster**

Nach § 13 Absatz 7 TMG werden Diensteanbieter für geschäftsmäßig angebotene Telemedien zu einem besseren Schutz ihrer IT-Einrichtungen verpflichtet. Diensteanbieter sind je nach Fallgestaltung z.B. die Betreiber einer Webseite und deren Webhoster. Soweit technisch möglich und wirtschaftlich zumutbar, müssen sie Maßnahmen nach dem Stand der Technik gegen unerlaubte Zugriffe auf ihre Systeme und personenbezogenen Daten sowie gegen Störungen (zum Beispiel durch Angriffe) absichern.

Eine der nach Beobachtungen des BSI am häufigsten unterlassenen Sicherungsmaßnahmen stellt z.B. das Nichteinspielen von Updates und Sicherheitspatches dar. Dadurch wird es Angreifern u.a. erleichtert, über die jeweilige Webseite Schadsoftware an die Besucher der Webseite zu verteilen.

*Wichtig:* Unter die Regelung fallen nur gewerbliche Webseiten; private oder Vereinswebseiten werden also in der Regel nicht betroffen sein. Allerdings kann eine Webseite bereits dann gewerblich sein, wenn durch sie Einnahmen erzielt werden, etwa durch Werbung.

**Was passiert jetzt gerade konkret?**

**SR:** Die Melde- und Absicherungspflichten gelten nicht für alle zum gleichen Zeitpunkt. Schon jetzt müssen die Inhaber atomrechtlicher Genehmigungen IT-Sicherheitsvorfälle an das BSI melden. Auch die Betreiber öffentlicher Telekommunikationsnetze und -dienste müssen ihre verschärften Absicherungs- und Meldepflichten nach dem Telekommunikationsgesetz (TKG) sofort erfüllen.

Eine Schonfrist haben hingegen die meisten Betreiber Kritischer Infrastrukturen. Denn erst in einer Rechtsverordnung wird endgültig festgelegt, was eine Kritische Infrastruktur – im Sinne des BSI-Gesetzes – ist. Daher können die entsprechenden Verpflichtungen vorher noch keine Wirkung entfalten.

| | Pflicht zur Umsetzung IT-Sicherheit nach Stand der Technik | Pflicht zur Überprüfung der Absicherung (z.B. durch Audit) | Unverzügliche Versorgung mit relevanten Informationen durch BSI | Meldepflicht von IT-Sicherheitsvorfällen | Möglichkeit der Beratung und Unterstützung durch das BSI |
|---|---|---|---|---|---|
| **KRITIS-Betreiber gemäß BSI-KRITIS-Verordnung (bis auf die Sonderfälle, siehe die drei folgenden Zeilen)** | Ja. Konkretisierung in Branchen spätestens 2 Jahre nach Inkrafttreten der Verordnung | Ja. Überprüfung und Nachweis alle 2 Jahre, erstmalig 2 Jahre nach Infkrafttreten der Verordnung. | Ja. | Ja. Spätestens ½ Jahr nach Inkrafttreten der Verordnung. | Ja. |
| **Öffentliche Telekommunikationsnetze gemäß BSI-KRITIS-Verordnung** | Ja. Konkretisierung durch IT-Sicherheitskatalog nach §109 TKG. (Altregelung) | BNetzA überprüft Umsetzung alle 2 Jahre. | Ja. | Ja, sofort. Meldepflicht an die BNetzA (Erweiterung einer Altregelung) | Ja. |
| **Öffentliche Telekommunikationsnetze (sonstige Betreiber)** | Ja. Konkretisierung durch IT-Sicherheitskatalog nach §109 TKG. (Altregelung) | BNetzA überprüft Umsetzung alle 2 Jahre. | Nein. | Ja, sofort. Meldepflicht an die BNetzA (Erweiterung einer Altregelung) | Nein. |
| **Energieversorgungsnetze gemäß BSI-KRITIS-Verordnung** | Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG (Erweiterung einer Altregelung) | Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG | Ja. | Ja. Mit Inkrafttreten der Verordnung. | Ja. |
| **Energieversorgungsnetze (sonstige Betreiber)** | Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG (Erweiterung einer Altregelung) | Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG | Nein. | Nein. | Nein. |
| **Energieanlagen gemäß BSI-KRITIS-Verordnung** | Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1b) EnWG | Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1b) EnWG | Ja. | Ja. Mit Inkrafttreten der Verordnung. | Ja. |
| **Genehmigungsinhaber nach §§ 6, 7 oder 9 Atomgesetz (z.B. Kernkraftwerke, atomare Lager)** | Ja. (Keine Änderung zum bestehenden Atomgesetz.) | Ja. (Keine Änderung zum bestehenden Atomgesetz). | Ja. | Ja (seit 25.07.2015). | Nein. Es sei denn, sie sind KRITIS-Betreiber. |

*Mit dem IT-Sicherheitsgesetz werden für KRITIS-Betreiber im Wesentlichen 5 Neuerungen eingeführt. Auf welche Betreiber welche Neuerungen wann und wie zutreffen, kann der Tabelle entnommen werden.*

→ **TH:** Zurzeit arbeitet das Bundesministerium des Innern zusammen mit uns sowie den fachlich zuständigen Ministerien und Aufsichtsbehörden und auch mit Vertretern der Branchen an der Frage, welche Betreiber konkret unter die neuen Regelungen des BSI-Gesetzes fallen; das soll im Rahmen der BSI-KRITIS-Verordnung geregelt werden. Die Verordnung wird in zwei Teilen erarbeitet: zuerst für die Sektoren Energie, IKT, Ernährung und Wasser, später dann für die Sektoren Transport und Verkehr, Finanzen und Gesundheit.

Sobald die Verordnung in Kraft getreten ist, haben die betroffenen Betreiber zwei Jahre Zeit, um den Stand der Technik in Bezug auf ihre IT-Sicherheit umzusetzen und dem BSI nachzuweisen. Außerdem muss dem BSI eine Kontaktstelle benannt werden, über die die Meldungen an das BSI (und ggf. Rückfragen des BSI) erfolgen können. Dies muss spätestens sechs Monate nach Inkrafttreten der Verordnung passieren.

Das BSI bereitet sich aktuell intensiv auf die neuen Aufgaben vor. Hier gibt es noch viel zu tun. Beispielsweise müssen die Meldekriterien und Meldewege festgelegt werden. Außerdem muss konkretisiert werden, was „Stand der Technik“ in Bezug auf IT-Sicherheit ist. Um hier Rechtssicherheit zu haben, können die Branchen branchenspezifische Sicherheitsstandards erarbeiten, die bei Eignung vom BSI anerkannt werden.

*Je mehr Menschen von einer Anlage mit einer kritischen Dienstleistung versorgt werden, umso wichtiger ist es, dass diese nicht ausfällt.*

### Verpflichtung der Provider

Betreiber öffentlicher Telekommunikationsnetze (das sind z.B. die Telekommunikationsgesellschaften) und Anbieter von öffentlich zugänglichen Telekommunikationsdiensten (das sind z.B. E-Mail-Dienstanbieter) haben künftig beträchtliche Sicherheitsverletzungen an Netzen oder Diensten der Bundesnetzagentur (BNetzA) zu melden. Dazu gehören insbesondere auch solche Vorfälle, die zu unerlaubten Zugriffen auf die IT ihrer Kunden führen könnten. Bei Bedarf kann die BNetzA die Öffentlichkeit informieren. Sofern die IT-Sicherheit betroffen ist, gibt die BNetzA die Informationen in jedem Fall an das BSI weiter. Die BNetzA kann die Netzbetreiber und Diensteanbieter zu Absicherungsmaßnahmen verpflichten.

Wenn einem Diensteanbieter Störungen auf den IT-Systemen seiner Nutzer bekannt werden, ist er verpflichtet, diese Nutzer darüber zu informieren. Diese Pflicht besteht allerdings nur, sofern der Nutzer dem Anbieter bereits bekannt ist. Im zumutbaren Rahmen ist der Anbieter verpflichtet, seine Nutzer auf Werkzeuge (z.B. Antiviren-Programme) hinzuweisen, mit denen die Nutzer selbst diese Störungen erkennen und beseitigen können.

**Wird das alles in der Rechtsverordnung geregelt?**

**SR:** Diese Erwartung hört man häufig. Es ist aber so, dass sich die Regelungen einer Rechtsverordnung nur in dem Rahmen bewegen dürfen, der vom Gesetz vorgegeben ist. Im Fall des IT-Sicherheitsgesetzes darf das BMI in der Rechtsverordnung nur regeln, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne des BSI-Gesetzes anzusehen sind. Daher darf die Verordnung gar keine Regelungen zu Meldewegen, Meldeschwellen, Auditoren oder anderen Themen enthalten.

**TH:** Genau, das IT-Sicherheitsgesetz ergänzt den seit Jahren mit dem UP KRITIS verfolgten kooperativen Ansatz zum Schutz Kritischer Infrastrukturen um einige wenige verpflichtende Elemente (der Beitrag „Kritische Infrastrukturen“ hierzu erschien im BSI-Magazin 2013/14). Und ganz in diesem Sinne wird die Ausgestaltung des Gesetzes auch kooperativ angegangen. Schon heute sind wir in intensiven Diskussionen in den Gremien des UP KRITIS, um den Rahmen für die branchenspezifischen Sicherheitsstandards zu definieren. Gleiches gilt für die Umsetzung der Meldepflicht und die Bedarfe und Wünsche der Betreiber an die zukünftig durch das BSI zu verteilenden Informationen.

Die BSI-KRITIS-Verordnung hingegen regelt das „Wer?“. Sie wird daher Angaben zu qualitativen und quantitativen Kriterien enthalten, anhand derer jeder KRITIS-Betreiber prüfen kann, ob er Anlagen betreibt, die zu den Kritischen Infrastrukturen im Sinne des Gesetzes gehören. Das qualitative Kriterium wird die Erbringung einer kritischen Dienstleistung sein. Eine solche Dienstleistung ist beispielsweise die Wasserversorgung, die Stromversorgung oder die Versorgung mit Lebensmitteln. Die quantitativen Kriterien enthalten hierzu dann Schwellenwerte, etwa in Bezug auf den Versorgungsgrad, denn letztlich geht es darum, wie viele Menschen von einer Anlage tatsächlich oder potenziell versorgt werden. Im Fokus stehen dabei immer die möglichen Folgen eines Ausfalls einer Anlage für die Bevölkerung in Deutschland.

**Nun betreffen die Neuerungen durch das IT-Sicherheitsgesetz nicht ausschließlich die Betreiber Kritischer Infrastrukturen. Was ändert sich für die Bürger?**

**SR:** Nun, von den Regelungen zum Schutz Kritischer Infrastrukturen profitieren die Bürger mittelbar. Sie bleiben dadurch hoffentlich von Ausfällen z.B. des Stroms oder der Wasserversorgung verschont. Jedenfalls sollten solche dann nicht auf Hackerangriffe oder IT-Sicherheitsrisiken zurückgehen.

→ Aber es gibt auch eine Reihe von Regelungen, von denen die Bürger unmittelbar profitieren. So müssen z.B. die Telekommunikationsanbieter ihre Nutzer jetzt benachrichtigen, wenn sie feststellen, dass von deren IT-Systemen Störungen ausgehen – etwa weil sie Teil eines Botnetzes sind. Die Nutzer müssen außerdem auf Werkzeuge hingewiesen werden, mit denen sie diese Störungen erkennen und beseitigen können. Sie sind damit nicht mehr ganz auf sich allein gestellt, sondern können vom Wissen ihrer Telekommunikationsanbieter profitieren.

Eine der weitreichendsten Änderungen, von denen die Bürger profitieren werden, ist eine Änderung im Telemediengesetz (TMG), nämlich die Verpflichtung der Webseitenbetreiber und ihrer Hoster, ihre IT künftig nach dem Stand der Technik gegen unerlaubte Zugriffe und Störungen abzusichern. Dadurch soll es Angreifern erschwert werden, über seriöse Webseiten Schadsoftware zu verbreiten. Diese sogenannten Drive-by-Downloads, bei denen sich die Nutzer durch den bloßen Besuch einer Webseite infizieren, sind nach wie vor ein großes Problem.


*Die Kritischen Infrastrukturen sind in neun Sektoren unterteilt.*

**Produktuntersuchungen durch das BSI**

Um sichergehen zu können, dass ein IT-Produkt frei von Schwachstellen ist, sind eingehende Untersuchungen notwendig. Viele Untersuchungsmethoden des sogenannten „Reverse Engineerings“ sind jedoch bisher mit rechtlichen Risiken behaftet. Damit das BSI seine Aufgaben im Hinblick auf die Bundesverwaltung und den Schutz Kritischer Infrastrukturen erfüllen kann, erhält es daher im neuen § 7a BSIG die Befugnis, IT-Produkte zu untersuchen. Stellt es bei seinen Untersuchungen Sicherheitslücken fest, darf es – nach vorheriger Einbindung des Herstellers – auch die Öffentlichkeit warnen, falls das erforderlich ist.

Eine „Stiftung Warentest“ für IT-Produkte wird das BSI dadurch jedoch nicht. Umfangreiche Tests und Vergleiche von IT-Produkten werden bereits heute in vielen Fachpublikationen veröffentlicht, mit denen das BSI nicht in Konkurrenz treten wird.

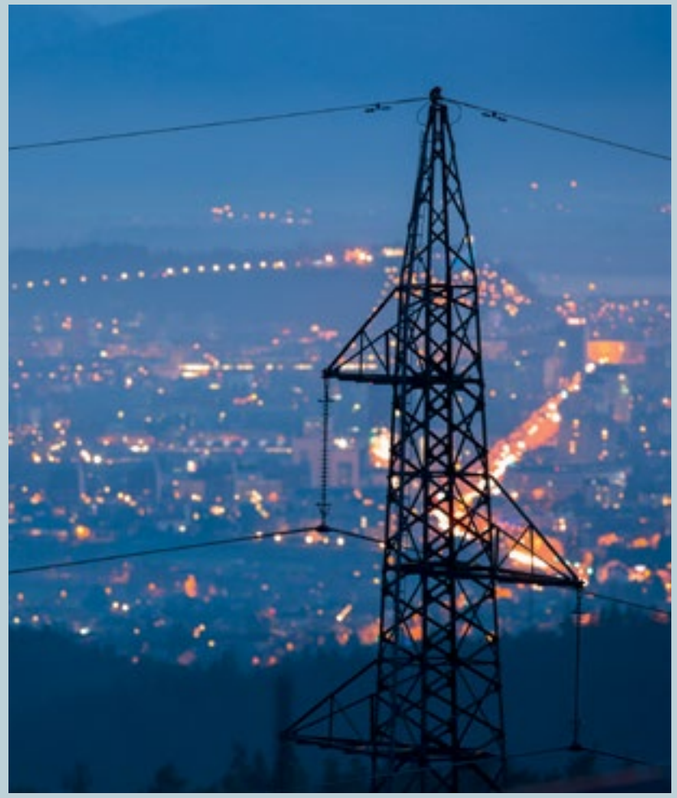
Doch auch der Diebstahl von personenbezogenen Daten der Bürger durch Angriffe auf Webserver wird durch die Umsetzung der Absicherungspflicht erschwert. Oftmals haben Webseitenbetreiber in der Vergangenheit selbst einfachste Maßnahmen, wie das Einspielen von Sicherheitspatches, unterlassen und den Angreifern den Datendiebstahl dadurch besonders leicht gemacht. Das ändert sich jetzt hoffentlich, sodass sich die Bürger sicherer im Internet bewegen können.



**Das klingt nach einer ganzen Reihe an Neuerungen. Kann das BSI das überhaupt bewältigen?**

**TH:** Das IT-Sicherheitsgesetz zielt ausdrücklich auf eine Stärkung des BSI ab. Mit den neuen Aufgaben kommen auch neue Stellen, also neue Mitarbeiter ins BSI. Die Personalgewinnung hat bereits begonnen. Nun gilt es, die neuen Anforderungen auch organisatorisch umzusetzen. Aber vieles baut auf Dingen auf oder erweitert Dinge, die das BSI bereits seit Jahren tut. Insofern sind wir überzeugt, dass wir die neuen Pflichten auch gut bewältigen können.

**SR:** Das kann ich nur unterstreichen. Ein wesentlicher Erfolgsfaktor hierbei ist, dass die zuständigen Bereiche im BSI seit Jahren intensiv und gut zusammenarbeiten. Ohne diese gelungene Teamarbeit von Personen verschiedenster Ausbildung hätten wir keine Chance, ein so dynamisches Thema immer wieder neu zu bewältigen. ■



**Verpflichtungen für KRITIS-Betreiber** Betreiber Kritischer Infrastrukturen werden durch die Neuregelungen des BSI-Gesetzes dazu verpflichtet, ihre informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, gemäß dem Stand der Technik abzusichern, um Störungen oder Ausfälle dieser Systeme zu vermeiden.

Die Betreiber müssen regelmäßig – spätestens alle zwei Jahre – die Einhaltung des Stands der Technik gegenüber dem BSI nachweisen. Der Stand der Technik kann für eine Branche im Rahmen eines branchenspezifischen Sicherheitsstandards konkretisiert werden, den die jeweiligen Branchen erarbeiten können.

Außerdem werden die unter das Gesetz fallenden KRITIS-Betreiber verpflichtet, erhebliche Sicherheitsvorfälle, d.h. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit, die die Funktionsfähigkeit der Kritischen Infrastrukturen beeinträchtigen können oder beeinträchtigt haben, an das BSI zu melden.

Das BSI wird zudem zur zentralen Meldestelle für Betreiber Kritischer Infrastrukturen in Bezug auf die Sicherheit in der Informationstechnik. Es bekommt die Aufgabe, Informationen, die für die Abwehr von Gefahren für die Informationstechnik wesentlich sind, zu sammeln, auszuwerten und deren potenzielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen zu untersuchen, ein Lagebild zu erstellen und kontinuierlich fortzuschreiben und die KRITIS-Betreiber sowie die zuständigen (Aufsichts-)Behörden zu unterrichten. KRITIS-Betreiber werden durch das Gesetz also nicht nur zur Meldung verpflichtet, sondern erhalten im Gegenzug vom BSI Informationen, Bewertungen und Empfehlungen. Darüber hinaus kann das BSI die KRITIS-Betreiber auf deren Wunsch bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen. Damit wird die Zuständigkeit des BSI für die Sicherheit der Informationstechnik der Bundesverwaltung erweitert auf die Kritischen Infrastrukturen.

# Der 14. Deutsche IT-Sicherheitskongress Bonn/Bad Godesberg

Vom 19. bis 21. Mai 2015 kam in Bonn zum 14. Mal die deutsche IT-Sicherheitsszene zusammen: Rund 600 Teilnehmer aus Politik, Verwaltung und Wirtschaft nutzten den 14. Deutschen IT-Sicherheitskongress in Bad Godesberg, um aktuelle Herausforderungen beim Schutz von IT-Systemen und der Kommunikation im Internet zu diskutieren.

Die inhaltliche Bandbreite der Keynotes, Fachvorträge und Diskussionsrunden erstreckte sich auf so unterschiedliche Themenfelder wie sichere Mobilkommunikation, IT-Sicherheitsmanagement, Cloud Computing oder Industrial Security. Deutlich wurde dabei insbesondere, dass die fortschreitende Digitalisierung nahezu aller Lebens- und Arbeitsbereiche immer neue Angriffsflächen für Cyber-Attacken schafft. Potenziell davon betroffen sind Wirtschaft, Wissenschaft und staatliche Stellen genauso wie Bürgerinnen und Bürger. In diesem Kontext herrschte weithin Konsens unter den Kongressteilnehmern, dass konventionelle Sicherheitsmechanismen heute an ihre Grenzen stoßen. Professionelles Risikomanagement dürfe sich nicht allein auf Risikovermeidung konzentrieren, sondern müsse verstärkt auch Risikominimierung mit einbeziehen. Dies aber impliziert als Konsequenz auch die Forderung nach verbesserten Möglichkeiten zur effektiven Krisenreaktion bei erfolgreichen Angriffen auf Netze und IT-Systeme. „Das Thema der Stunde ist Risikomanagement“, hob BSI-Präsident Michael Hange hervor. Seiner Ansicht nach müsse man lernen, mit Unsicherheit besser umzugehen, weil sie im Cyber-Raum ebenso wenig wie im sonstigen Leben vollständig beseitigt werden könne.

## Plädoyer gegen „digitale Sorglosigkeit“

Gleich zu Kongressbeginn konstatierte Bundesinnenminister Dr. Thomas de Maizière in seiner Eröffnungsrede eine „digitale Sorglosigkeit“ und rief in diesem Zusammenhang insbesondere Unternehmen zu mehr Eigenverantwortung auf.

Tatsächlich stieg die Infektionsrate von Rechnern im letzten Halbjahr in besorgniserregendem Ausmaß an, wie Markus Schaffrin, Geschäftsbereichsleiter beim eco-Verband, in Bad Godesberg erklärte: „Unsere Statistiken belegen, dass rund 40 Prozent der Rechner mit Schadsoftware infiziert sind. Und es ist nicht nur ein Schädling, sondern es sind im Schnitt zehn Schädlinge, die sich auf den Rechnern finden.“

Viele Unternehmen wüssten noch nicht, dass sie bereits angegriffen worden sind, kommentierte Hartmut Isselhorst, Leiter der Abteilung Cyber-Sicherheit im BSI: „Ich glaube, dass dieser Zustand sich ändern wird, sobald erste Erfahrungen mit Angriffen gemacht werden.“ Dann allerdings trete meist eine „digitale Hilflosigkeit“ ein, so der Abteilungsleiter weiter. Mit umfangreichen Informationsangeboten und Dienstleistungen böte das BSI pragmatische Unterstützung – sowohl bei der Frage, was als schnelle Reaktion im Fall der Fälle zu tun ist, als auch zur Prävention, die zu einer nachhaltig erhöhten IT-Sicherheit führt.


## IT-Security muss leicht gemacht werden

Bereits bei der Produktentwicklung ist es essenziell, IT-Sicherheit über den gesamten Lebenszyklus des Produkts hinweg zu bedenken und so zu konzipieren. Produkte müssen bei ihrer Entwicklung vom Nutzer her erstellt und entwickelt werden – wie es auch bei Tablets und Smartphones der Fall ist. Denn nur eine „leicht gemachte Sicherheit“, so der Innenminister, sei wirklich gute IT-Sicherheit. Dies bedeutet darüber hinaus auch, dass Nutzer darauf vertrauen können müssen, dass im Hintergrund laufende Funktionen und Prozesse sicher entwickelt wurden und Sicherheitslücken geschlossen werden, sobald sie aufgedeckt worden sind.

## Staat trägt Mitverantwortung

Ungeachtet ständig neu entstehender Bedrohungsszenarien habe sich die Erwartungshaltung der Bürger an den Staat nicht wesentlich geändert – es werde erwartet, dass der Staat auch im Internet eine Schutz- und Gewährleistungsfunktion übernimmt und einen Teil der Verantwortung für das Internet als Infrastruktur übernimmt. „Der Staat hat seine Rolle, seine Mitverantwortung, dafür zu sorgen, dass die Menschen frei und sicher leben können, auf eine Weise, dass kein anderer Schaden nimmt“, erklärt der Bundesinnenminister.

Ein weiterer Schwerpunkt des Kongresses war der Entwurf des mittlerweile in Kraft getretenen IT-Sicherheitsgesetzes. Es weist dem BSI neue Aufgaben zu – nämlich u.a. als zentraler Ansprechpartner für alle Fragen rund um die IT-Sicherheit Kritischer Infrastrukturen mit herausragender Bedeutung für unser Gemeinwesen zu fungieren. ■

*„Ich glaube, ein wesentlicher Aspekt dieses Kongresses ist die Tatsache, dass sich in Deutschland der Staat sehr intensiv um die IT-Sicherheit der Bürger und der Unternehmen kümmert."*

*Peter Hohl, Geschäftsführer SecuMedia Verlags GmbH*

*„Auch im Internet soll der Staat eine Schutz- und Gewährleistungsfunktion haben und trägt eine Mitverantwortung für das Internet als Infrastruktur."*

*Dr. Thomas de Maizière, Bundesminister des Innern*


*„Wir befinden uns in einem grundlegenden Wandel des Wirtschaftssystems. Durch die Digitalisierung sind Vernetzungen möglich, die wir so bisher nicht kannten."*

*Dr. Klaus Mittelbach, Vorsitzender der Geschäftsführung des Zentralverbandes der Elektrotechnik- und Elektronikindustrie e.V.*


*„Deutschland braucht ein IT-Sicherheitsgesetz, um kritische Infrastrukturen mit besonderer Bedeutung für das Gemeinwohl zuverlässig vor Cyber-Gefahren schützen zu können. Dabei ist mir der kooperative Ansatz des Gesetzes besonders wichtig."*

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

# Schätzen mit System

**Wie können IT-Sicherheitsteams den Aufwand von Schutzmaßnahmen bemessen? Eine neue Arbeitshilfe zur Planung für Ressourcen in IT-Sicherheitsteams bietet eine Lösung.**

Ein erfolgreiches Managementsystem der Informationssicherheit (ISMS) braucht Struktur, Organisation und Personal. Erhebungstechniken für quantifizierbare Aufgaben können für die Ermittlung von Personalbedarf nicht in jedem Fall eingesetzt werden, stattdessen werden überschlägig geschätzte Prognosen vorgenommen. Welche personelle Stärke ist für ein IT-Sicherheitsteam angemessen? Eine Frage, die in der Vergangenheit zu vielen ergebnisoffenen Diskussionen geführt hat. Ein Schätzverfahren zur Feststellung des Aufwandes und zur Planung des personellen Ressourceneinsatzes für IT-Sicherheitsteams, bei dem auch der Bundesrechnungshof mitgewirkt hat, ist nun als Lösung und Arbeitshilfe anerkannt. Damit lassen sich die Aufgaben zur Informationssicherheit, die Prioritätensteuerung und die zeitlichen Aufwände transparent darstellen. Das Schätzverfahren beschreibt die fachlichen Anforderungen für ein effektives ISMS und unterstützt dabei, den Mindestpersonalbedarfs zu ermitteln.

*Günther Ennen, Referatsleiter "Informationssicherheitsberatung für Behörden"*



### Möglichkeiten und Grenzen der Arbeitshilfe

Empirische Daten zur Berechnung der Aufwände für die Tätigkeiten der IS-Teams liegen nicht vor, daher ist es zulässig und hilfreich, mit Schätzungen zu beginnen. Als Basis hierfür dienen Erfahrungswerte von Behörden aus der Vergangenheit. Die Arbeitshilfe erhebt dabei keineswegs den Anspruch, zur Begründung von Bedarfsanforderungen für mehr Personal verwendet zu werden. Oft lassen sich durch eine interne Umorganisation des vorhandenen Personals die Aufgaben zur Informationssicherheit bewältigen. Die Kriterien zur Schätzung der Aufwände sind so gewählt, dass sie grundsätzlich für jede Behörde anwendbar sind. Behördenspezifische, individuelle Besonderheiten werden hierbei nicht abgebildet. Das beschriebene Vorgehen entbindet eine Behörde jedoch nicht von der Notwendigkeit, nach einer Konsolidierungsphase zusätzlich eine Personalbedarfsermittlung gemäß den im „Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung“ anerkannten Methoden durchzuführen.

### Standardbehörde als Modell

Die Arbeitshilfe geht von dem Modell einer „Standardbehörde“ aus, Abweichungen von dem gewählten „Standard“ werden auf Basis von gewichteten Wertetabellen durch prozentuale Zeitzuschläge bzw. Zeitabschläge hinsichtlich der Aufwände berücksichtigt.

**Die „Standardbehörde“**

- hat rund 500 Mitarbeiter
- verfügt über eine homogene IT-Landschaft
- betreibt IT-Systeme und IT-Verfahren mit normalem Schutzbedarf
- hat keine Außenstellen
- benötigt keine Anforderungen an die Hochverfügbarkeit von IT-Systemen oder Anwendungen

Zu den Aufgaben des ISMS zählen zunehmend die Risikobewertung aktueller Warnungen, die Reaktion auf aktuelle Sicherheitsempfehlungen sowie zeitkritische Warnungen, Hersteller-Sicherheitsupdates und Patches und die täglichen Berichte zur Lage der Informationssicherheit. Aufgaben, die gemeinhin in Zuständigkeit des IT-Betrieb erfolgen, wie z.B. Tests von Software sowie Abnahme- und Freigabeverfahren, die Mitwirkung bei der Erstellung von Testplänen oder die Bewertung von Sicherheitsprodukten erfordern ebenfalls die Mitwirkung des IS-Teams. Die Arbeitshilfe ist ein minimaler und zielführender Ansatz, der sich in vielen Behörden bereits bewährt hat. ■

*Die Arbeitshilfe und das Schätztool stehen unter dem folgenden Link kostenlos zum Download bereit: www.bsi.bund.de/Personalschaetzung*

*Weitere Informationen zum „Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung“ finden sich im Web unter www.orghandbuch.de*

# Das BSI-Tool in der Praxis

## Ein Erfahrungsbericht zur Anwendung des BSI-Tools zur Aufwandsabschätzung beim Aufbau eines ISMS

**Der IT-Planungsrat hat die „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ beschlossen. Diese gilt verbindlich sowohl für Bund als auch für Länder. Eine der darin umzusetzenden Maßnahmen ist der Aufbau eines Informationssicherheits-managementsystems (ISMS) gemäß BSI-Standards.**

**Ausgangslage**
In Nordrhein-Westfalen wurde durch eine ressortübergreifende Arbeits-gruppe (AG) der Umsetzungsaufwand für die Einführung eines ISMS nach den durch den IT-Planungsrat vorgegebenen Rahmenbedingungen bestimmt. Dabei identifizierte die AG die betroffenen wesentlichen Behör-den und erarbeitete eine IST-Erhebung zur Informationssicherheit in der Landesverwaltung NRW.

**Vorgehensweise**
Aus diesen individuellen Rückmeldun-gen wurde mit Unterstützung eines externen Dienstleisters und unter Verwendung des BSI-Schätztools eine vollständige, behördenscharfe Aufwandsschätzung erzeugt. Wo keine detaillierteren Angaben vorlagen, wurden plausible Annahmen getroffen. Gleichzeitig erfasste man die bereits besetzten Stellen.

**Resultat und Wirkung**
Das Ergebnis, insbesondere die ermit-telten Personal- und Sachaufwände, wurde in die Haushaltsberatungen ein-gebracht. Der Haushaltsentwurf wurde inzwischen von der Landesregierung beschlossen. Nach Verabschiedung des Haushalts durch den Landtag NRW stehen Mittel zum Aufbau eines ISMS zur Verfügung.
Das vom BSI bereitgestellte Schätztool hat wesentlich zur Versachlichung der Diskussion bei dem oft strittigen Thema einer Aufwandabschätzung beigetragen. ■

**Hintergrundwissen:**

**Was ist die Leitlinie „Informationssicherheit”?**
- Verabschiedet vom IT-Planungsrat im März 2013
- Erreichung eines verbindlichen Mindestsicherheitsniveaus zwischen Bund und Ländern bei IT-gestützter und ebenenübergreifender Zusam-menarbeit
- Maßnahmen zur Umsetzung
- Sensibilisierungsmaßnahmen zur Informationssicherheit
- Schulungen im Kontext des Verwaltungs-CERT-Verbunds
- Unterstützung bei IT-Grundschutz-Umsetzung
- Einführung eines Infomationssicher-heitsmanagementsystems gemäß Vorgaben des BSI
- Umsetzung einheitlicher Mindest-standards in der Informationssicher-heit
- Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung
- Gemeinschaftliche Abwehr von Angriffen auf die IT-Systeme der Verwaltung

*Helmut Nehrenheim, Referent im Ministerium für Inneres und Kommuna-les des Landes Nordrhein-Westfalen*

*Dr. Frank Laicher, Referent im Ministe-rium für Inneres und Kommunales des Landes Nordrhein-Westfalen*



*Trends wie Cloud Computing, Industrie 4.0 und BYOD bringen neue Sicherheitsheraus-forderungen mit sich, die im IT-Grundschutz Berücksichtigung finden*

# BSI modernisiert den IT-Grundschutz

## Hilfe zur Selbsthilfe

**Der IT-Grundschutz des BSI gibt Behörden und Unternehmen ein umfassendes Kompendium mit IT-Sicherheitsanforderungen und Um-setzungsempfehlungen an die Hand – das angesichts der dynamischen Bedrohungslage und Technologie-entwicklung schier unüberschaubare Ausmaße angenommen hat. Grund genug, das Standardwerk rundum zu modernisieren und stärker an der Praxis der IT-Nutzer auszurichten.**

Wohl nirgendwo sonst auf der Welt hat sich im Lauf von mehr als zwei Jahrzehnten ein derart umfangreiches Reservoir an Methoden und Maßnahmen zum Schutz von Infor-mationen, IT-Systemen und Netzen herausgebildet wie in Deutschland. Ursprünglich war der sogenannte „IT-Grundschutz“ als ein Standard-werk konzipiert, das hauptsächlich der öffentlichen Verwaltung eine fundierte Systematik zur Erkennung unterschiedlicher Sicherheitsrisiken inklusive entsprechender Handlungs-empfehlungen an die Hand geben sollte. Schnell jedoch griff auch die Privatwirtschaft auf das Werk zurück, weil der IT-Grundschutz des BSI einen pragmatischen Weg zur Feststellung des individuellen Schutzbedarfs und zum Schutz der eigenen IT-Landschaft aufzeigt. Pragmatisch insofern, als die kontinuierlich weiterentwickelte Informations- und Methoden-sammlung anstelle einer zeit- und kostenaufwendigen Risikoabschätzung von pauschalen Gefährdungsklassen für unterschiedliche Systeme und Anwendungen je nach Einsatzgebiet ausgeht. Damit entfällt die Notwen-digkeit einer detaillierten Ermittlung von Eintrittswahrscheinlichkeiten samt Abschätzung der jeweiligen Scha-denshöhe. Mit dem IT-Grundschutz lässt sich daher ein angemessenes Sicherheitsniveau auch ohne tiefergehendes IT-Security-Know-how auf wirtschaftlich vertretbare Art und Weise umsetzen.

*Holger Schildt, Referent "IT-Grund-schutz und Allianz für Cyber-Sicherheit"*

### Komplexität wird aufgelöst

In engem Schulterschluss mit der Praxis schreibt das BSI den IT-Grundschutz im Licht stetig neuer Cyber-Gefahren permanent fort. Denn Trends wie Cloud Computing, Industrie 4.0 und die Zunahme beruflich-privater Mischnutzung von Smartphones oder Tablets bringen neue Sicherheitsherausforderungen mit sich – die im IT-Grundschutz selbstverständlich Berücksichtigung finden müssen. Inzwischen füllen die BSI-Standards und die IT-Grundschutz-Kataloge nebst Handreichungen und Empfehlungen nicht weniger als 5.000 Seiten. Der größte Vorteil des IT-Grundschutzes, nämlich seine einzigartige Detailtiefe, wird nun selbst zu einem Problem: Der Umfang wirkt einschüchternd und schreckt ab. Viele Anwender fühlen sich von der schieren Menge der dargebotenen Informationen überfordert. Andererseits wissen sie, dass der IT-Grundschutz ohne Bezug zur aktuellen Gefährdungslage und ohne konkrete Sicherheitsempfehlungen kaum einen Wert hätte. Was also ist zu tun? Als Ausweg aus diesem Dilemma beschloss das BSI eine grundlegende Modernisierung des IT-Grundschutzes – und zwar so, dass sich der Anspruch an ein umfassendes Standardwerk mit der berechtigten Forderung nach einfacher Handhabbarkeit verbindet.

### Trennung von Anforderungen und Umsetzung

Möglich wird dies durch eine Überarbeitung der grundlegenden Bausteine, die anders als früher die jeweiligen Anforderungen ohne weitere Umsetzungsempfehlungen in komprimierter Form auf höchstens zehn Seiten zusammenfassen. Das hat zum einen den Vorteil der leichteren Lesbarkeit und reduziert zum anderen den Aufwand bei der Erstellung der IT-Grundschutz-Bausteine. Das BSI kann in Zukunft dadurch deutlich zeitnäher mit neuen Bausteinen auf aktuelle Entwicklungen reagieren. Die sprichwörtliche Detailtiefe wird dabei in zielgruppengerecht aufbereitete Umsetzungshinweise – zum Beispiel für IT-Administratoren oder Haustechniker – quasi ausgelagert. So gelingt es, die oftmals einschüchternde Komplexität der früheren Bausteine auszublenden. Durch die Trennung der Anforderungen von den Umsetzungshinweisen kann das BSI die notwendigen Informationen genau auf die Bedürfnisse unterschiedlicher Rollen in Unternehmen und Organisationen aller Art zuschneiden. So benötigt ein IT-Sicherheitsbeauftragter in der Regel kein umfangreiches Wissen darüber, wie die Anforderungen im Detail umgesetzt werden können. Mit den modernisierten Bausteinen sparen Anwender Zeit und Aufwand, was wiederum die Akzeptanzchancen für den IT-Grundschutz in Deutschland insgesamt verbessert.

Die Anforderungen dieser Bausteine sind zukünftig in drei Kategorien gegliedert: Basis-, Standard- und Anforderungen für einen höheren Schutzbedarf. Vorrangig sollten die Basis-Anforderungen umgesetzt werden, da sie mit geringem Aufwand den größtmöglichen Nutzen erzielen. Darauf aufbauend vervollständigen die Standard-Anforderungen den Stand der Technik und adressieren den normalen Schutzbedarf. Ergänzend dazu bieten die IT-Grundschutz-Kataloge Vorschläge für Maßnahmen bei hohem Schutzbedarf. Doch das BSI modernisiert nicht nur die Bausteine selbst, sondern auch die sogenannten Schichten, in denen sich diese Bausteine in die Architektur des IT-Grundschutz-Modells einfügen. Dazu werden die bisherigen Schichten „Übergreifende Aspekte“, „Infrastruktur“, „IT-Systeme“, „Netze“ und „Anwendungen“ durch ein neues Modell ersetzt: Die IT-Grundschutz-Bausteine werden künftig in prozess- und systemorientierte Gruppen aufgeteilt. Prozessorientiert sind Bausteine, die übergreifende Aspekte wie Konzepte, Regelungen oder den IT-Betrieb betreffen – etwa das Patch-Management. Anwendungen, IT-Systeme und die Infrastruktur hingegen gelten als systemorientiert. Neu hinzu kommen Bausteine für industrielle Steuerungsanlagen, da deren Schutz nun ebenfalls in den Fokus des modernisierten IT-Grundschutzes rückt.

### Flexible Einstiegsvarianten und praxisbewährte Profile

Neue Wege geht das BSI überdies bei der Vorgehensweise, um den Einstieg in den IT-Grundschutz zu erleichtern. Denn die Erfahrung lehrt, dass die bisherige Ablauffolge, bei der zunächst eine Strukturanalyse, Schutzbedarfsfeststellung mit Modellierung und ein Basis-Sicherheitsscheck zu durchlaufen waren, gerade von kleinen und mittelständischen Unternehmen als enorme Hürde empfunden wurde. Zudem entfalteten Schutzmaßnahmen erst zu einem relativ späten Zeitpunkt ihre Wirkung – solange blieb die betreffende Institution den vielfältigen Risiken schutzlos ausgeliefert. Je nachdem, welche Schutzvorkehrungen in einer Einrichtung bereits realisiert sind, kann es also durchaus zweckmäßig sein, von der bisherigen IT-Grundschutz-Methodik zunächst abzuweichen.
So könnte eine Institution im ersten Schritt beispielsweise flächendeckend alle Basisanforderungen umsetzen, um möglichst schnell und aufwandsarm einen Großteil aller Risiken zu minimieren. Die detaillierte Schutzbedarfsanalyse würde dann zu einem späteren Zeitpunkt mit einer anderen Vorgehensweise erfolgen. In anderen Fällen kann es demgegenüber sinnvoll sein, sich gleich zu Beginn auf den Schutz herausragender Werte in der Institution zu konzentrieren, sich also zuallererst um die besonders schützenswerten „Kronjuwelen“ zu kümmern.
Ein weiterer Schwerpunkt des Modernisierungsprojekts liegt auf der Neuentwicklung sogenannter IT-Grundschutz-Profile. Deren Grundidee wird bereits im herkömmlichen IT-Grundschutz verwirklicht – nämlich in Form von Beispiel-Sicherheitskonzepten, die exemplarisch aufzeigen, wie ein Sicherheitskonzept für etwa kleine, mittlere oder große Informationsverbünde zu planen, umzusetzen und zu pflegen ist. Die neuen Profile sind darüber hinaus als direkt nutzbare Schablonen zu verstehen, mit denen verschiedene Anwendergruppen den IT-Grundschutz an ihre Bedürfnisse anpassen können. Die Erarbeitung der neuen Profile kann in Kooperation mit dem BSI durch Anwender in der Praxis selbst erfolgen – mit dem klaren Fokus auf branchen- und zielgruppenspezifische Anpassungsmöglichkeiten. Denkbar wäre zum Beispiel, dass Mitarbeiter von Anwaltskanzleien oder Arztpraxen definieren, welche Empfehlungen essenziell, optional oder auch verzichtbar sind. Auf diese Weise entstehen die IT-Grundschutz-Profile von der Zielgruppe für die Zielgruppe. Interessant ist der neue Profilansatz aber nicht nur für kleine Institutionen, sondern etwa auch für Kommunalverwaltungen, Krankenhäuser und sogar Betreiber kritischer Infrastrukturen, zum Beispiel aus dem Versorgungssektor. Denn der enge Praxisbezug und der Modellcharakter der neuen Profile helfen Institutionen jeder Größenordnung, Aufwand, Zeit und Kosten bei der individuellen Umsetzung ihres IT-Grundschutzes zu sparen. ■

# Sicher, effizient und bürgernah

## De-Mail in der öffentlichen Verwaltung

**Die E-Mail ist ein Erfolgsmodell. Sie genießt allgemein große Verbreitung und Akzeptanz in der Bevölkerung und der Wirtschaft. Auch aus der öffentlichen Verwaltung der Bundesrepublik ist die schnelle und bequeme Kommunikation per E-Mail nicht mehr wegzudenken. Doch dieses weit verbreitete Medium hat auch seine Schattenseiten: In puncto Vertraulichkeit, Integrität und Authentizität gibt es noch deutliches Verbesserungspotenzial. Der Rat von IT-Sicherheitsexperten, allgemein zumindest E-Mails mit wichtigem oder vertraulichem Inhalt gezielt zu verschlüsseln, findet wenig Widerhall – vor allem deshalb, weil die meisten Anwender heutige Verschlüsselungsverfahren als zu kompliziert und daher als alltagsuntauglich empfinden.**


*Die BSI-Richtlinie zur De-Mail-Bildübertragung bei der Ausstellung von hoheitlichen Dokumenten ist seit Herbst 2014 für alle Kommunalverwaltungen verfügbar*

**Authentizität** definiert die Sicherheit darüber, dass der vorgebliche, also sichtbare Absender einer E-Mail auch der tatsächliche Absender ist.

**Integrität** definiert den Schutz des Inhalts einer E-Mail, sodass dieser während der Übertragung vollständig unverändert bleibt.

**Vertraulichkeit** definiert die Gewährleistung, dass eine E-Mail bzw. deren Inhalte nur dem hierfür bestimmten Empfängerkreis zugänglich sind.

Mehr Akzeptanz verspricht dagegen De-Mail, denn dieses Verfahren erreicht höhere IT-Sicherheit auf einem anderen Weg: De-Mail verwirklicht einen geschlossenen Kommunikationsverbund, in dem ausschließlich vom BSI akkreditierte Dienstleister zugelassen sind. Anders als E-Mail-Provider im Internet müssen sie zur Aufnahme in den De-Mail-Verbund einen umfangreichen Prüfprozess anhand klar definierter Kriterien absolvieren. Grundlage hierfür bietet das De-Mail-Gesetz und die entsprechenden technischen Richtlinien des BSI.
Vertraulichkeit und Integrität garantiert De-Mail dank verschlüsselter Versandkanäle, während Authentizität durch eine eindeutige Identifikation aller Kommunikationspartner im Verbund gewährleistet wird.

Gleichwohl: De-Mail hat nicht den Anspruch, die herkömmliche E-Mail-Infrastruktur komplett zu ersetzen. Ziel des Verfahrens ist es vielmehr, für ausgewählte Einsatzzwecke die klassischen Vorteile der E-Mail mit einem nachweislich höheren IT-Sicherheitsniveau anzubieten.

### Einführung läuft auf Hochtouren

Den Grundstein für De-Mail legte die Bundesregierung im April 2011 mit der Verabschiedung des De-Mail-Gesetzes. In den beiden Folgejahren bestanden vier De-Mail-Diensteanbieter ihre Akkreditierungsprüfung durch das BSI und können nun den De-Mail-Service deutschlandweit anbieten. Zum Verbund gehören derzeit die 1&1 De-Mail GmbH, Mentana-Claimsoft, Telekom Deutschland und T-Systems International.

Deutlich erweitert hat sich das Einsatzgebiet von De-Mail mit dem Inkrafttreten des E-Government-Gesetzes vor zwei Jahren. Denn seither kann bei rechtsverbindlicher Kommunikation unter bestimmten Bedingungen mit der Versendung einer De-Mail die Schriftform ersetzt werden. Gleichzeitig verpflichtet das Gesetz die Bundesbehörden, spätestens ab Frühjahr 2016 einen De-Mail-Zugang für Bürger und Unternehmen zur Übermittlung elektronischer Dokumente anzubieten. Bereits seit März 2015 stellt der Bund seinen nachgeordneten Behörden eine zentrale De-Mail-Anbindung zur Verfügung.
Ein Vorzug dieses Bundesgateways besteht darin, dass es die Anbindung der Mailsysteme aller Bundesbehörden nach einem vereinfachten Verfahren erlaubt – was bis März 2016 schrittweise erfolgen soll. Mitarbeiter und Mitarbeiterinnen der Bundesbehörden können sichere De-Mails dann ohne große Umstellung mit ihrem gewohnten E-Mail-Client versenden und empfangen. Komfort und einfache Bedienung sind auch bei IT-Sicherheitslösungen eine Grundvoraussetzung für breite Nutzerakzeptanz.

### Weniger Behördengänge, Einsparung von Wartezeiten

Für Bürger und Unternehmen bringt die De-Mail-Anbindung von Behörden spürbare Zeit- und Kostenvorteile. Denn Behördengänge oder der postalische Dokumentenversand werden in vielen Fällen überflüssig. Mit Blick auf die Verwaltungseffizienz bietet die Anbindung an die De-Mail-Infrastruktur ein noch weiter gehendes Potenzial – beispielsweise durch eine technische Integration von De-Mail in Fachverfahren oder Dokumentenmanagementsysteme der jeweilige Behörde. Auf diese Weise lassen sich eingesandte Dokumente medienbruchfrei weiterverarbeiten und nach Abschluss des zugehörigen Vorgangs ohne manuellen Aufwand elektronisch archivieren.

Welche Effekte durch eine solche De-Mail-Integration künftig möglich werden, veranschaulicht schon jetzt ein Pilotprojekt der Städte Köln und Göttingen zur digitalen Bildübertragung im Zusammenhang mit der Ausstellung von Personalausweisen: Mit Zustimmung des Antragstellers wurden hierbei biometrische Passbilder von teilnehmenden Fotografen direkt nach der Aufnahme per De-Mail an die ausstellende Behörde übersandt. Der bislang notwendige Fotoausdruck und das anschließende Wiedereinscannen der Lichtbilder in der Behörde entfallen. ■

*Ingrid Grüning, Referentin "Sicherheit in eID-Anwendungen"*

# Sichere Kommunikationsplattform für das intelligente Energienetz

Die intelligente Vernetzung des zukünftigen Energiesystems stellt Deutschland vor große Herausforderungen, bietet zugleich aber auch große Chancen und Perspektiven für die beteiligten Akteure im deutschen Energiemarkt. Bei der Etablierung eines einheitlichen Sicherheitsniveaus im intelligenten Energienetz nimmt Deutschland in Europa eine Vorreiterrolle ein. Durch die Fortentwicklung der Sicherheitsvorgaben für wichtige Systemkomponenten des intelligenten Energienetzes ergeben sich komplexe Aufgabenstellungen für das BSI.

Mit intelligenten Informationsnetzen können Energieerzeugung und -verbrauch effizient verknüpft und ausbalanciert werden. Wichtige Elemente eines solchen Netzes sind intelligente Messsysteme, auch „Smart Metering Systems“ genannt. Auf der einen Seite sorgen sie für Verbrauchstransparenz, auf der anderen Seite für die sichere Übermittlung von Messdaten. Mit der zusätzlichen Fähigkeit, eine Plattform für die Steuerung von elektronischen Verbrauchsgeräten und Erzeugungsanlagen zu bieten, verbessern sie zudem das Last- und Verteilnetz. Zentrale Komponente eines intelligenten Messsystems ist das Smart Meter Gateway als Kommunikationseinheit mit integriertem Sicherheitsmodul.



### Bund und Wirtschaft erarbeiten gemeinsame Sicherheitsstandards

Die Schaffung verbindlicher Rahmenvorgaben für die Herstellung und den Betrieb von intelligenten Messsystemen ist Grundvoraussetzung für Vertrauen in die neue Technik und für ihre Akzeptanz, insbesondere weil personenbezogene Daten verarbeitet werden. Im Auftrag des Bundesministeriums für Wirtschaft und Energie entwickelte das BSI daher Anforderungen an vertrauenswürdige Produktkomponenten (Smart Meter Gateway mit integriertem Sicherheitsmodul), deren sicheren IT-Betrieb (Administration) und an die vertrauenswürdige Kommunikationsinfrastruktur (Smart Metering Public Key Infrastruktur).

Eingebunden in die Entwicklung wurden verschiedene Verbände aus den Bereichen Telekommunikation, Informationstechnik, Energie, Wohnungswirtschaft und Verbraucherschutz sowie die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Bundesnetzagentur sowie die Physikalisch-Technische Bundesanstalt.

### Smart Meter Gateway mit integriertem Sicherheitsmodul

Das BSI entwickelte sicherheitstechnische Vorgaben in Form von zwei Schutzprofilen (Protection Profiles, PP) sowie daran anschließend eine Technische Richtlinie (TR) für die Kommunikationseinheit eines intelligenten Messsystems (Smart Meter Gateway mit integriertem Sicherheitsmodul).

Ein intelligentes Messsystem besteht daher aus einem Smart Meter Gateway und einer oder mehreren hieran angeschlossenen Messeinrichtungen (Zählern). Die Einhaltung der sicherheitstechnischen Vorgaben werden im Rahmen eines Zertifizierungsverfahren nach Common Criteria (CC) durch das BSI überprüft. Aktuell befinden sich beim BSI acht Smart Meter Gateway-Hersteller, die einer Veröffentlichung zugestimmt haben, im CC Zertifizierungsverfahren.

### Schutz der Privatsphäre „by design“

Der Schutz der Privatsphäre ist von Anbeginn durch die Beteiligung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) bei der Entwicklung berücksichtigt worden. Dies ist notwendig, um das Erzeugen von detaillierten Nutzerprofilen und das damit einhergehende große Ausforschungspotenzial in Bezug auf die Lebensgewohnheiten des Endkunden zu verhindern. Hierzu können Auswertungsprofile im Smart Meter Gateway so gestaltet werden, dass für verschiedene dezentral abgebildete Tarifprofile nur die notwendigen abrechnungsrelevanten Verbräuche zur Verfügung gestellt werden. Dadurch wird die geforderte Datenvermeidung und notwendige Datensparsamkeit erreicht.


*Das Smart Meter Gateway als Kommunikationseinheit in einem intelligenten Messsystem und als zentrale Komponente zwischen Weitverkehrsnetz (WAN), Lokalen Metrologischen Netz (LMN) und dem Heimnetz (HAN)*

**Gewährleistung des sicheren Betriebs intelligenter Messsysteme**

Für den sicheren technischen Betrieb des intelligenten Messsystems ist der Smart-Meter-Gateway-Administrator verantwortlich. Daher muss sichergestellt sein, dass der IT-Betrieb beim Administrator Mindestanforderungen zur Durchsetzung der Informationssicherheit genügt. Derzeit umfassen die Anforderungen der Technischen Richtlinie eine Prüfung des ISMS (Managementsystem für Informationssicherheit) sowie eine über ISO 27001 hinausgehende Bewertung konkreter Sicherheitsmaßnahmen anhand der IT-Grundschutz-Kataloge (BSI als Zertifizierungsstelle). Die bestehenden Vorgaben werden derzeit in Abstimmung mit Fachexperten aus

*Dennis Laupichler, Referent "Industriekooperation und Standardisierung"*

den beteiligten Branchenverbänden durch eine weitere Alternative ergänzt, die eine Prüfung nach ISO 27001 nativ sowie ein für den Administrator umzusetzendes Maßnahmenpaket vorsieht. Bei einer Zertifizierung nach ISO 27001 nativ sind Zertifizierungsstellen beteiligt, die bei der Deutschen Akkreditierungsstelle (DAkkS) gemäß IEC/ISO 27006 für ISMS akkreditiert sind.

**Vertrauenswürdige Kommunikationsinfrastruktur im Weitverkehrsnetz**

Das BSI ist Inhaber der Zertifikate der Wurzelzertifizierungsstelle (Root) der Smart-Metering-Public-Key-Infrastruktur. Darunter liegend operieren private Unternehmen, sogenannte Sub-CAs (untergeordnete Zertifizierungsstellen), welche die Ausgabe von Endnutzerzertifikaten für die Marktteilnehmer übernehmen.

Die Root bildet hier den zentralen Vertrauensanker der intelligenten Messsysteme. Denn um den Schutz

der übermittelten Messdaten zu gewährleisten, ist für die Verbindung des Smart Meter Gateways zu einem autorisierten Marktteilnehmer im Weitverkehrsnetz eine gegenseitige Authentisierung der Kommunikationspartner erforderlich. Die Kommunikation erfolgt dabei stets über einen verschlüsselten, integritätsgesicherten Kanal. Die technischen, personellen und organisatorischen Sicherheitsanforderungen für die Ausstellung von Zertifikaten werden von der Root in einer Certificate Policy (Root-CP) festgelegt. Der Wirkbetrieb der Root wird seit dem 1. März 2015 unter Aufsicht des BSI von einem Zertifizierungsdiensteanbieter durchgeführt. Des Weiteren werden den Marktteilnehmern zusätzlich zur Root verschiedene Testsysteme zur Ausgabe von digitalen Test-Zertifikaten bereitgestellt, um die Entwicklung und Erprobung der Smart Meter Gateways und zugehöriger Komponenten in Feldtests und Piloten zu unterstützen.

**Fortentwicklung der Sicherheitsvorgaben im intelligenten Energienetz**

Das Schutzprofil für das Smart Meter Gateway stellt bereits mit seinen Mindestanforderungen die Basis für die Etablierung eines einheitlichen Sicherheitsniveaus im intelligenten Energienetz dar. Aufgrund der verschiedenen Einsatzszenarien und adressierten Anwendungsfälle im Zuge des Eckpunktepapiers des BMWi zum Themenschwerpunkt „Intelligente Netze“ vom 9. Februar 2015 wurden nun neue und zusätzliche Anforderungen an das Smart Meter Gateway und die angeschlossenen Komponenten gestellt.

Um das Smart Meter Gateway im Sinne einer sicheren Kommunikationsplattform für das intelligente Energienetz weiterzuentwickeln, müssen zuerst die sichere Kommunikation von netzdienlichen Informationen, von Stromverbrauchs- und Erzeugungswerten sowie das sichere Bewirken von Last- und Erzeugungsmanagementmaßnahmen ermöglicht werden. Um das volle Potenzial einer sicheren und standardisierten Kommunikationsplattform zu entfalten, müssen perspektivisch auch die Fähigkeiten zur Messung anderer Sparten (Gas, Wasser, Wärme) und die Umsetzung von sich aktuell entwickelnden Mehrwertdiensten z.B. in den Bereichen Gebäudeautomatisierung, Smart Home und betreutes Wohnen folgen. Die Entwicklung von zusätzlichen Sicherheits- und Interoperabilitätsanforderungen für Spezialanwendungen (Groß-Gasmessanlagen, Strom-Großverbraucher, Wind- und PV-Parks) sowie die sichere Anbindung von dezentralen Komponenten der Ladesäulen-Infrastruktur schließt sich dem unter Berücksichtigung internationaler Standards an. Bei der Weiterentwicklung müssen alle bisher beteiligten Ressorts, Partnerbehörden, Hersteller und Anwender eingebunden werden, sodass ein zielgerichteter Rollout von intelligenten Messsystemen auch von den Beteiligten getragen und gesteuert werden kann. Das Verbandsanhörungsverfahren mit den entsprechenden fachlichen Arbeitsgruppen des BSI hat sich im Zuge der Entwicklung der Schutzprofile und der Technischen Richtlinie erfolgreich bewährt und wird dementsprechend für die Weiterentwicklung fortgesetzt werden.

**Ausblick zum Rechtsrahmen**

Aufgrund der grundrechtsrelevanten Regelungsmaterie und der Vermeidung einer weiteren Zersplitterung des Energierechts war es notwendig, sämtliche Regelungsgegenstände in einem neuen Stammgesetz zusammenzufassen. Dies dient der Verfahrensklarheit und ermöglicht es auch, Regelungen außerhalb des Rechts der Energieversorgung mit Strom und Gas (z.B. im Bereich Smart Home, Fern- und Heizwärme) festzulegen. Ziel des Bundesministeriums für Wirtschaft und Energie ist es, das Gesetz zur Digitalisierung der Energiewende im zweiten Halbjahr 2015 zu veröffentlichen und nach einem gefassten Kabinettsbeschluss Bundestag wie Bundesrat zur Zustimmung bzw. Beschlussfassung vorzulegen. Gegenstand des neuen Stammgesetzes über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG) werden die Festlegung hoher technischer Standards (Schutzprofile und technische Richtlinien) zur Gewährleistung von Datenschutz und Datensicherheit, bereichsspezifischer Datenschutzregeln für die Marktkommunikation sowie Regelungen im Zusammenhang mit dem Einbau und der Finanzierung von intelligenten Messsystemen sein. ■

*Mehr Infos im Web unter: www.bsi.bund.de/SmartMeter*

# Die Mitarbeiter des BSI

Auch im Jahr 2015 ist das BSI wieder unter Deutschlands beliebtesten Arbeitgebern im IT-Bereich. IT-Absolventen haben das BSI zum wiederholten Mal in das Ranking gewählt – in diesem Jahr auf Platz 16, gleich hinter namhaften Firmen wie Google, SAP, IBM und Microsoft.

Der entscheidende Erfolgsfaktor für die Arbeit des BSI sind seine Mitarbeiter. Denn das Zukunftsthema IT-Sicherheit aktiv mitgestalten zu können, ist Herausforderung und Chance gleichermaßen.

Die IT-Sicherheit in der Informationsgesellschaft zu begleiten, ist für die Mitarbeiter des BSI nicht nur Beruf, vielmehr Berufung. Hierfür können die BSI-Mitarbeiter auf eine umfangreiche Wissensbasis aus unterschiedlichen Ausbildungshintergründen wie Ingenieurwesen, Informatik, Verwaltungs-/Betriebs- und Finanzwirtschaftslehre zurückgreifen.

Das BSI engagiert sich, die Möglichkeiten der Personalentwicklung im öffentlichen Dienst für kompetente und engagierte Mitarbeiter voll auszuschöpfen. Eine Höherqualifizierungen der Mitarbeiterinnen und Mitarbeiter wird in der strategischen Personalplanung frühzeitig berücksichtigt. Zurzeit unterteilt sich die Mitarbeiterstruktur des BSI in 377 Beamte und 201 Tarifbeschäftigte. Die konkrete Aufteilung der unterschiedlichen Dienstgrade für verbeamtete und tarifbeschäftigte Kollegen ist in der Infografik dargestellt.

# Was bringt und brachte das Jahr 2015 in Sachen IT-Sicherheit?

## Fragen an BSI-Präsident Michael Hange

**Das Interview führte Joachim Gutmann, Journalist aus Hamburg**

***Herr Hange, was war für Sie 2015 das herausragende Ereignis in Sachen IT-Sicherheit? Und was bedeutet dieses Ereignis für das BSI?***

**Michael Hange:** Ganz eindeutig die Verabschiedung des IT-Sicherheitsgesetzes. Es ist ein Meilenstein, weil erstmals gesetzlich das Ziel formuliert wird, gemeinsam mit den Betreibern den Schutz kritischer Infrastrukturen zu verbessern. Es trägt damit der zunehmenden Bedrohung durch Cyberangriffe Rechnung und ermöglicht durch mehr Lageinformationen aus der Wirtschaft, neue Strategien der Abwehr zu entwickeln – auch zum Schutz der Bürgerinnen und Bürger.

Zudem stärkt das Gesetz die Rolle des BSI als zentrale Stelle für Belange der IT-Sicherheit für Wirtschaft und Gesellschaft. Mit dem IT-Sicherheitsgesetz wird gesetzlich nachvollzogen, was Bürger und Wirtschaft ohnehin vom BSI erwarten, nämlich nicht nur die IT der Bundesverwaltung abzusichern, sondern auch Hilfestellung für andere Anwender zu leisten. Diese Erwartungen werden wir erfüllen.

***Das Gesetz weist dem BSI neue Aufgaben und neue Ressourcen zu. Entspricht beides Ihren Erwartungen?***

**MH:** Der erste Teil dieser Frage ist leicht zu beantworten. Das Parlament hat dem BSI durch die Erweiterung der bisherigen operativen Aufgaben mehr Verantwortung übertragen: als Meldestelle, bei der Produktprüfung, hinsichtlich der Warnfunktionen und bei der Standardsetzung in der Bundesverwaltung. Die Beratungsfunktion auch für die Wirtschaft wird gestärkt, unsere Einflussmöglichkeiten auf Standards der IT-Sicherheit werden erweitert. Daraus erwächst aber auch die Verpflichtung des BSI, dieser Verantwortung gerecht zu werden und bei Bedarf rasch praxistaugliche Empfehlungen anzubieten. Im Ergebnis setzt sich damit der seit Jahren laufende Veränderungsprozess des BSI hin zur operativ handelnden Behörde mit Schwerpunkt IT-Sicherheit fort.

Zum zweiten Teil der Frage: Die 50 zugebilligten Stellen für 2016 können nur ein Anfang für die Aufgabenwahrnehmung aus dem IT-Sicherheitsgesetz sein. In den Folgejahren sind weitere Stellen für eine qualifizierte Aufgabenwahrnehmung erforderlich. Denn IT-Sicherheit ist das Ergebnis sehr dynamischer und hochkomplexer Prozesse. Wenn wir im Wettlauf mit den Angreifern mithalten wollen, müssen wir auch personell gerüstet sein.

***Wie flexibel muss die gesetzliche Grundlage sein, auf der das BSI arbeitet, um mit den rasanten (technischen) Entwicklungen auf der Bedrohungsseite Schritt zu halten?***

**MH:** Wir spiegeln unser Handeln fortlaufend an den technischen Entwicklungen und der Gefährdungslage. Neue Technologien bzw. neue Geschäftsmodelle, deren Bedrohungspotenzial bzw. deren Sicherheitsgewinn antizipiert werden müssen, stellen hier eine besondere Herausforderung dar. Diesen „Evaluierungsprozess“ machen wir seit 2014 in Form eines jährlichen Lageberichts für Öffentlichkeit und Politik transparent. Aus ihm ergibt sich die erforderliche Flexibilität sowohl für die gesetzliche Grundlage als auch kooperative Ansätze des BSI. Über den gesetzlichen Handlungsbedarf muss jedoch letztlich der Gesetzgeber entscheiden, da will ich keine Vorgaben machen.

***Wird die Einbindung des BSI in die Struktur des BMI den neuen Aufgaben noch gerecht oder müsste das BSI nicht eine unabhängige Behörde werden?***

**MH:** Die Frage der Eigenständigkeit des BSI ist in der Tat im parlamentarischen Raum und auch in einigen Medien aufgeworfen worden. Wir arbeiten als IT-Sicherheitsdienstleister für die gesamte Bundesverwaltung in Form von Schutz-, Warn- und Beratungsfunktionen. Das BSI unterstützt auch die Stellen des Bundes, die Kontrollaufgaben wahrnehmen wie z.B. die Bundesbeauftragte für den Datenschutz und Informationssicherheit. In über 60 spezialgesetzlichen Regelungen unterstützt das BSI darüber hinaus auch andere Ressorts in Fragen der Gesetzgebung mit Bezug zur IT-Sicherheit (z.B. Smart Meter, Gesundheitskarte). Im Rahmen dieser Aufgaben würde ich mir eine Eigenständigkeit in der direkten Unterstützung anderer Ministerien wünschen. Eine vollständige Unabhängigkeit halte ich aber für nicht realistisch, da wir im Kern eine Dienstleistungs- und Umsetzungsbehörde in der IT-Sicherheit sind.

*„Mit dem IT-Sicherheitsgesetz wird gesetzlich nachvollzogen, was Bürger und Wirtschaft ohnehin vom BSI erwarten, nämlich nicht nur die IT der Bundesverwaltung abzusichern, sondern auch Hilfestellung für andere Anwender zu leisten.“*

***Die Schlagzeilen des Jahres 2015 waren auch von zahlreichen Cyber-Angriffen geprägt: Welcher Angriff steht beispielhaft für die Entwicklung der IT-Sicherheitslage und welche Maßnahmen leiten Sie hieraus ab?***

**MH:** Hier sind natürlich die sogenannten APT-Angriffe wie z.B. auf den Deutschen Bundestag zu nennen. Mit dieser qualitativen Entwicklung müssen wir uns technisch, aber auch gesellschaftlich auseinandersetzen. In führenden NATO-Staaten wird die Bedrohung durch Cyber-Angriffe als eine der größten Bedrohungen ihrer nationalen und öffentlichen Sicherheit angesehen. Diese Diskussion ist in Deutschland bislang noch nicht geführt worden.

Neben den reaktiven Fähigkeiten müssen wir auch präventiv handlungsfähig bleiben: Wichtig für das BSI – wenn auch weitaus weniger beachtet – war z.B. die Entscheidung des Haushaltsausschusses des Deutschen Bundestages, das BSI künftig regelmäßig mit der IT-Sicherheitsprüfung der Rechenzentren in der Bundesverwaltung zu betrauen.

***Auch 2015 waren die Snowden-Enthüllungen politisch und medial präsent: Wie schätzen Sie die Enthüllungen ein?***

**MH:** Aus IT-sicherheitstechnischer Sicht haben die Enthüllungen von Snowden für Medien und Politik sicherlich eine einschneidende und nachhaltige Wirkung. Sie veranschaulichen, wie verletzbar IT-Infrastrukturen und -Systeme sind. Aus systemischer Sicht haben insbesondere der immense Aufwand von Nachrichtendiensten sowie auch Hinweise auf Kooperationen von US-Global-Playern mit der NSA auch Fachleute überrascht. Aber: Es ist zu befürchten, dass einige Unterlagen auch als Blaupausen von Nachahmern für Aktivitäten im z.B. kriminellen Bereich genutzt werden. Das BSI hat darum seine Analysen in bestimmten Angriffsszenarien erheblich verstärkt.

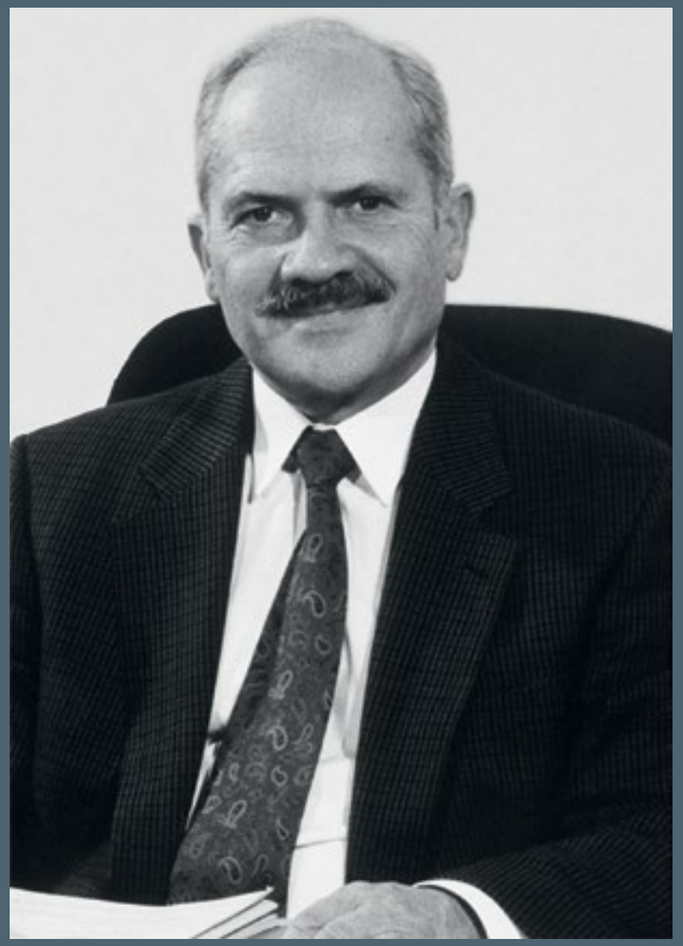
Aus informatischer Sicht haben die Veröffentlichungen viele Bürgerinnen und Bürger, aber auch viele Unternehmen aus der digitalen Sorglosigkeit geholt. Jetzt müssen wir aber aufpassen, dass das Pendel nicht zu weit in die andere Richtung ausschlägt und einer digitalen Hoffnungslosigkeit Platz macht. Auch wenn ein hundertprozentiger Schutz nicht möglich ist, so kann man mit 20 Prozent Aufwand schon 80 bis 90 Prozent Sicherheit erreichen.

***Nach 24 Jahren verabschieden Sie sich zum Ende dieses Jahres vom BSI und gehen in den Ruhestand. Wie fällt Ihr persönliches Resümee aus?***

**MH:** Bezogen auf das BSI auf jeden Fall ein positives Resümee. Das Amt ist an und mit den Herausforderungen gewachsen. Dabei waren das hohe fachliche Engagement der Mitarbeiter und Mitarbeiterinnen für das Thema IT-Sicherheit sowie die Zusammenarbeit mit ihnen für mich ein Gewinn. Mein Ziel war und ist, dass das BSI als kompetenter IT-Sicherheitspartner wahrgenommen wird. Ich denke, dies ist uns trotz oder gerade wegen des innovativen und dynamischen Charakters des Themas IT-Sicherheit gut gelungen. Diese Flexibilität und Agilität werden wir uns auch in Zukunft erhalten müssen, insbesondere auch vor dem Hintergrund der Digitalisierung. Initiatives Handeln wird auch künftig notwendig sein, da sich in den letzten 25 Jahren die Bedeutung der deutschen und europäischen IKT-Branche im Vergleich erheblich geschmälert hat. ■

# Nachruf auf Dr. Otto Leiberich

*Von Michael Hange*



Am 23. Juni 2015 ist Herr Präsident a.D. Dr. Otto Leiberich nach kurzer schwerer Krankheit im Alter von 87 Jahren verstorben.

Herr Dr. Leiberich hat als Gründungspräsident das Bundesamt für Sicherheit in der Informationstechnik (BSI) bis heute richtungsweisend geprägt. Durch seinen Weitblick und sein außerordentliches Engagement legte er mit den Themen Kryptografie und Zertifizierung die Grundlagen für die Entwicklung und die zukünftigen Aufgaben des BSI. Er hat dadurch maßgeblich zum heutigen Ansehen des Amtes in der Öffentlichkeit beigetragen.

Seine herausragende berufliche Leistung ist die Gründung des BSI im Jahr 1991. Dieses Ziel verfolgte Dr. Leiberich mit Einsatz, Ausdauer und der Gabe, in Politik, Wirtschaft und Wissenschaft für seine Idee zu werben und zu überzeugen. Der Kerngedanke seiner Botschaft war, dass ein Bundesamt für Sicherheit in der Informationstechnik über den staatlichen Geheimschutz hinaus für die IT-Sicherheit aller gesellschaftlichen Gruppen beratend und unterstützend zuständig sein sollte.

In Anbetracht der Bedeutung der IT-Sicherheit im Rahmen der Digitalisierung der gesamten Gesellschaft ist dies aus heutiger Sicht eine sehr vorausschauende Weichenstellung.

Otto Leiberich stand auch für die strategische und operative Ausrichtung des Amtes in seiner Gründungsphase und hat damit ein „Start-up"-Bewusstsein im BSI geschaffen.

1993 trat Otto Leiberich in den Ruhestand, in dem er sich weiterhin mit der Kryptologie beschäftigte. In einem in Fachkreisen viel beachteten Artikel im Jahr 2000 schrieb er „Ich selbst habe als Kryptologe beruflich 45 Jahre erlebt und überblicke durch die Kontakte zu älteren Kollegen nahezu 100 Jahre Kryptologie." In der Tat ist Otto Leiberich Chronist der gewaltigen Veränderung der Kryptologie in Deutschland. Er hat die Entwicklung aktiv miterlebt und mitgestaltet – von der Kryptografie als Geheimwissenschaft bis hin zur Kryptographie als tragende Säule der heutigen IT-Sicherheit.

Otto Leiberich war Mathematiker und Kryptologe mit Leidenschaft – und das auch nach seiner Pensionierung. Der Weg dorthin ist ihm als Jahrgang 1927 – wie vielen seiner Generation – nicht leicht gemacht worden. Von der Schulbank wurde er als Soldat eingezogen und holte nach dem Krieg zunächst das Abitur nach, um dann das Studium der Mathematik aufzunehmen, das er 1953 mit der Promotion abschloss.

1953 trat er in die Zentralstelle für das Chiffrierwesen als junger Kryptologe ein. Otto Leiberich übernahm nach Führungspositionen in der mathematischen Kryptologie sowie der Leitung eines größeren Rechenzentrums ab 1972 die Verantwortung über die Zentralstelle für das Chiffrierwesen.

Wir – die jungen Mitarbeiter vor fast 25 Jahren – sind und waren Dr. Otto Leiberich dankbar für die Schaffung von Gestaltungsräumen und Perspektiven in dem 1991 gegründeten BSI. Wir haben ihn als Chef und Menschen geradlinig, offen und vor allem authentisch erlebt, bis ins hohe Alter mit Interesse für Fragen der Kryptologie und IT-Sicherheit.

Wir werden ihn als tatkräftige und geradlinige Persönlichkeit im Gedächtnis behalten. ■

# Kalender 2015

## Das hat das BSI bewegt

**7. Januar 2015:**
**DDoS-Angriff auf bundeskanzlerin.de**
Die Webseiten der Bundeskanzlerin und des Bundestages werden aufgrund einer DDoS-Attacke für mehrere Stunden lahmgelegt.

**14. Januar 2015:**
**Berliner Forum Cyber-Sicherheit**
Zum zweiten Mal findet das von BAKS und BSI ausgerichtete Forum statt und konzentriert sich vor allem auf globale Aspekte der Cyber-Sicherheit.

**20. – 22. Januar 2015:**
**OMNICARD**
Schwerpunkte der diesjährigen OMNICARD sind Themen rund um elektronische Identifikation in Bereichen wie elektronischen Bezahlsystemen, eGovernment, Cyber Security, Smart Home oder eHealth.

**10. Februar 2015:**
**Safer Internet Day**
„Let's create a safer internet together" heißt das Motto des diesjährigen Safer Internet Day. Im Zentrum des Interesses steht an diesem Tag, wie ein besseres Internet für Kinder und Jugendliche realisiert werden kann. Über 100 Länder aus aller Welt beteiligen sich an dem jährlich stattfindenden Aktionstag.

**9. – 12. Februar 2015:**
**E-World**
Strategien, Innovationen und Weichenstellungen für die Zukunft des Energiemarktes stehen im Mittelpunkt der E-World.

**16. – 20. März 2015:**
**CeBIT**
Schwerpunkte des BSI-Messeauftritts auf der CeBIT sind IT-Grundschutz und dessen Weiterentwicklung, Internet-Sicherheit, Cloud Computing, die Allianz für Cyber-Sicherheit sowie sichere Lösungen für die mobile Kommunikation.

**8. – 9. April 2015:**
**Cyber-Angriff TV5 Monde**
Der französische Fernsehsender TV5 Monde wird Opfer eines Cyber-Angriffs. Der Sendebetrieb wird dadurch vorübergehend vollständig zum Erliegen gebracht. Des Weiteren sind Webseite und Social-Media-Kanäle des Senders einige Stunden nicht verfügbar.

**13. – 17. April 2015:**
**Hannover Messe**
Auf der Hannover Messe dreht sich Vieles um Industrie 4.0. Das BSI informiert am eigenen Stand über Herausforderungen der Cyber-Sicherheit und IT-Sicherheitsprojekte mit Bezug zur Industrie. Im Rahmen von Live-Demonstrationen werden mögliche Angriffsszenarien auf industrielle Anlagen und Schutzmöglichkeiten aufgezeigt.

**16. – 17. April 2015:**
**BSI/a-i3 Symposium**
Die Arbeitsgruppe Identitätsschutz im Internet e.V. beschäftigt sich mit dem Schutz von Identitäten und


Identifizierungsdaten im Internet. In Kooperation mit dem BSI tagt im Haus der IT-Sicherheit in Bochum zum zehnten Mal das Symposium und stellt unter anderem das Trusted Cloud Datenschutz-Profil für Cloud-Dienste vor.

**8. Mai 2015:**
**Jobmesse ITS.Connect**
Das BSI nutzt die Firmenkontaktbörse für IT-Sicherheit in der Ruhr-Universität Bochum, um sich als attraktiver Arbeitgeber Studierenden und Absolventen vorzustellen.

**15. Mai 2015:**
**Cyber-Angriff auf den Deutschen Bundestag**
Im Zuge der Abwehr des Cyber-Angriffs auf den Deutschen Bundestag unterstützt das BSI die IT-Experten der Bundestagsverwaltung bei der Analyse des Vorfalls.

**19. – 21. Mai 2015:**
**14. Deutscher IT-Sicherheitskongress**
„Risiken kennen, Herausforderungen annehmen, Lösungen gestalten" - unter diesem Motto steht der 14. Deutsche IT-Sicherheitskongress. Dabei geht es unter anderem um die Absicherung gegen Gefahren im Cyber-Raum und eine hierfür notwendige intensive Kooperation von Staat, Wirtschaft und Wissenschaft.

**7. – 8. Juni 2015:**
**G7-Gipfel, Schloss Elmau**
Erhöhte Cyber-Sicherheit auch beim Zusammentreffen der sieben Staats- und Regierungschefs in Bayern.

**8. – 9. Juni 2015:**
**Deutscher Präventionstag**
Schwerpunktthema des Kongresses in Frankfurt am Main ist „Prävention rechnet sich. Zur Ökonomie der Kriminalprävention." Neben dem Kongress liefert der Deutsche Präventionstag Informationen und Dokumentationen zur Kriminalprävention.

**11. – 12. Juni 2015:**
**Potsdamer Konferenz für Nationale CyberSicherheit**
Veranstaltet vom Hasso-Plattner-Institut führt die Konferenz Vertreter aus Politik, Verwaltung, Wirtschaft und Wissenschaft zusammen, um

Handlungsmöglichkeiten für die Cyber-Sicherheit zu analysieren.

**14. – 19. Juni 2015:**
**27th Annual FIRST Conference**
Auf der jährlichen Konferenz des internationalen Vereins der Computer-Notfall-Teams (FIRST) in Berlin tauschen sich Vertreter internationaler CERTs zu IT-Sicherheitsthemen aus und entwickeln Ansätze für mögliche zukunftsfähige Konzepte zur IT-Sicherheit.

**25. Juli 2015:**
**IT-Sicherheitsgesetz tritt in Kraft**
Das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz) adressiert insbesondere die Betreiber Kritischer Infrastrukturen sowie die Betreiber von Webseiten und führt zu

# Kalender 2015

## Das hat das BSI bewegt

einer Verbesserung der IT-Sicherheit in Deutschland, von der Wirtschaft und Privatanwender profitieren.

**22. – 23. August 2015:**
**FrOSCon**
Der Fachbereich Informatik der Hochschule Bonn-Rhein-Sieg informiert in Kooperation mit FrOSCon e.V. und LUUSA (Linus/Unix Usergroup)

in Vorträgen und Workshops zu Open Source und freier Software. Das BSI ist mit einem Standauftritt vertreten.

**29. – 30. August**
**Tag der offenen Tür der Bundesregierung**
Wie jedes Jahr lädt die Bundesregierung zum Tag der offenen Tür nach Berlin ein. Auch das BSI informiert an Ständen im Bundesinnenministerium und im Bundespresseamt zu Themen der IT- und Internet-Sicherheit.

**1. September 2015:**
**Forum Digitale Gesellschaft**
Die Veranstaltungsreihe beleuchtet zentrale Fragen der voranschreitenden Digitalisierung der Gesellschaft und stellt diese zur Debatte. Auftakt bildet am 21. August die Expertenrunde „Big Data - eine Herausforderung für den Datenschutz“ im Bundesinnenministerium. Am 1. September folgt die Dialogrunde mit Thomas de Maizière zum Thema „Schutz von Bürgern und Online-Handel vor Cyberkriminalität“.

**29. September 2015:**
**UP KRITIS Tagung**
Die öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und zuständigen staatlichen Stellen tagt im Bundespresseamt zum Thema „Schutz Kritischer Infrastrukturen zwischen Kooperation und Regulierung“.

**Oktober 2015:**
**European Cyber Security Month (ECSM)**
Der Aktionsmonat im Rahmen der EU-weiten Kampagne dreht sich um die Cyber-Sicherheit der Bürger. Internetnutzer in Europa sollen für Risiken im Internet sensibilisiert werden und Hilfestellung erhalten. In Zusammenarbeit mit verschiedenen Kooperationspartnern koordiniert das BSI die Aktivitäten anlässlich des ECSM in Deutschland.

**6. – 8. Oktober 2015:**
**it-sa**
Auf der IT-Security-Messe in Nürnberg informieren sich Sicherheitsbeauftragte, Entwickler und Anbieter zu allen Themen rund um IT-Sicherheit, wie Cloud Computing, IT-Forensik, Datensicherung und Hosting.

**18. - 19. November 2015:**
**Nationaler IT-Gipfel**
Zum Zweck der Gestaltung des digitalen Wandels haben Politik, Wirtschaft, Wissenschaft und Gesellschaft mit dem Nationalen IT-Gipfel eine entsprechende Plattform geschaffen. Zentrale Themen aus der Digitalen Agenda der Bundesregierung werden aufgegriffen und innerhalb von konkreten Projekten erarbeitet. Die Vorstellung der Ergebnisse findet auf dem IT-Gipfel in Berlin statt.



**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:** September 2015
**Texte und Redaktion:** Bundesamt für Sicherheit in der Informationstechnik (BSI)
**Konzept, Redaktion und Gestaltung:** Fink & Fuchs Public Relations AG, Berliner Straße 164, 65205 Wiesbaden Internet: www.ffpr.de
**Bildnachweis:** Titel: Steffen Kugler/Bundesregierung; S. 2: ra2studio/Shutterstock (o.l.), Rawpixel/Shutterstock (o.r.); Steffen Kugler/Bundesregierung (u.l.), FWStudio/Shutterstock (u.r.); S. 3: BSI; S. 4: ra2studio/Shutterstock; S. 5: ra2studio/Shutterstock; S. 6: BSI (l.), ra2studio/Shutterstock (r.); S 7: Photonyx Images/Shutterstock (o.), BSI (m.r.); S. 8: Photonyx Images/Shutterstock (o.); S. 9: Photonyx Images/Shutterstock; S. 12: Steffen Kugler/Bundesregierung; S. 13: BSI; S. 14: maraga/Shutterstock (o.), BSI (u.); S. 15: maraga/ Shutterstock, BSI (u.l.), BSI (o.r.); S. 16: Alexandru Marian/ Shutterstock; S. 17: BSI (o.l.), BSI (u.l.); S. 19: Alexandru Marian/Shutterstock; S. 21: urbans/Shutterstock; S. 22: Daniel Kunzfeld/BSI; S. 23: Daniel Kunzfeld/BSI (u.l.), Daniel Kunzfeld/BSI (o.r.); S. 24: Daniel Kunzfeld/BSI (o.l.), Daniel Kunzfeld/BSI (u.l.), Daniel Kunzfeld/BSI (o.r.), Daniel Kunzfeld/BSI (m.o.r.), Daniel Kunzfeld/BSI (m.u.r.), Daniel Kunzfeld/BSI (u.r.); S. 25: Daniel Kunzfeld/BSI (o.l.), Daniel Kunzfeld/BSI (m.u.l.), Daniel Kunzfeld/BSI (u.l.), Daniel Kunzfeld/BSI (o.r.), Daniel Kunzfeld/BSI (m.o.r.), Daniel Kunzfeld/BSI (m.u.r.); S. 26: Rawpixel/Shutterstock (o.), BSI (u.); S. 27: Rawpixel/Shutterstock; S. 28: BSI (m.o.), BSI (m.u.), Rawpixel/Shutterstock (r.); S. 29: BSI (m.u.), hitmanphoto/iStock; S. 30: hitmanphoto/iStock; S. 31: hitmanphoto/iStock; S.32: hitmanphoto/iStock (o.), BMI (m.); S. 33: LoloStock/Shutterstock (o.), BSI (u.); S. 34: gui jun peng/Shutterstock;
S. 35: gui jun peng/Shutterstock; S. 36: gui jun peng/Shutterstock (o.), BSI (m.l.), Piotr Adamowicz/Shutterstock; S. 37: gui jun peng/Shutterstock (o.), Gencho Petkov/Shutterstock (u.); S. 38: Den Rise/Shutterstock; S. 39: Den Rise/Shutterstock; S. 40: Daniel Kunzfeld/BSI; S. 41: Daniel Kunzfeld/BSI; S. 42: BSI; S. 44: Steffen Kugler/Bundesregierung (m.u.), BSI (o.r.); S. 45: BSI (o.l.), Steffen Kugler/Bundesregierung (o.r.), K. Herschelmann/Hasso Plattner Institut (m.r.); S. 46: BSI (m.), Rainer Jensen/dpa (u.r)
**Druck:** Druck- und Verlagshaus Zarbock GmbH & Co KG, Sontraer Str. 6, 63086 Frankfurt a.M., Internet: www.zarbock.de
**Artikelnummer:** BSI-Mag 15/702
Das BSI-Magazin erscheint zweimal im Jahr. Es ist Teil der Öffentlichkeitsarbeit des BSI. Es wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

www.bsi.bund.de