Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Magazin 2017/01

Mit Sicherheit

Cyber-Sicherheitsstrategie für Deutschland 2016

BSI INTERNATIONAL

BSI: Schlüsselrolle im Avalanche-Takedown

CYBER-SICHERHEIT

Gut gerüstet für neue Bedrohungslagen

DAS BSI

180 neue Köpfe für eine gemeinsame Mission

EDITORIAL

Neue Dimension

„Die Bedrohung durch professionelle und vermutlich staatlich gelenkte Cyber-Angriffe ist hoch."

Eine Information im gesellschaftlichen Bewusstsein verlässlich zu verankern, ist eine ebenso herausfordernde wie komplexe Aufgabe. Vor allem, wenn diese Information zwar von allen Experten als existenziell wichtig, von der Bevölkerung, der Wirtschaft und der Verwaltung aber als mehr oder minder marginal eingestuft wird. Die Information, dass Cyber-Sicherheit existenziell wichtig ist, hat lange Zeit so sehr unter diesem „Verdikt" gelitten, dass manche Warner von „digitaler Sorglosigkeit" sprachen, aber gern überhört wurden.

Doch die Zeiten haben sich geändert. Spätestens seit Krankenhäuser, Kraftwerke, Telekommunikationsanbieter gehackt und erpresst wurden, spätestens seit der Bundestag und die Parteien angegriffen wurden, spätestens seit die US-Geheimdienste von gezielter Wahlbeeinflussung durch Russlands Regierung berichtet haben, ist das Thema Cyber-Sicherheit im Bewusstsein einer breiten Öffentlichkeit angekommen.

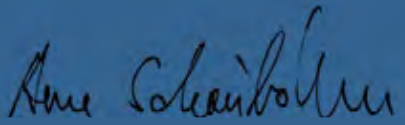
Auch in Europa, auch in Deutschland, stehen wichtige Wahlen an. Dies allein ist Anlass genug, sich über eine mögliche gezielte Manipulation der öffentlichen Meinung durch Dritte zu sorgen, insbesondere im Hinblick auf den Bundestagswahlkampf 2017. Gemeinsam mit anderen europäischen Sicherheitsbehörden versucht das BSI daher, eine mögliche Beeinflussung kommender Wahlen durch Cyber-Angriffe zu verhindern. Die Verteidigungsfähigkeit der Regierungsnetze wird hierzu kontinuierlich optimiert.

Die Bedrohung durch professionelle und vermutlich staatlich gelenkte Cyber-Angriffe ist hoch. Wie aus unserem aktuellen Lagebericht hervorgeht, wurden in den Regierungsnetzen monatlich rund 44.000 infizierte E-Mails abgefangen, bevor sie im Postfach eines Empfängers landeten. Im Vergleich zum Vorjahr handelt es sich um eine Vervierfachung. Täglich gibt es rund 20 hochspezialisierte Angriffe auf das Regierungsnetz.

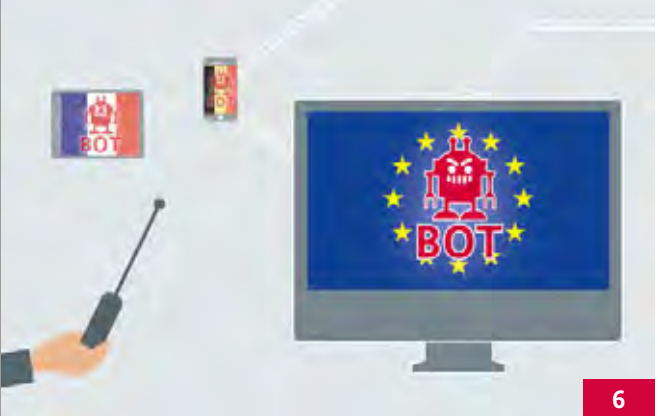
Doch nicht nur der Angriff an sich ist eine Gefahr. Viel schwerer wiegt die politische Dimension und Wirkrichtung dieser Angriffe. Sie müssen gar nicht erfolgreich sein. Sie müssen nur den Zweifel säen, dass ein demokratisches Wahlergebnis nicht an der Wahlurne, sondern im Hinterzimmer einer (staatlich beauftragten) Hackergruppe entstanden ist.

Darum ist es so wichtig, dass das Bewusstsein für die Bedeutung von Cyber-Sicherheit jetzt in der Öffentlichkeit angekommen ist. Diese Karte müssen wir spielen. Wir müssen kontinuierlich und öffentlichkeitswirksam informieren. Und wir müssen zeigen, wie wir die Widerstandsfähigkeit Deutschlands gegen Cyber-Gefahren jeglicher Art erfolgreich erhöhen. Das BSI als die nationale Cyber-Sicherheitsbehörde wird dabei eine prägende Rolle einnehmen.

Ich wünsche Ihnen eine anregende Lektüre.



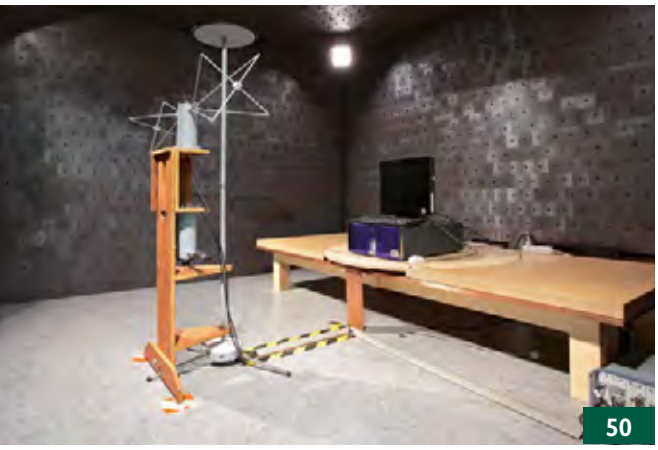
Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik



6


16


32


50

58

INHALT

AKTUELLES


Foto: Catharina Frank

ECSM

European Cyber Security Month

Auch in diesem Jahr beteiligt sich das BSI wieder am European Cyber Security Month (ECSM, https://cybersecurity-month.eu/). Der europaweite Aktionsmonat zielt darauf ab, EU-Bürger, Organisationen und Unternehmen für das Thema IT-Sicherheit zu sensibilisieren und das Bewusstsein für die Bedrohungen der Cyber-Sicherheit zu schärfen. Unter Federführung der europäischen IT-Sicherheitsbehörde European Union Network and Information Security Agency (ENISA) finden den ganzen Oktober über Aktionen, Veranstaltungen und Awareness-Kampagnen statt. Das BSI fungiert hierbei sowohl als Koordinierungsstelle für Deutschland als auch als Akteur mit eigenen Maßnahmen.

https://www.bsi.bund.de/ECSM

Rückblick

6. Deutscher IT-Sicherheitspreis 2016

Bereits zum 6. Mal wurde im vergangenen Oktober der Deutsche IT-Sicherheitspreis von der Horst Görtz Stiftung in Darmstadt verliehen. Die Schirmherrschaft übernahm erstmals Bundesforschungsministerin Prof. Dr. Johanna Wanka. Unter 45 Einreichungen wählte eine Expertenjury die jeweils beste Innovation aus den Bereichen IT-Sicherheit, Kryptografie, System- und Netzsicherheit sowie Abwehr von Cyber-Angriffen aus. Mit dem Preis möchte die Stiftung einen kleinen Beitrag für IT-Sicherheit „Made in Germany“ leisten. Die Jury setzt sich aus IT-Sicherheitsfachleuten aus Wissenschaft und Wirtschaft zusammen.

Sicherer E-Mail-Dienst

Posteo erhält als Erster Zertifikat

Das BSI hat im Dezember 2016 die finale Fassung der Technischen Richtlinie „Secure E-Mail Transport“ und die dazugehörige Prüfspezifikation veröffentlicht, auf dessen Basis Posteo als erstem E-Mail-Dienstanbieter ein Zertifikat über sichere E-Mail-Dienste ausgestellt wurde. Hierzu erklärt Arne Schönbohm, Präsident des BSI: „Mit der Technischen Richtlinie setzen wir einen neuen Standard für die Cyber-Sicherheit in der Digitalisierung, von dem E-Mail-Provider und Anwender gleichermaßen profitieren.“

https://www.bsi.bund.de/dok/8664710

CeBIT 2017

Das BSI auf der CeBIT

Vom 20. - 24. März 2017 ist das BSI mit den Fokusthemen Cyber-Sicherheit, IT-Grundschutz sowie Mobile Security auf der CeBIT vertreten. Interessierte Besucher erfahren am Messestand mehr über Angebote und Lösungen des BSI für mehr IT- und Cyber-Sicherheit in Staat, Wirtschaft und Gesellschaft. Absolventen und Bewerber können sich zudem über die Karrieremöglichkeiten in der Cyber-Sicherheitsbehörde informieren. Zu finden ist das BSI auf der CeBIT in Halle 6, Stand H30.

CSCG

Cyber Security Challenge Germany

Talentierte Nachwuchskräfte im Bereich der IT-Sicherheit sind nach wie vor gefragt. Das Institut für Internet-Sicherheit if(is) und der TeleTrusT Bundesverband IT-Sicherheit e.V. möchten bei der jährlichen „Cyber Security Challenge Germany“ (CSCG, https://www.cscg.de/) neue Talente entdecken. Nachwuchshacker von 14 bis 30 Jahren sind ab Mai dazu aufgerufen, spannende Online-Challenges zu lösen. Die Gewinner des Finales im September in Berlin dürfen sich dann bei der European Cyber Security Challenge (ECSC) mit der europäischen Elite messen.

E-world energy & water

Rückblick

BSI als Aussteller auf der Messe E-world 2017

Das BSI beteiligte sich bereits zum fünften Mal mit einem Ausstellungsstand an der Messe „E-world energy & water“, die vom 7. bis 9. Februar 2017 in Essen stattfand. Mit mehr als 24.000 Besuchern und 640 Ausstellern ist die E-world die europäische Leitmesse der Energie- und Wasserwirtschaft. Das BSI informierte wieder über die Sicherheits- und Interoperabilitätsvorgaben (Schutzprofile, Technische Richtlinie TR-03109) für das Smart Meter Gateway, die Smart Metering PKI, die Zertifizierung nach Common Criteria sowie Informationssicherheit bei Administration und Betrieb intelligenter Messsysteme.

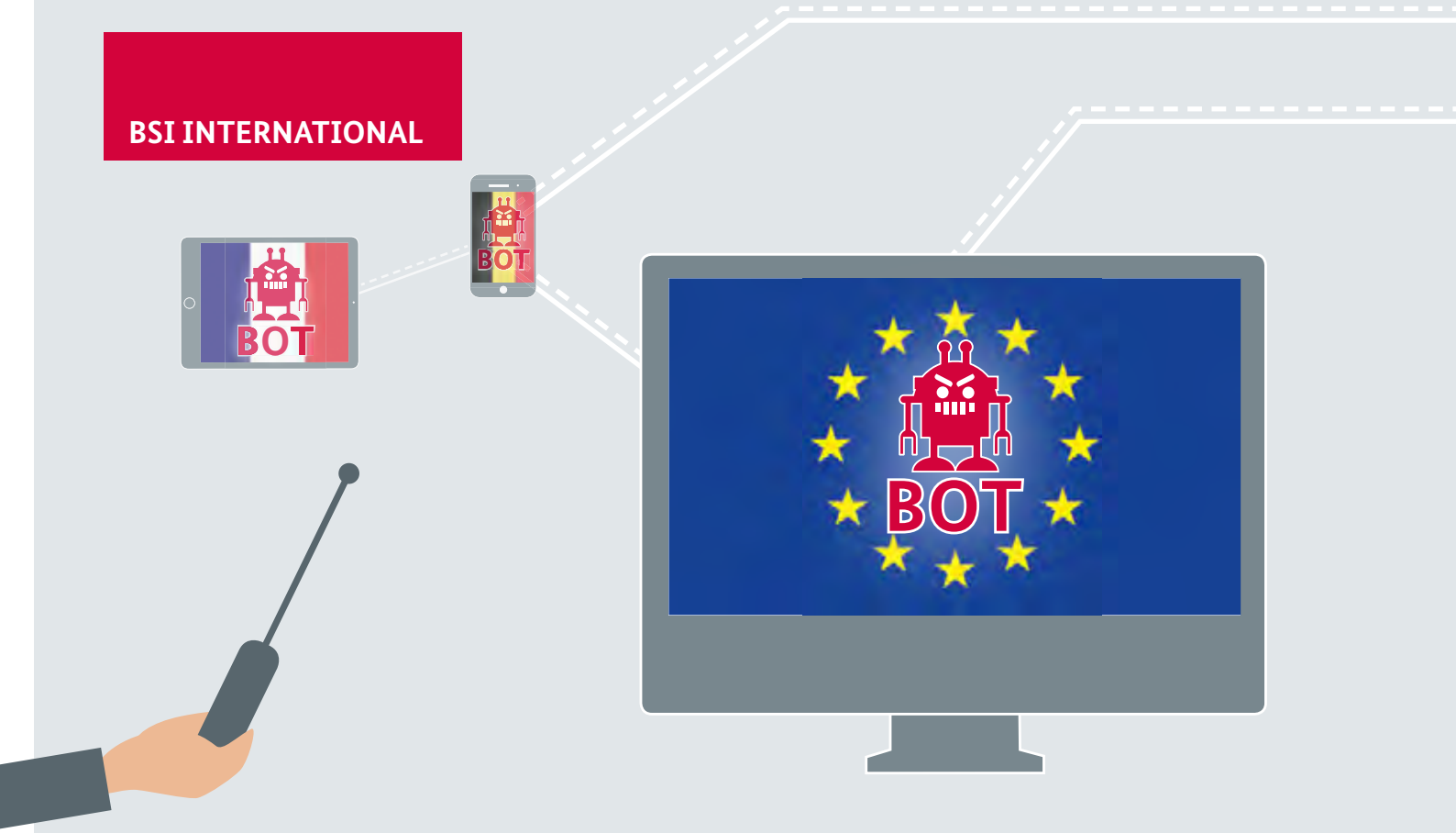
www.bsi.bund.de/SmartMeter

Auf der Zielgeraden

Die Modernisierung des IT-Grundschutzes

Ein bedeutender Schritt bei der Überarbeitung der bewährten BSI-Methodik zum Aufbau eines ganzheitlichen Informationsmanagementsystems ist geschafft: Der im Herbst 2016 vorgestellte Community Draft des Risikomanagement-Standards 200-3 beinhaltet erstmals alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes. Dadurch können Anwender künftig mit deutlich weniger Aufwand ein angestrebtes Sicherheitsniveau erreichen. Zur CeBIT 2017 wird der Standard 200-2 zur IT-Grundschutz-Vorgehensweise vorgestellt. Mit der Veröffentlichung dieser Publikationen sind zwei Meilensteine im Rahmen der IT-Grundschutz-Modernisierung gesetzt. Im nächsten Schritt werden weitere Bausteine für das IT-Grundschutz-Kompendium veröffentlicht.

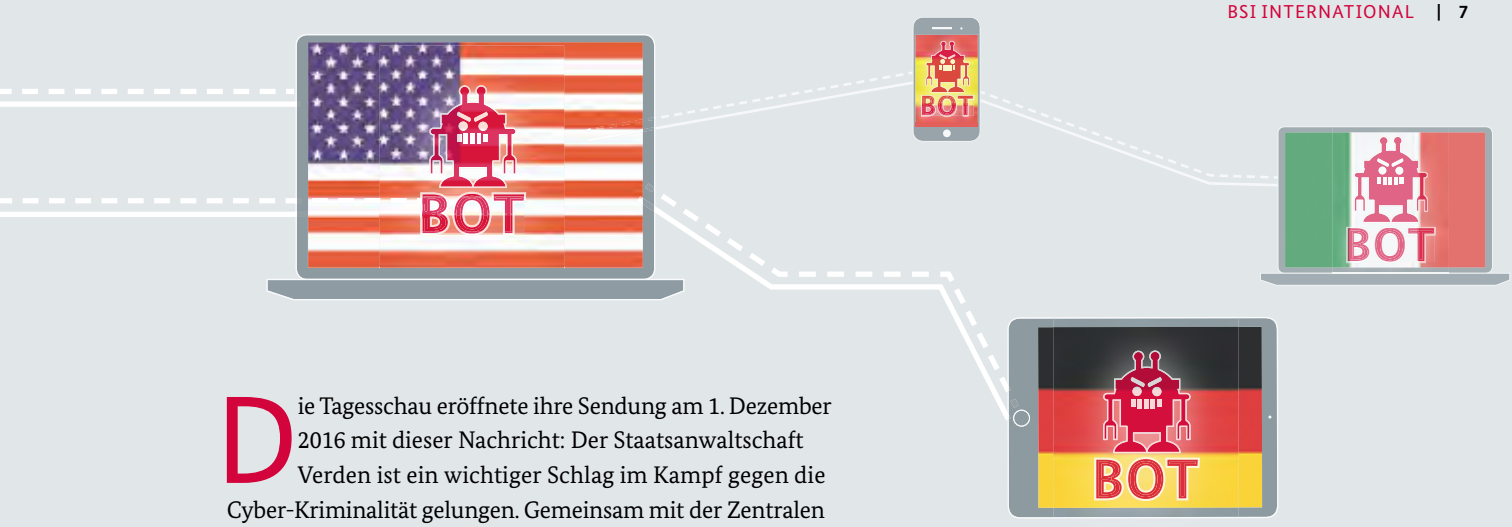
BSI INTERNATIONAL



BSI: Schlüsselrolle im Avalanche-Takedown

Schlag gegen internationale Cyber-Kriminalität

Den deutschen Strafverfolgungsbehörden gelang am 30. November 2016 ein spektakulärer Coup gegen die internationale Cyber-Kriminalität: Mit der Zerschlagung des Botnetzinfrastruktur Avalanche wurde ein Schadsoftware-Ring ausgehoben, der mindestens seit 2009 weltweit Millionen von Internetnutzern geschädigt hatte. Blickt man hinter die Kulissen der jahrelangen Ermittlungen, wird deutlich, dass es kein Zufall war, dass die Mitwirkenden des Fahndungserfolgs ausgerechnet im Herzen der Bundesrepublik zu finden sind. Denn als nationale Cyber-Sicherheitsbehörde leistete das BSI einen international bedeutenden Beitrag zu diesem wichtigen Etappensieg im immerwährenden Kampf gegen das Verbrechen im Internet. Der Fall „Avalanche“ ist ein Paradebeispiel, das die Bedeutung des BSI als Gestalter der Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft anschaulich illustriert.



Die Tagesschau eröffnete ihre Sendung am 1. Dezember 2016 mit dieser Nachricht: Der Staatsanwaltschaft Verden ist ein wichtiger Schlag im Kampf gegen die Cyber-Kriminalität gelungen. Gemeinsam mit der Zentralen Kriminalinspektion (ZKI) Lüneburg konnten Verantwortliche des seit mindestens 2009 international agierenden Bot-Netzwerks Avalanche verhaftet werden. Bundesinnenminister Dr. Thomas de Maizière nannte die Aktion einmalig und bezeichnete sie als „eine Kampfansage an die internationale Kriminalität im Cyber-Raum".

Die Festnahmen sind ein Höhepunkt des immer noch anhängigen jahrelangen Ermittlungsverfahrens. In der Natur der Sache liegt, dass Internetverbrechen nicht mit den klassischen Methoden der Strafverfolgung aufgeklärt werden können – schon allein deshalb, weil das Internet bekanntermaßen keine Ländergrenzen kennt. So waren Behörden und Institutionen aus mehr als 30 Ländern an den Vorbereitungen beteiligt, darunter Strafverfolger aus den USA, einschließlich FBI, sowie Europol, die Non-Profit-Organisation „The Shadowserver Foundation", Fraunhofer FKIE und weitere internationale Partner. Die enge Abstimmung zwischen allen Beteiligten, darunter das BSI, über Präsenzmeetings, Telefon- und Videokonferenzen während des gesamten Verfahrens war für den Erfolg von höchster Bedeutung.

TECHNISCHES KNOW-HOW EINGEBRACHT

Auch innerhalb der Bundesrepublik waren neben der Staatsanwaltschaft Verden und der ZKI Lüneburg eine Reihe weiterer Institutionen wie das LKA Niedersachsen und das BKA involviert. Eine herausragende Rolle beim Kampf gegen Avalanche spielte das BSI mit Unterstützung der Botnetzforscher des Fraunhofer FKIE: Zwar ist das BSI keine Strafverfolgungsbehörde, konnte aber durch sein technisches Know-how und die erforderlichen Infrastrukturen entscheidend dazu beitragen, die Täter dingfest zu machen.

Zur Unterstützung der Strafverfolgungsbehörden erfolgte unter anderem eine Binärcodeanalyse der Schadsoftware von mehr als 20 Botnetzen, eine Analyse von C&C-Servern, die Generierung der Botnetzdomänen sowie die Realisierung neuer innovativer Sinkholemechanismen inkl. der benötigten Software.

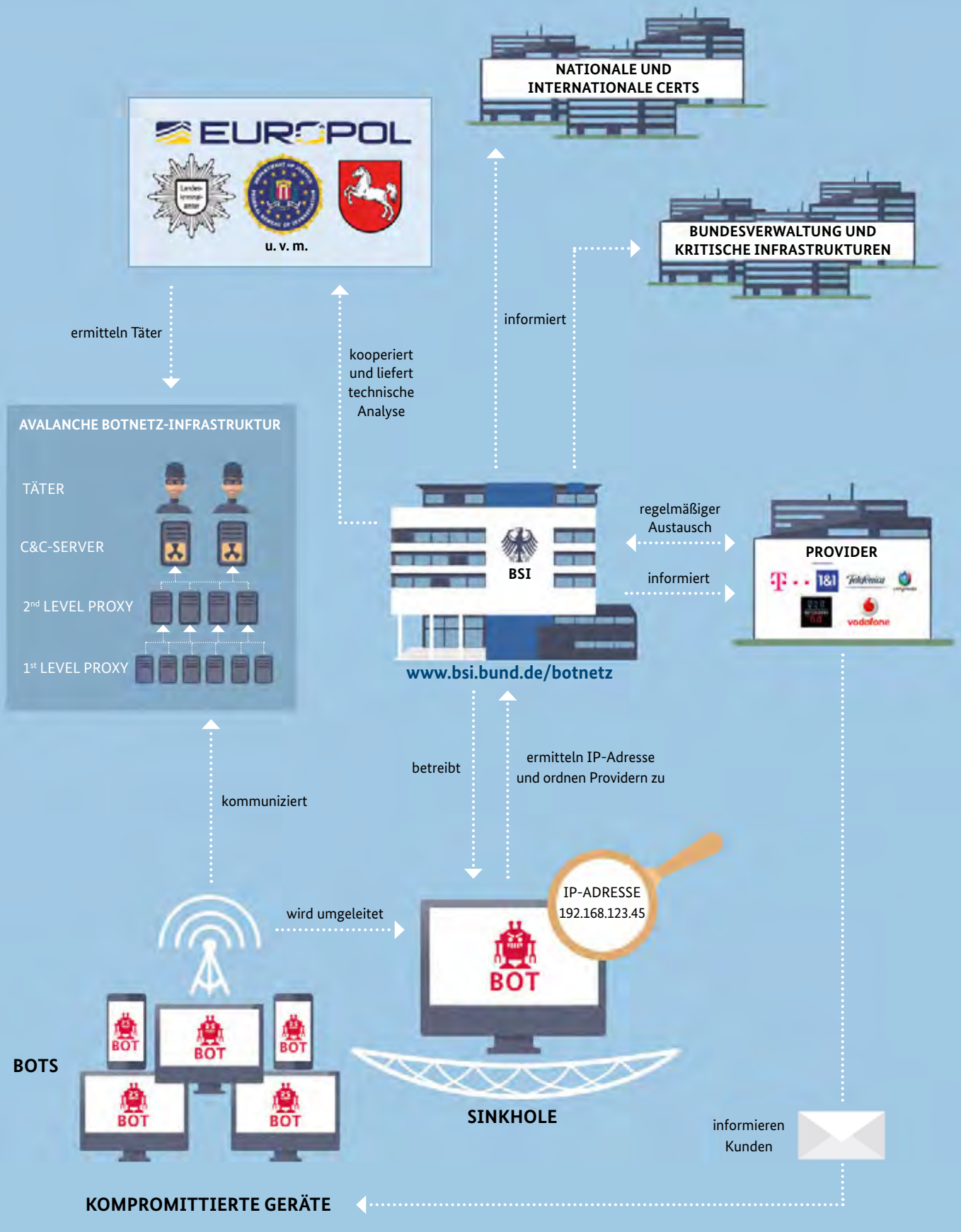
Avalanche ist nicht die erste Botnetzinfrastruktur, die erfolgreich abgeschaltet wurde. Das Besondere aber: Bei dieser Aktion wurden nicht nur 20 Botnetze gleichzeitig abgeschaltet, sondern es wurden konsequent von Anfang an die Strafverfolgungsbehörden unterstützt und einbezogen. Wenn, wie bereits häufiger geschehen, IT- oder Sicherheitsfirmen Botnetze lahmlegen, tauchen sie kurze Zeit später an anderer Stelle wieder auf – denn die Urheber werden nicht belangt. Umgekehrt finden Strafverfolgungsbehörden in anderen Ländern bei Operationen gegen Cyber-Verbrechen keine solche technische Unterstützung wie hier durch das BSI.

Den Stein ins Rollen brachten Strafanzeigen von Opfern der Angriffswelle durch die als „Windows-Verschlüsselungs-Trojaner" bekannt gewordene Ransomware im Jahr 2012. Sie tappten in die Falle der ersten auffällig gewordenen Ausläufer von Avalanche, indem sie Anhänge von Phishing-Mails öffneten, in denen sich Erpresser-Software verbarg. Der Schadcode verschlüsselte die Festplatten der Nutzer, eine Meldung mit der Aufforderung zur Zahlung eines „Lösegelds" erschien – andernfalls würden die Daten auf ewig verschlüsselt bleiben. Nach ersten Ermittlungen durch das ZKI Lüneburg und die Staatsanwaltschaft Verden erging im Sommer 2013 ein Unterstützungsgesuch an das BSI.

THE SHADOWSERVER FOUNDATION

The Shadowserver Foundation wurde 2004 gegründet. Die Vereinigung von freiwilligen Internet-Sicherheitsspezialisten hat sich zum Ziel gesetzt, einen aktiven Beitrag im Kampf gegen das Internetverbrechen zu leisten. Wesentlicher Bestandteil der Arbeit ist das Sammeln von Erkenntnissen über infizierte Systeme sowie kriminelle Strukturen und deren Weitergabe zur Warnung Betroffener. Im Avalanche-Verfahren unterstützte das Expertenteam als Schnittstelle zu den Domain-Registries sowie bei der Bereitstellung von Servern zur Etablierung der Sinkholes. **Weitere Informationen unter www.shadowserver.org**

ZERSCHLAGUNG DER BOTNETZ-INFRASTRUKTUR „AVALANCHE“



SCHUTZ DER BÜRGER AN ERSTER STELLE

Bereits in dieser frühen Phase der verdeckten Ermittlungen der Strafverfolger lag der Fokus des BSI darauf, Internetnutzer vor den Avalanche-Angriffen zu schützen. Dabei konnte das BSI auf eine etablierte Infrastruktur zurückgreifen. Bereits bei anderen Anlässen hatte das BSI Warnungen über die Plattform BSI für Bürger herausgegeben und mit Partnern wie botfrei.de und dem Anti-Botnetz-Beratungszentrum zusammengearbeitet. Nur wenig später, im Januar und April 2014, warnte das BSI die Öffentlichkeit zudem zweimal vor den Folgen eines 37-millionenfachen Identitätsdiebstahls. Auch dieser ging auf das Konto der Strippenzieher hinter Avalanche, auch wenn dies in Anbetracht der laufenden Ermittlungen nicht preisgegeben werden konnte.

Internet-Anbieter (Provider) bekommen täglich eine Flut von Meldungen über infizierte Systeme, die jedoch teilweise auch falsche und unzutreffende Daten enthalten. Infolgedessen konnten früher Opfer häufig nicht informiert werden. Um diesem Problem zu begegnen, etablierte das BSI mit dem Providerinformationssystem PI einen weltweit einzigartigen Informationskanal. Damit werden Infektionsmeldungen aus hochqualitativen und geprüften BSI-Quellen bei den Providern mit hoher Priorität bearbeitet. Denn nur die Provider können die IP-Adressen einem Netzwerkanschluss zuordnen, nicht das BSI selbst. Nach Kenntnis des BSI entstand so eine weltweit besondere Zusammenarbeit. Ab August 2014 informiert das BSI auf diese Weise stündlich die Provider über infizierte Rechner. Diese können anhand der IP-Adressen nachverfolgen, welche Kunden betroffen waren, und sie entsprechend warnen. So konnten – schon lange vor dem Takedown – die Nutzer vor den Folgen geschützt werden. Zudem stellte das BSI Signaturen, die aus der Analyse der ermittelten Schadcode-Varianten gewonnen wurden, den Herstellern von Antiviren-Software zur Verfügung. So profitierten deren Nutzer von dieser Maßnahme. Vorausgesetzt, diese hielten ihre Schutzsoftware immer auf dem aktuellen Stand.

DIE FALLE SCHNAPPT ZU

Neben dem wichtigen Schutz der Bürger hat das BSI die Ausmaße der Botnetz-Infrastruktur weiter untersucht und analysiert – ein enormer Aufwand, zumal Avalanche sehr weit verzweigt war. Wie sich später herausstellen sollte, waren Opfer in über 180 Ländern betroffen. Auch die Komplexität der Infrastruktur war hoch: Sie bestand aus einer mehrstufigen Anordnung von Proxyservern zur Verschleierung der eigentlichen Command&Control-Server, die mit Double-Fast-Flux-Technologie arbeitete – diese sorgt dafür, dass Serverstandorte und Domains blitzschnell gewechselt werden können, um sich der Entdeckung zu entziehen. Mit diesen Erkenntnissen konnte das BSI helfen, den letzten entscheidenden Schritt vorzubereiten: den Takedown von Avalanche, bei dem am 30. November 2016 über 800.000 Domains beschlagnahmt oder blockiert wurden. Es folgten insgesamt fünf Festnahmen, 37 Hausdurchsuchungen und die Beschlagnahme von 39 Servern in verschiedenen Ländern – 221 weitere Server wurden durch die Hosting-Provider abgeschaltet.

Das Ermittlungsverfahren ist damit zwar noch nicht beendet. Der Takedown bedeutet dennoch einen wichtigen Sieg – und trägt dazu bei, das Internet zu einem sichereren Ort zu machen. Für mindestens ein Jahr werden die Bots auf das Sinkhole umgeleitet, sodass die Botnetze nicht mehr von Kriminellen genutzt werden können. So lange haben Anwender zunächst Zeit, ihre Rechner zu säubern und besser zu schützen. ■

SINKHOLING

Als Sinkhole wird ein Computersystem bezeichnet, auf das Anfragen von botnetzinfizierten Systemen umgeleitet werden. Im Falle von Avalanche hat das BSI in Zusammenarbeit mit Fraunhofer FKIE und der Shadowserver Foundation die Sinkhole-Infrastruktur aufgesetzt. In der Folge konnten die Bots der Avalanche-Infrastruktur nicht mehr mit den Servern der Urheber kommunizieren – die Kontrolle über die befallenen Rechner wurde ihnen auf diese Weise entrissen. Voraussetzung für die Einrichtung von Sinkholes ist das Wissen der Behörde um die Botnetz-Domänen der Avalanche-Botnetze. Nur so können die ermittelten Domänen auf Sinkhole-Server umgeleitet werden, sodass die Bots nicht mehr von den Tätern kontrolliert werden können. Zudem bieten Sinkholes einen weiteren Vorteil: Auf dem Sinkhole-System werden die Aufrufe der anfragenden Rechner mit IP-Adressen und Zugriffszeit registriert. Das BSI konnte somit die jeweiligen Provider der Nutzer identifizieren und ihnen die gesehenen IP-Adressen weiterleiten. Diese wiederum erhielten dadurch die Möglichkeit, die betroffenen Kunden anhand der IP-Adressen zu erkennen und ihnen entsprechende Warnungen und Empfehlungen zur Desinfektion ihrer Computer zukommen zu lassen. Sinkholes stellen somit eine unverzichtbare Infrastruktur für die Zerschlagung von Botnetzen dar.

Weitere Informationen: https://www.bsi-fuer-buerger.de/botnetze

Neues Label für Cloud-Sicherheit

von Dr. Clemens Doubrava, Referat Informationssicherheit in der Cloud und in Anwendungen

BSI und ANSSI entwickeln gemeinsam ESCloud Label

Mit der Gründung der Working Group „ESCloud“ starten BSI und ANSSI (Agence nationale de la sécurité des systèmes d'information) gemeinsam eine Initiative zur Cloud-Sicherheit. Perspektivisch soll sie in eine gesamteuropäische Kooperation münden.

Am 12. Dezember 2016 unterzeichneten Arne Schönbohm (Präsident des BSI) und Guillaume Poupard (Directeur général der ANSSI) ein Memorandum of Understanding, mit dem sie die Working Group „ESCloud“ gründeten, die das Label weiterentwickeln wird. Am Folgetag wurde dies dann öffentlichkeitswirksam auf der Digitalkonferenz im Rahmen der Deutsch-Französischen Konsultationen vor herausragenden Persönlichkeiten aus Politik und Wirtschaft vorgestellt. Und auch Bundesinnenminister Dr. Thomas de Maizière ließ es sich nicht nehmen, die Wichtigkeit des Vorhabens persönlich zu unterstreichen.

Das Vorhaben steht in der Kontinuität der Zusammenarbeit, die sich seit vielen Jahren zwischen den beiden nationalen Cyber-Sicherheitsbehörden bewährt hat.

NEUE WEGE DER ZUSAMMENARBEIT

Mit dem ESCloud-Label und der Working Group wird ein ganz neuer Weg beschritten. Bei den bisherigen Kooperationen (z. B. bei den Zertifizierungen nach Common Criteria) einigte man sich auf eine gemeinsame Art der Prüfung, die dann von den Partnern in gleicher Weise und Qualität durchgeführt wird. So kann das Ergebnis auch von den anderen Partnern wie ein eigenes akzeptiert werden.

ESCloud geht hier noch einen Schritt weiter. Unter dem Qualitätslabel werden ganz unterschiedliche Ansätze vereint, die beide die Sicherheit von Cloud-Diensten definieren und nachweisen. Aufseiten der ANSSI ist das deren eigene Zertifizierung nach „SecNumCloud“ und das BSI bringt das Wirtschaftsprüfer-Testat nach dem BSI-Anforderungskatalog C5 ein. Beide führen zu einem Sicherheitsniveau, das professionelle Cloud-Dienste auf jeden Fall erreichen sollten.

Dieses Konstrukt funktioniert nur, da es auf verschiedenen bestehenden Voraussetzungen basiert. Zunächst braucht es eine sehr große Übereinstimmung bei den Zielen bezüglich der Informationssicherheit von Cloud-Diensten. Diese sind in den sogenannten Core Principles von ESCloud definiert. Hinzu kommt das auf gute und langjährige Erfahrungen gegründete Vertrauen, dass der Weg des anderen ein äquivalent guter ist. Die Entscheidung für die eine oder andere Vor-

v. l. n. r.: Generaldirektor der französischen Cyber-Sicherheitsbehörde ANSSI Dr. Guillaume Poupard, Bundesinnenminister Dr. Thomas de Maizière und BSI-Präsident Arne Schönbohm

gehensweise ist ja in jedem Fall wohlbegründet und geht von bestimmten Voraussetzungen aus. Und diese sind in Deutschland und Frankreich unterschiedlich. Auf beiden Wegen wird das Ziel erreicht. Und schließlich darf nicht ein Konkurrenzdenken oder eine negative Einstellung des „not invented here" zu einer Handlungsmaxime werden, die eine gemeinsame Arbeit ad absurdum führen würde.

Die lange Zusammenarbeit und das gemeinsame Ziel ermöglichen es dem BSI und der ANSSI, diesen Weg zu gehen.

EUROPA IM BLICK

Mit dem gesunden Selbstbewusstsein und der ausgewiesenen Expertise, die beiden Behörden zu eigen ist, kann der Kreis derer, die an ESCloud mitarbeiten möchten, weiter ausgebaut werden, um das Ganze zu einer europäischen Dimension zu führen. Auf diese Weise werden europäische Werte wie die Zusammenarbeit und das Vertrauen verschiedener Nationen und Kulturen eindrucksvoll unterstrichen: Anstatt zu versuchen, alles gleich zu machen, lässt man sich von Unterschieden nicht beirren und strebt einem gemeinsamen Ziel entgegen.

STÄNDIGER AUSTAUSCH

So war das BSI dieses Jahr auch wieder auf der französischen IT-Sicherheitsmesse „Forum FIC" (Forum International de la Cybersécurité) vertreten und konnte den BSI-Anforderungskatalog C5 sowie ESCloud gemeinsam mit der ANSSI in einem gut besuchten Workshop auf der Messe vorstellen. Die Reaktionen auf diese neue Zusammenarbeit sind durchweg positiv. Der neue BSI-Vizepräsident Dr. Gerhard Schabhüser nutzte seine Anwesenheit zur Kontaktpflege und um ein besseres Verständnis der Marktteilnehmer zu bekommen. Dies hilft in beiden Ländern, Lösungen zu entwickeln, die über die eigenen Grenzen hinaus die Herausforderungen bestmöglich adressieren. ■

ESCloud

Weitere Informationen: https://www.bsi.bund.de/ESCloudLabel

C5 – Praktische Cloud Compliance

von Dr. Markus Held, Referatsleiter Informationssicherheit in der Cloud und in Anwendungen

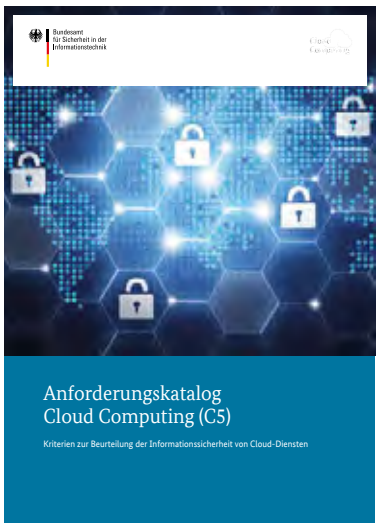
Sicherheitsempfehlungen für Cloud-Computing-Anbieter

Cloud Computing ist ein wesentlicher Baustein der Digitalisierung. Geschäftsprozesse und Geschäftsmodelle verändern sich damit schneller als je zuvor operativ und strategisch. Damit die Wertschöpfung nachhaltig funktioniert, muss aber nach wie vor eine angemessene IT-Sicherheit gewährleistet sein.

Der zur CeBIT 2016 vom BSI vorgestellte Anforderungskatalog Cloud Computing C5 (Cloud Computing Compliance Controls Catalogue) wurde vom Markt so gut angenommen, dass bereits das erste Testat auf Basis des C5 an Amazon Web Services vergeben werden konnte. C5 fasst diejenigen Sicherheitsanforderungen an Cloud-Diensten zusammen, die bei einem professionellen Cloud-Einsatz keinesfalls unterschritten werden sollten. Hinzu kommen Transparenzanforderungen zu den Rahmenbedingungen der Leistungserbringung des Cloud-Anbieters (z. B. Systembeschreibung, Angaben über die zuständige Jurisdiktion und staatliche Zugriffsrechte auf die Daten).

Das BSI rät Unternehmen und Behörden, darauf zu bestehen, dass der Cloud-Anbieter sich vertraglich mindestens verpflichtet, den C5 einzuhalten. Entsprechende Nachweise sollten unbedingt eingefordert werden. Die Erfüllung der Anforderungen und die Richtigkeit der Transparenzangaben

v. l. n. r.: PwC-Vorstandssprecher Prof. Dr. Norbert Winkeljohann, Vice President Compliance von Box Crispen Maung und BSI-Präsident Arne Schönbohm, bei der Übergabe des C5-Testats an Box.



sollten mindestens durch die Vorlage eines von Wirtschaftsprüfern testierten Prüfungsberichts nachgewiesen werden. Auf dieser Basis können Cloud-Kunden einerseits eine fundierte Entscheidung treffen, ob ein Cloud-Dienst den eigenen Ansprüchen genügt. Andererseits ist im C5-Konzept explizit vorgesehen, dass Kunden mit den Cloud-Diensten eigene, höherwertige Anforderungen aushandeln können.

BSI IM DIALOG MIT DER WIRTSCHAFT ZU CLOUD COMPUTING

Anfang Februar 2017 lud das BSI Vertreter der Wirtschaft und wirtschaftsnaher Behörden zur Veranstaltung „BSI im Dialog“ zum Thema Cloud-Sicherheit nach Frankfurt am Main ein. Der Vorstandssprecher von PwC Deutschland, Prof. Dr. Norbert Winkeljohann, betonte bei seiner Begrüßungsrede die Notwendigkeit, in der Digitalisierung die Sicherheit von Cloud Computing nachvollziehbar zu gestalten. BSI-Präsident Arne Schönbohm zeigte auf, welche strategische Bedeutung die Sicherheit von Cloud Computing für das BSI als nationale Cyber-Sicherheitsbehörde hat. Er mahnte zudem an, dass das im Anforderungskatalog C5 definierte Sicherheitsniveau beim professionellen Cloud-Einsatz nicht unterschritten werden darf. Überdies kündigte er die Veröffentlichung eines BSI-Mindeststandards zur sicheren Cloud-Nutzung an, der alle Bundesbehörden anhalten werde, beim Einsatz externer Cloud-Dienste den C5 einzufordern. Dr. Markus Held, Referatsleiter für Informationssicherheit in der Cloud und in Anwendungen beim BSI, gab in seinem Vortrag einen Überblick über das Cloud-Sicherheits-Portfolio des BSI, das im Austausch mit der Praxis stetig weiterentwickelt wird. Im Anschluss erläuterte der renommierte Datenschutz-Experte Prof. Dr. Georg Borges von der Universität des Saarlandes die Cloud-Datenschutzzertifizierung TCDP. Ergänzend führte Markus Vehlow, Partner bei PwC, aus, wie eine gemeinsame Prüfung von Datenschutz und IT-Sicherheit bei Cloud-Diensten auf Basis von TCDP und C5 effizient durchgeführt werden kann. Die Seite der Cloud-Anbieter vertrat Crispen Maung, Vice President Compliance von Box, Inc., der aufzeigte, dass Compliance zu Sicherheitsstandards für professionelle Cloud-Anbieter ein wichtiger Wettbewerbsfaktor ist. Zum Abschluß überreichten die Wirtschaftsprüfer von PwC das neu erlangte C5-Testat an Box, Inc., vertreten durch Herrn Maung.

AUSBLICK UND FAZIT

Mit dem „Mindeststandard Sichere Nutzung von Cloud-Diensten“ werden Dienststellen der Bundesverwaltung angehalten, angemessene Prozesse zur Sicherstellung der Cloud-Sicherheit durchzuführen und beim Bezug von Cloud-Diensten auf die Einhaltung des C5 zu achten. In Kürze wird das BSI zudem ein gemeinsames Papier mit dem internationalen IT-Revisorenverband ISACA veröffentlichen, das eine Prüfung durch Innenrevisoren des Cloud-Anbieters oder des Cloud-Kunden auf C5-Basis unterstützt.

Das BSI legt bei der Weiterentwicklung des C5 und des zugehörigen Produktportfolios Wert auf Praxisnähe und den engen Dialog mit allen Interessenvertretern aus Staat, Wirtschaft und Gesellschaft. Auf dieser Basis wird das BSI seine Cloud-Sicherheitsstandards konsequent und kontinuierlich pflegen und weiterentwickeln. ■

Das Bundeskabinett hat Ende Januar den Gesetzesentwurf zur Umsetzung der EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie) beschlossen. Die NIS-Richtlinie, die im August 2016 in Kraft getreten ist, definiert Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der europäischen Union. Damit wurde ein einheitlicher Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cyber-Sicherheit, eine stärkere Zusammenarbeit der Mitgliedstaaten der Europäischen Union sowie Mindestsicherheitsanforderungen an und Meldepflichten für Kritische Infrastrukturen, sowie für bestimmte Dienste wie Cloud-Services und Online-Marktplätze geschaffen. Das BSI erhält vor diesem Hintergrund neue Aufgaben und Befugnisse – eine wichtige Voraussetzung, um die Cyber-Sicherheit in Deutschland weiter zu verbessern.

Gesetzesentwurf zur NIS-Richtlinie:

Mehr Aufgaben und Befugnisse für das BSI

Umsetzung bis Mai 2018 gefordert

Die NIS-Richtlinie ist ein wichtiger Schritt für mehr Cyber-Sicherheit in Europa. Die Bundesregierung hat nun die Grundlage dafür geschaffen, die europäischen Vorgaben rechtzeitig und zeitnah auch in nationales Recht umzusetzen. Dabei war die Ausgangsposition hierfür denkbar gut: In Deutschland existiert seit Juli 2015 mit dem IT-Sicherheitsgesetz bereits ein einheitlicher Rechtsrahmen für die Zusammenarbeit von Staat und Unternehmen für mehr Cyber-Sicherheit bei den Kritischen Infrastrukturen (KRITIS). Es schreibt KRITIS-Betreibern vor, IT-Sicherheit nach dem „Stand der Technik" umzusetzen und erhebliche IT-Sicherheitsvorfälle an das BSI zu melden. Der Gesetzesentwurf zur Umsetzung der NIS-Richtlinie erweitert nun die Aufsichts- und Durchsetzungsbefugnisse des BSI gegenüber KRITIS-Betreibern. Gleichzeitig wird die Zusammenarbeit zwischen den Bundesländern und dem BSI gestärkt. Das BSI hat so die Möglichkeit, Länder in Zukunft noch umfassender zu unterstützen und ihnen seine technische Expertise zur Verfügung zu stellen.

MEHR BEFUGNISSE FÜR DAS BSI

Trotz stärkerer Befugnisse wird sich das BSI dafür einsetzen, dass der im IT-Sicherheitsgesetz verankerte, mit dem UP KRITIS seit 10 Jahren gelebte kooperative Ansatz auch bei der Umsetzung der NIS-Richtlinie weiterverfolgt wird, da die Herausforderungen nur von Staat und Wirtschaft gemeinsam angenommen werden können. Damit wird das BSI seiner Vorreiterrolle in Europa auf dem Gebiet der Cyber-Sicherheit gerecht. Gleichzeitig ergänzt der Gesetzesentwurf das IT-Sicherheitsgesetz sinnvoll. Denn künftig sollen auch Anbieter von digitalen Diensten Mindestanforderungen und Meldepflichten unterliegen. Davon betroffen sind sowohl Online-Marktplätze und -Suchmaschinen als auch Anbieter von Cloud-Computing-Diensten. Das Bundesinnenministerium geht davon aus, dass hierzulande zwischen 500 und 1.500 Unternehmen von der Neuregelung betroffen sind. Das BSI wird künftig als Kontrollinstanz prüfen, ob sie die neuen Auflagen einhalten.

„Die neue NIS-Richtlinie ist ein wichtiger Schritt für mehr Cyber-Sicherheit in Deutschland. Denn mit dem Gesetzesentwurf wird der nächste Schritt nach dem IT-Sicherheitsgesetz unternommen, um einen höheren Schutz für Staat, Wirtschaft und Bevölkerung vor Cyber-Angriffen zu gewährleisten", kommentiert Arne Schönbohm, Präsident des BSI. „Der Gesetzesentwurf muss bis Mai 2018 in nationales Recht umgesetzt werden."

WIE DAS BSI UNTERNEHMEN UNTERSTÜTZT

Die mit dem Internet vernetzten Kritischen Infrastrukturen sind ein Ziel von Cyber-Angriffen. Neben den aus Sicht der Bevölkerung zu vermeidenden Versorgungsausfällen sind allein durch die Ausfallzeiten bei Attacken Schäden in Millionenhöhe nicht auszuschließen. Um Unternehmen künftig noch wirksamer zu unterstützen, richtet das BSI derzeit Mobile Incident Response Teams (MIRTs) ein. Diese Spezial-Taskforces bestehen aus Cyber-Sicherheitsexperten des BSI, die besonders schwerwiegende Cyber-Attacken auf Wunsch der Betreiber vor Ort untersuchen und bei deren Bewältigung helfen. Ein Beispiel wäre ein Cyber-Angriff, der wichtige IT-Steuerungen eines Kraftwerks lahmlegt. Aber auch eine Attacke auf eine Chemieanlage, bei der von einer großen Gefährdung der Bevölkerung auszugehen ist, könnte den Einsatz eines MIRT rechtfertigen. ■

CYBER-SICHERHEIT

GUT GERÜSTET FÜR NEUE BEDROHUNGSLAGEN

Cyber-Sicherheitsstrategie für Deutschland 2016

Die Bundesregierung hat im November 2016 die vom Bundesminister des Innern vorgelegte „Cyber-Sicherheitsstrategie für Deutschland 2016“ beschlossen. Sie bildet den ressortübergreifenden strategischen Rahmen für die Aktivitäten der Bundesregierung mit Bezügen zur Cyber-Sicherheit und schreibt die Cyber-Sicherheitsstrategie aus dem Jahr 2011 fort.

Fünf Jahre sind im Zeitalter der Digitalisierung eine sehr lange Zeit. Neue Möglichkeiten der Kommunikation und Interaktion wie durch die Sozialen Netze, neue Geschäftsfelder wie das Internet der Dinge, neue Felder für Forschung und Entwicklung wie selbstlernende Maschinen haben diese Jahre geprägt. Vernetzte elektronische Geräte bestimmen verstärkt den Lebens- und Arbeitsalltag der Menschen. Durch die zunehmende maschinelle Erzeugung von Daten sowie die zunehmende Verbreitung von intelligenten Sensoren entstehen riesige Datenmengen.

Auch die Gefährdungen der digitalen Gesellschaft durch Cyber-Angriffe haben sich in dieser Zeit verändert. Die Angreifer haben neue Geschäftsmodelle entdeckt und setzen diese immer schneller um, beispielsweise im Bereich der Erpressung mithilfe von Ransomware. Täglich kommen neue Varianten von Ransomware auf den Markt, mit denen Daten verschlüsselt und Lösegeld erpresst werden soll. Durch die Vernetzung von Geräten des Internets der Dinge, wie Smart-TVs, Netzwerk-Kameras oder Babyphones, entstehen schlagkräftige Botnetze, die zu DDoS-Angriffen mit Bandbreiten genutzt werden, die zuvor nur theoretisch denkbar waren.

Diese sich stetig ändernden Rahmenbedingungen machen es erforderlich, auch die Abwehrmaßnahmen zu aktualisieren, zu ergänzen und in einer neuen ressortübergreifenden Strategie zu bündeln. Die strategischen Ansätze und Ziele der Cyber-Sicherheitsstrategie 2011 haben dabei im Wesentlichen auch heute noch Bestand. Zahlreiche der darin vorgesehenen Maßnahmen sind seither umgesetzt worden. Als organisatorische Maßnahme wurde mit dem Cyber-Sicherheitsrat an der Schaltstelle von Politik und Wirtschaft ein hochrangiges Gremium für strategische Impulse und

VIER HANDLUNGSFELDER

SCHWERPUNKTE DER CYBER-SICHERHEITSPOLITIK SOLLEN IN DEN KOMMENDEN JAHREN DIE FOLGENDEN VIER HANDLUNGSFELDER SEIN:

- Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung wird gestärkt: Hier geht es darum, alle Anwender in die Lage zu versetzen, Chancen und Risiken beim Einsatz von Informationstechnik zu erfassen, zu bewerten und ihr Handeln daran auszurichten. Hierfür müssen die entsprechenden vertrauenswürdigen Technologien und Rahmenbedingungen vorliegen und kontinuierlich weiterentwickelt werden. So soll ein Basis-Zertifizierungsverfahren für sichere IT-Verbraucherprodukte eingeführt und dessen Kriterien durch das BSI festgelegt werden. Parallel dazu werden die bestehenden Ressourcen im BSI zur Erarbeitung von technischen Richtlinien, zur Zertifizierung und zur Unterstützung der nationalen Akkreditierungsstelle im Bereich der IT-Sicherheit weiter gestärkt.

- Die Kooperation zwischen Staat und Wirtschaft bei der Cyber-Sicherheit soll ausgeweitet werden: Eine vertrauensvolle Zusammenarbeit und ein enger Austausch zwischen Staat und Wirtschaft sind unabdingbar, um Cyber-Sicherheit in Deutschland dauerhaft auf einem hohen Niveau gewährleisten zu können. Dabei sind im Sinne eines kooperativen Ansatzes auch neue Wege zu beschreiten, um die jeweiligen Kompetenzen zu bündeln und zu nutzen. Eine Schlüsselrolle kommt dabei der Zusammenarbeit mit den Providern zu. Dies gilt vor dem Hintergrund aktueller Angriffe insbesondere für Maßnahmen der Provider, um Cyber-Bedrohungen zu erkennen, mit erkannten Vorfällen/Infektionen umzugehen und um die Wirkung laufender Angriffe abzuschwächen.

- Es wird eine leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur aufgebaut: Sie soll die verschiedenen Akteure auf Bundesebene wirksam verzahnen und daneben die Länder, Kommunen und die Wirtschaft im Blick behalten. Das Nationale Cyber-Abwehrzentrum bietet auf Bundesebene bereits die entsprechende Struktur, unter deren Dach die einzelnen Akteure im Rahmen ihrer jeweiligen Zuständigkeiten zusammenarbeiten. Es gilt, diese Zusammenarbeit zu intensivieren und die Länder künftig stärker einzubinden.

- Deutschland wird aktiv in der europäischen und internationalen Cyber-Sicherheitspolitik positioniert: Ein hohes Niveau an Cyber-Sicherheit ist angesichts der transnationalen Vernetzung in einer digitalisierten Welt nur durch Einbettung und Verstärkung der nationalen Maßnahmen in die entsprechenden europäischen, regionalen und internationalen Prozesse erreichbar. Deutschland wird sich hierfür auch weiterhin aktiv in die europäische und internationale Cyber-Sicherheitspolitik einbringen und vor allem EU-Pilotprojekte, bei denen die rechtlichen und technischen Fragen im Zusammenhang mit der grenzüberschreitenden Verarbeitung und Nutzung von Daten adressiert werden, aktiv vorantreiben.

Die „Cyber-Sicherheitsstrategie für Deutschland 2016“ sieht über 30 strategische Ziele und Maßnahmen zur Verbesserung der Cyber-Sicherheit in diesen vier Handlungsfeldern vor. Die dafür erforderlichen Cyber-Budgets sollen durch das jeweils zuständige Ressort, also das Innen-, Wirtschafts- und Verteidigungsministerium, festgelegt werden.

mit dem beim BSI angesiedelten Cyber-Abwehrzentrum eine Plattform für den strategischen und operativen Austausch zwischen den Behörden geschaffen.

Der wesentliche Leitgedanke der jetzt verabschiedeten Cyber-Sicherheitsstrategie 2016 ist es, die Handlungsfähigkeit und Souveränität Deutschlands auch im Zeitalter der Digitalisierung zu gewährleisten. Sie soll ermöglichen, dass Deutschland die enormen Chancen und Potenziale der Digitalisierung optimal nutzen kann. Doch eine zwingende Voraussetzung dafür ist, dass die Sicherheitsrisiken beherrschbar sind. Ziel der Strategie ist es daher, Cyber-Sicherheit in einem Maße herzustellen, das der Bedeutung und der Schutzwürdigkeit der vernetzen Informationsinfrastrukturen angemessen ist, ohne die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen.

SCHNELLE MOBILE REAKTION AUF ANGRIFFE

Besondere Bedeutung kommt der schnellen Hilfe vor Ort zu. Denn die Cyber-Angriffe der letzten Zeit haben gezeigt, dass es kaum institutionalisierte staatliche Strukturen gibt, die Betroffenen zeitnah vor Ort über die üblichen IT-Sicherheitsmaßnahmen hinaus bei der Aufbereitung eines Vorfalls oder der Abwehr eines laufenden Angriffs helfen können. Hierbei geht es zum einen um die technische Bewältigung von Sicherheitsvorfällen, zum anderen um die Tätigkeit der Sicherheitsbehörden vor Ort auf Basis der jeweiligen gesetzlichen Grundlage.

Diese Lücke soll bei allen mit der Cyberabwehr befassten behördlichen Einrichtungen schnell geschlossen werden, und zwar durch eine Art „mobile Einsatztruppe“. Die notwendige Koordination bei solchen Einsätzen verschiedener Behörden erfolgt unter Wahrung der rechtlichen Grenzen im Nationalen Cyber-Abwehrzentrum.

- Im BSI werden „Mobile Incident Response Teams“ (MIRTs) eingerichtet, die Cyber-Vorfälle in den für das Gemeinwesen besonders bedeutenden Einrichtungen analysieren und bereinigen sollen. Die 2017 einsatzbereiten MIRTs des BSI werden in der Lage sein, auf Ersuchen und mit Einwilligung von Verfassungsorganen, Bundesbehörden sowie Betreibern Kritischer Infrastrukturen und vergleichbar wichtigen Einrichtungen vor Ort schnell, flexibel und adressatengerecht bei der technischen Bewältigung von Sicherheitsvorfällen zu unterstützen, wenn hieran ein besonderes öffentliches Interesse besteht. Ein Angriff wie beispielweise 2015 auf den Deutschen Bundestag könnte so noch effizienter verfolgt und abgemildert werden. Ziel dieser Unterstützung ist es, den sicheren technischen Betrieb der betroffenen Einrichtung schnell wiederherzustellen.
- Im Bundeskriminalamt (BKA) soll dafür eine spezialisierte Ermittlungseinheit eingerichtet werden, die in Absprache mit der zuständigen Staatsanwaltschaft oder Bundesanwaltschaft die ersten unaufschiebbaren strafprozessualen Maßnahmen für die Strafverfolgungsbehörden umsetzt. Sie ist eine jeweils aus vier Cybercrime-Experten des BKA bestehende, rotierende 24/7-Rufbereitschaft, um notwendige polizeiliche Sofortmaßnahmen außerhalb der Regelarbeitszeit einzuleiten.
- Im Bundesamt für Verfassungsschutz (BfV) werden „Mobile Cyber-Teams“ aufgebaut, bestehend aus IT-Spezialisten, nachrichtendienstlichen Fachleuten mit Erfahrung in der Auswertung von Cyber-Angriffen und – bei Bedarf – fremdsprachigen Mitarbeitern. Bei einem Cyber-Angriff mit nachrichtendienstlichem oder extremistischem oder terroristischem Hintergrund kommen diese Cyber-Teams vor Ort zum Einsatz. Das betrifft auch mögliche Sabotageangriffe. Der Bundesnachrichtendienst (BND) kann einen Angriff sowohl in der Vorbereitungs- als auch in der Durchführungsphase beobachten.
- Im Verteidigungsbereich übernimmt diese Aufgabe der Militärische Abschirmdienst (MAD). Zusätzlich werden aus den Angriffen resultierende Informationsabflüsse registriert. Auch die Bundeswehr kann mit ihren Organisationselementen (u. a. Incident Response Teams) Beiträge zur gesamtstaatlichen Sicherheitsvorsorge leisten.

STRATEGISCHE BEGLEITUNG

Eine zukunftsoffene Cyber-Sicherheitsstrategie darf sich nicht allein auf die Festlegung strategischer Maßnahmen beschränken. Denn die Dynamik der Digitalisierung ist nur durch einen ständigen Strategieprozess zu Fragen der Cyber-Sicherheit beherrschbar, aus dem sich weitere strategische Maßnahmen entwickeln können. Neue Gefahren müssen frühzeitig erkannt und innovative Lösungen erforscht und erarbeitet werden. Eine maßgebliche Rolle soll hierbei dem mit der Cyber-Sicherheitsstrategie 2011 eingerichteten Nationalen Cyber-Sicherheitsrat als strategischem Ratgeber der Bundesregierung zukommen. Seine Rolle wird gestärkt. Hier sollen langfristige Handlungsnotwendigkeiten und Trends identifiziert und hieraus Impulse zur Stärkung der Cyber-Sicherheit in den vier Handlungsfeldern abgeleitet werden. Dabei wird der Nationale Cyber-Sicherheitsrat in Zukunft verstärkt auch auf das Expertenwissen aus Gesellschaft, Wirtschaft und Wissenschaft zurückgreifen. ■

Drei Fragen an Bundesinnenminister Dr. Thomas de Maizière

Warum musste die Cyber-Sicherheitsstrategie 2011 fortgeschrieben werden?

Die strategischen Ansätze und Ziele der Cyber-Sicherheitsstrategie von 2011 haben im Wesentlichen auch heute noch Bestand. Angesichts der technischen Entwicklung und weltweit wachsenden Bedeutung der Digitalisierung in den letzten fünf Jahren war es allerdings geboten, die Strategie im letzten Jahr fortzuschreiben. Sie bildet den Überbau für sämtliche Aktivitäten der Bundesregierung zur Verbesserung der Cyber-Sicherheit in Deutschland. Dabei wollen wir die Balance zwischen Freiheit und Sicherheit auch in der digitalen Welt bewahren.

Kann die Strategie schon Antworten geben auf geänderte Intentionen von Cyber-Attacken?

Mit „neuen Intentionen“ sprechen Sie die Cyber-Attacken an, die mit dem Ziel erfolgen, Einfluss auf die freie Meinungsbildung zu nehmen. Solchen Attacken können auch Angriffe auf die Informationstechnik von Regierung, Parlament oder Medienhäusern vorausgehen. Diese können langfristig Gefahren für die freiheitliche Gesellschaft und die Demokratie darstellen. Hier gilt es, zu sensibilisieren, aufzudecken und aufzuklären.

Welche Rolle nimmt das Bundesinnenministerium bei der Umsetzung der Strategie ein?

Das Bundesinnenministerium koordiniert die Umsetzung der Cyber-Sicherheitsstrategie. Herr Staatssekretär Vitt in seiner Funktion als Beauftragter der Bundesregierung für Informationstechnik zeichnet hierfür verantwortlich. Zusätzlich ist er der Vorsitzende des Nationalen Cyber-Sicherheitsrates. Dem Cyber-Sicherheitsrat kommt bei der Umsetzung eine maßgebliche Rolle zu. Hier sollen langfristige Handlungsnotwendigkeiten und Trends identifiziert und Impulse zur Stärkung der Cyber-Sicherheit abgeleitet werden. Dadurch wird die Rolle des Cyber-Sicherheitsrates als strategischer Ratgeber der Bundesregierung gestärkt. Das BSI ist bei allen Fragen der Cyber-Sicherheit unsere Schlüsselbehörde.

Weitere Informationen: https://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyber-Sicherheitsstrategie/cyber-sicherheitsstrategie_node.htlm

VERTRAUENSVOLLE ZUSAMMENARBEIT

Fünf Jahre Allianz für Cyber-Sicherheit

Cyber-Angriffe können nur durch enge Kooperation und kontinuierliche Kommunikation bei der Gefahrenabwehr erfolgreich verhindert werden. Doch das setzt Vertrauen bei allen Beteiligten voraus. Die Allianz zeigt, wie dies praktisch funktionieren kann.

Die Allianz für Cyber-Sicherheit wurde gegründet als Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom). Sie suchten nach einem Weg, möglichst viele Unternehmen und Institutionen freiwillig für ein Thema zu interessieren und zu engagieren, das völlig zu Unrecht ein Schattendasein fristete: die gemeinsame Cyber-Abwehr. 2012 initiiert, gehören der Allianz mittlerweile 2045 Institutionen an, davon 101 Partnerunternehmen und 45 Multiplikatoren.

Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz das Ziel, die Widerstandsfähigkeit des Standortes gegenüber Cyber-Angriffen zu stärken, die IT-Sicherheitskompetenz in deutschen Organisationen auszubauen, aktuelle und valide Informationen zu Gefährdungen im Cyber-Raum bereitzustellen und eine einheitliche Lagebeurteilung voranzutreiben. Die Initiative unterstützt zudem den Informations- und Erfahrungsaustausch zwischen den Teilnehmern. „Die Geschichte der Allianz ist eine Erfolgsgeschichte“, ist sich BSI-Präsident Arne Schönbohm sicher. „Und sie zeigt beispielhaft, wie IT-Sicherheit in Deutschland erfolgreich organisiert und umgesetzt wird.“

Die Basis ist Vertrauen: Die Allianz bietet als Plattform Unternehmen, Behörden, Forschung und Wissenschaft sowie anderen Institutionen ein breites Informationsangebot zu verschiedensten Themen der Cyber-Sicherheit.

Registrierte Teilnehmer der Allianz erhalten Zugriff auf ein erweitertes Informationsangebot, insbesondere zur Cyber-Sicherheitslage durch monatliche Lageberichte, Warnmeldungen sowie weitergehende Hintergrundinformationen. Aufgrund der teilweise vertraulichen Natur dieser Informationen muss die Weitergabe dieser Inhalte restriktiv gehandhabt werden und unterliegt Beschränkungen nach dem Traffic Light Protocol (TLP).

Vertrauen fördert den offenen Austausch von Erfahrungen. In Erfahrungskreisen (ERFA) werden in der Allianz ausgesuchte Sicherheitsthemen in regelmäßigen Workshops oder Schulungen für die Teilnehmer abgehandelt. Expertenkreise der Sicherheitsspezialisten aus Wirtschaft, Forschung und Behörden diskutieren Probleme und schlagen Lösungen vor, von denen die Teilnehmer profitieren. Partner und Multiplikatoren tauschen ihre Erfahrungen bei den Partnertagen während der CeBIT und der IT-Sicherheitsmesse it-sa aus. Vierteljährlich finden die Cyber-Sicherheitstage statt, an denen auch Nichtmitglieder teilnehmen können. „Indem jeder Teilnehmer vom Wissen und den Erfahrungen der anderen profitiert, trägt die Allianz das Thema Cyber-Sicherheit in die Breite“, freut sich BSI-Präsident Schönbohm.

Denn aus Austausch erwächst Wissen: die Wissensdatenbank der Allianz. Ihre zentralen Komponenten sind der monatliche erscheinende Bericht zur IT-Sicherheitslage und die verschiedenen Themenlagebilder. Sie stehen den Mitgliedern der Allianz zur Verfügung. In Abhängigkeit vom Thema sind die Informationen im öffentlichen, nichtöffentlichen und vertraulichen Bereich zugänglich. Darüber enthält die Datenbank diverse themenbezogene Unterlagen wie z. B. Studien, Umfragen, Tutorials, Leitfäden, Warnungen und eine Mediathek. Noch in einer weiteren Form hat die Allianz dazu beigetragen, Vertrauen aufzubauen. Die Meldestelle im Rahmen des Internetportals der Allianz hat sich als wichtige Quelle erwiesen, um Erkenntnisse aus Cyber-Angriffen in das Lagebild des BSI einfließen zu lassen. Opfer von Angriffen können Vorfälle in ihren Organisationen hier melden. Die Meldung erfolgt über ein Onlineformular, bei Bedarf auch anonym. Die Meldungen werden statistisch und fachlich ausgewertet und für die Erstellung des aktuellen Lagebildes verwendet. „Dies hat sich gewissermaßen wie eine Blaupause für die Erkenntnisse erwiesen, die aus der Meldepflicht des IT-Sicherheitsgesetzes erwachsen können“, meint Schönbohm. Denn der Cyberschutz wird umso stärker, wenn nicht nur das Wissen des BSI, sondern auch möglichst viel Know-how anderer Institutionen in die Abwehrstrategie einfließt und die Inhalte auf vielen unterschiedlichen Erfahrungswerten basieren.

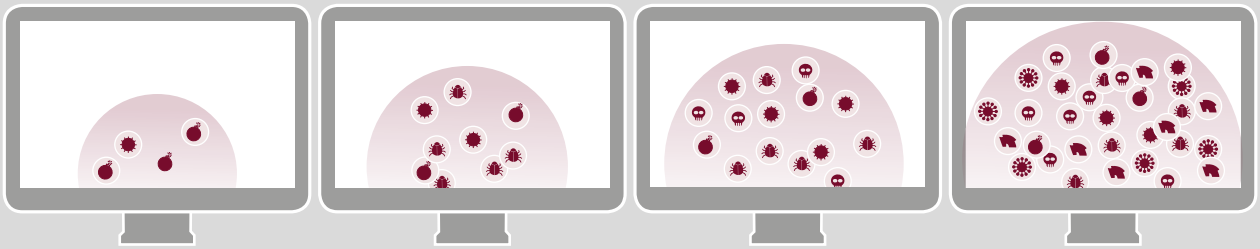
Die intensive und offene Kooperation und Kommunikation in der Allianz zeigt aber auch, dass Deutschland in der Organisation der Cyberabwehr den richtigen Weg eingeschlagen hat: „Indem präventive und nachrichtendienstliche Aufgaben nicht in ein- und derselben Behörde wahrgenommen werden, waren überhaupt erst die Voraussetzungen für eine vertrauensvolle Zusammenarbeit gegeben“, meint Präsident Arne Schönbohm. Der Erfolg der Allianz in den letzten fünf Jahren gibt ihm Recht. ■

Allianz für Cyber-Sicherheit

Weitere Informationen: https://www.allianz-fuer-cybersicherheit.de

Digitalisierung und Vernetzung gefährden IT-Sicherheit

JÄHRLICHER ANSTIEG BEKANNTER SCHADPROGRAMMVARIANTEN

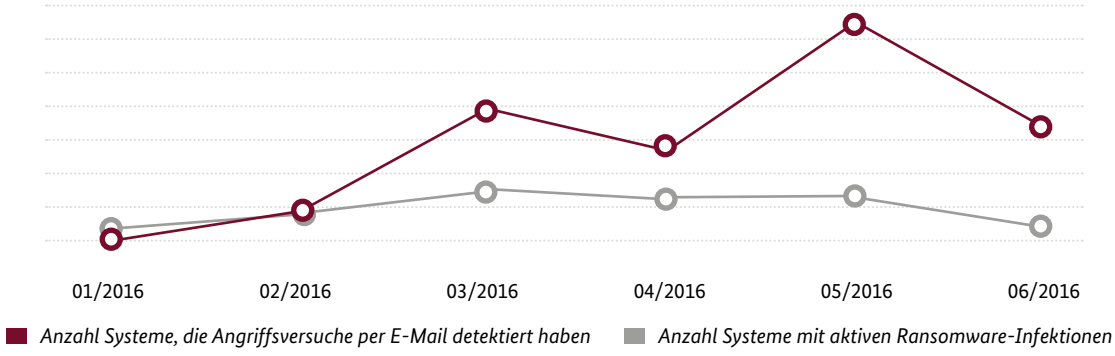


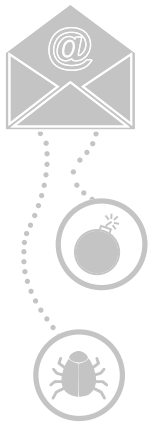
182,9 Mio.	326,0 Mio.	470,0 Mio	597,5 Mio
2013	2014	2015	2016

Quelle: AV-Test

RANSOMWARE-ANGRIFFE: ANSTIEG SEIT 2016

Nutzer sollten weiterhin aufmerksam bei unbekannten und zweifelhaften Mails sein.





SPAM-MAILS MIT SCHADPROGRAMM-ANHÄNGEN LEGEN WEITER ZU

Im ersten Halbjahr 2016 nahm die gesamte Spamaktivität im Vergleich zum Vorjahr um **73%** zu. Im Bereich des klassischen Spams aber nur eine Zunahme von **16%**.

Schadsoftware, die per Spam-Mails verbreitet wird, hat hingegen um **1.270%** extrem zugelegt.

Immer mehr Varianten verbreiten sich in kurzer Zeit und setzen so die klassischen Abwehrmaßnahmen außer Kraft: 2016 wurden täglich rund

380.000

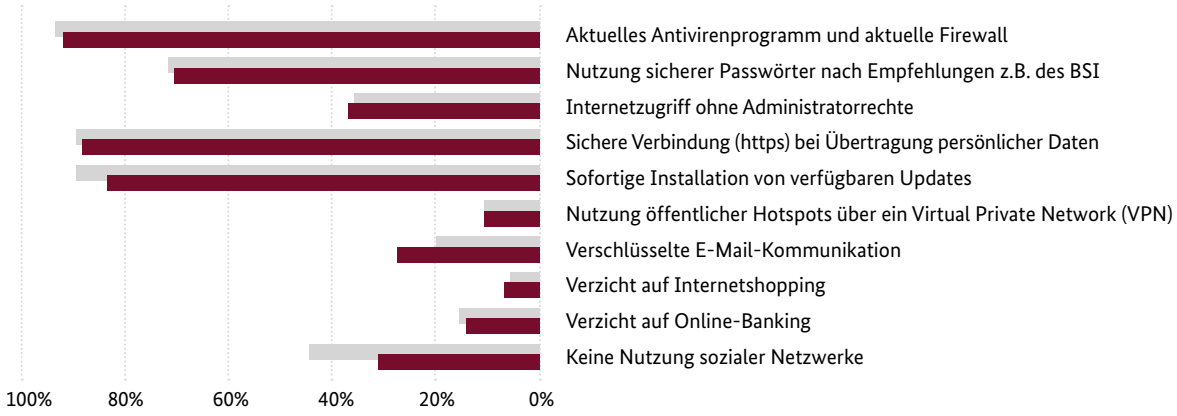
neue Schadprogrammvarianten entdeckt.

Weitere Informationen: https://www.bsi.bund.de/Lageberichte

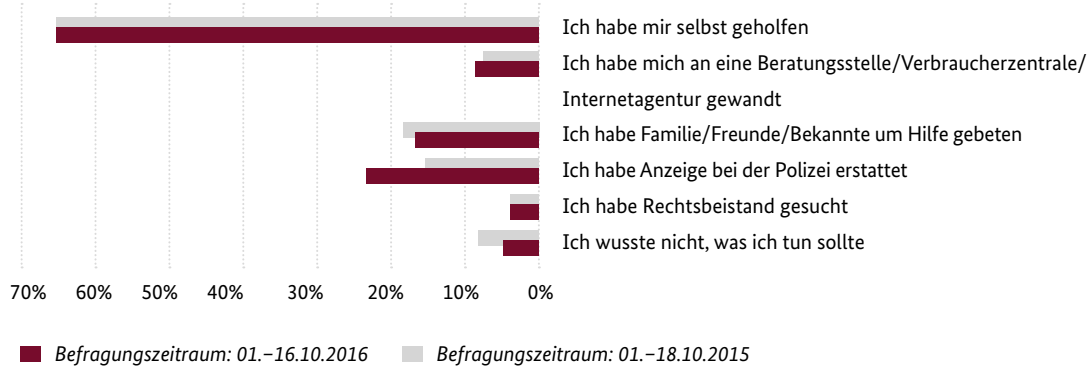
Quelle: Bericht zur Lage der IT-Sicherheit in Deutschland 2016 (BSI).

Kompetenz im Umgang mit Cyber-Kriminalität steigt

MÖGLICHST WENIG AUFWAND: NUTZER GREIFEN AUF GÄNGIGE SCHUTZMASSNAHMEN ZURÜCK[1)]



OPFER VON CYBER-KRIMINALITÄT ZEIGEN STRAFTATEN EHER BEI DER POLIZEI AN[1)]



IN VERDÄCHTIGEN SITUATIONEN REAGIEREN INTERNETNUTZER, INDEM SIE...[2)]

... die betreffende Internetseite verlassen oder E-Mail löschen **(83,4%)**
... sich an den Seitenbetreiber wenden **(12,9%)**
... sich an die Internetbeschwerdestelle wenden **(8,5%)**
... sich an die Polizei wenden **(26,9%)**

Nur **3,1%** der Internetnutzer reagieren in verdächtigen Situationen gar nicht.

[1)] Quelle Zahlen 2015: https://www.bsi.bund.de/dok/7023566, Zahlen 2016: https://www.bsi.bund.de/dok/8558402
[2)] Quelle: BSI/ProPK, Online-Umfrage 2015 und 2016 anlässlich des Europäischen Monats der Cyber-Sicherheit (ECSM).

Optimieren durch Teilen

Die DCSO als Cyber-Sicherheits-Kompetenzzentrum

Die DCSO (Deutsche Cyber-Sicherheitsorganisation GmbH) ist Cyber-Security-Kompetenzzentrum und Dienstleister für große Unternehmen der deutschen Wirtschaft. Die Organisation wurde Ende 2015 als herstellerunabhängiger Managed Security Service Provider von der Allianz SE, BASF SE, Bayer AG und der Volkswagen AG gegründet.

Die DCSO unterstützt Unternehmen darin, sich sowie ihre Lieferketten vor kriminellen Hackern, Wirtschaftsspionage, ausländischen Geheimdiensten und Sabotage zu schützen – und damit den Standort Deutschland in der vernetzten Weltwirtschaft zu stärken.

Angreifer sind heute hochprofessionell in ihrer Arbeitsweise und entlang der Kill Chain exzellent organisiert. Auf Unternehmensseite hingegen gibt es oftmals keine oder nur begrenzte Kooperation untereinander. Angreifer müssen lediglich eine Schwachstelle finden, während Unternehmen gezwungen sind, sich gegen alle potenziellen Angriffsvektoren zu schützen. Zielgerichtete Attacken bleiben so über Wochen, Monate, gar über Jahre unentdeckt. Dieses starke Ungleichgewicht führt zu strategischen Nachteilen der Wirtschaft.

Die DCSO verfolgt das Prinzip „Optimieren durch Teilen“: Operative Erkenntnisse über Cybergefahren und ihre Bekämpfung werden von Kunden an die DCSO zurückgespielt und danach in anonymisierter Form automatisch an alle anderen Teilnehmer verteilt. Diese selbstverstärkende Rückkopplung führt zu mehr Sicherheit bei allen Unternehmen.

Mittels einer gemeinsamen Threat-Intelligence-Plattform und einer eigenen Netzwerksensorik hilft die DCSO ihren Kunden, Angriffe deutlich schneller zu erkennen. Ein Team aus Incident-Response-Experten erarbeitet gemeinsam mit betroffenen Konzernen effektive Strategien gegen erfolgte Angriffe. Zudem stärkt die DCSO die Abwehrkraft der Unternehmen durch einen Technologieevaluierungs-Service und eine GRC-Plattform (Governance, Risk Management and Compliance), die die Sicherheitsüberprüfung der Lieferkette unterstützt.

Als von deutschen Konzernen getragenes Unternehmen agiert die DCSO vollkommen herstellerunabhängig und ist allein ihren Mitgliedern und Kunden verpflichtet. Die Ausrichtung der DCSO wird von einem Fachbeirat gesteuert, in dem große Kunden, Forschungsinstitute und Behörden vertreten sind. Gewinne werden vollständig in Forschung und Entwicklung reinvestiert.

Das Bundesministerium des Innern und das Bundesamt für Sicherheit in der Informationstechnik sind wichtige Partner der Wirtschaft. Deshalb hat die DCSO diese in ihr Kompetenzzentrum und den Informationsaustausch von Beginn an mit einbezogen. ■

Kurzprofil Martin Wülfert

Martin Wülfert leitet seit Mai 2016 die Deutsche Cyber-Sicherheitsorganisation GmbH (DCSO) mit Sitz in Berlin. Der Diplom-Physiker und Betriebswirt verantwortet die geschäftliche Entwicklung der im November 2015 gegründeten Organisation. Dazu gehören unter anderem der Ausbau des Portfolios, das Marketing sowie die Gewinnung von Fachbeiratsmitgliedern.

Weitere Informationen: https://dcso.de/de/

Das IT-Sicherheitsgesetz

GESETZ ZUR ERHÖHUNG DER SICHERHEIT INFORMATIONSTECHNISCHER SYSTEME (IT-SIG)

- Am 25.7.2015 in Kraft getreten
- Verpflichtet Betreiber Kritischer Infrastrukturen, die Informationstechnik ihrer kritischen Anlagen nach dem Stand der Technik abzusichern
- Alle zwei Jahre Nachweispflicht über IT-Sicherheit
- Erhebliche IT-Störungen müssen an das BSI gemeldet werden

WAS SIND KRITISCHE INFRASTRUKTUREN?

- Organisationen und Einrichtungen, die grundlegende Versorgungsdienstleistungen anbieten (z.B. Strom, Trinkwasser, Nahrung)
- Einrichtungen, deren Ausfall oder Beeinträchtigung dramatische Folgen für Staat, Wirtschaft und Gesellschaft in Deutschland hätte

1. TEIL BSI-KritisV SEIT 3. MAI 2016 IN KRAFT

- Betroffene Sektoren: Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung
- Spätestens sechs Monate nach Inkrafttreten der Verordnung müssen eine Kontaktstelle beim BSI benannt und erhebliche IT-Störungen an das BSI gemeldet werden (bis 3. November 2016)
- Zwei Jahre Zeit nach Inkrafttreten der Verordnung, den Stand der Technik in IT-Sicherheit umzusetzen und dem BSI nachzuweisen (bis 3. Mai 2018)

ÄNDERUNGSVERORDNUNG AB FRÜHJAHR 2017

- Betroffene Sektoren: Finanz- und Versicherungswesen, Transport und Verkehr sowie Gesundheit
- Spätestens sechs Monate nach Inkrafttreten der Verordnung müssen eine Kontaktstelle beim BSI benannt und erhebliche IT-Störungen an das BSI gemeldet werden (bis Herbst 2017)
- Zwei Jahre Zeit nach Inkrafttreten der Verordnung, den Stand der Technik in IT-Sicherheit umzusetzen und dem BSI nachzuweisen (bis Frühjahr 2019)

Bundesamt für Sicherheit in der Informationstechnik

DAS BSI ...

- bewertet und analysiert die eingehenden Meldungen
- setzt diese in Beziehung zu anderen Meldungen und Erkenntnissen
- erstellt daraus ein Lagebild
- versendet Warn- und Alarmierungsmeldungen inklusive Handlungsempfehlungen an die Betreiber Kritischer Infrastrukturen

POSITIVE BILANZ

- Mehr als **85 %** der erwarteten Betreiber haben eine Kontaktstelle beim BSI benannt und werden mit aktuellen Lageinformationen versorgt
- **50 %** der unter die BSI-KritisV fallenden Energieversorger und TK-Anbieter haben sich freiwillig registriert
- Seit 2007 ist die Anzahl an Organisationen im UP KRITIS von 40 auf über **430** angewachsen

UP KRITIS PROFIL & ZIELE

- Öffentlich-private Partnerschaft
- Betreiber Kritischer Infrastrukturen, Verbände und zuständige Behörden
- Erhöhung der Resilienz der Kritischen Infrastrukturen
- Möglichst uneingeschränkte Sicherstellung der Versorgungssicherheit
- Umsetzung des IT-Sicherheitsgesetzes

Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen.

DAS BSI

Neuer BSI-Vizepräsident stellt sich vor

Interview mit Dr. Gerhard Schabhüser

Herr Dr. Schabhüser, Sie haben vor Kurzem den Posten des Vizepräsidenten übernommen. Wo kommen Sie her und wie war Ihr bisheriger Karriereverlauf?

Ich bin gebürtiger Westfale und kam 1961 im Münsterland zur Welt. Mein Studium beendete ich als Diplom-Mathematiker und promovierte anschließend in diesem Bereich. Meine erste berufliche Stelle war bereits beim BSI, das im gleichen Jahr 1991 gegründet wurde und aus der Zentralstelle für Sicherheit in der Informationstechnik, ZSI, hervorging.

Beim BSI war ich anfangs für die Bewertung kryptografischer Verfahren zuständig. Nach ein paar Jahren wechselte ich zum Design, also zur Entwicklung von Verschlüsselungsverfahren.
In dieser Phase habe ich sehr viele BSI-Projekte zur Bereitstellung von Kryptosystemen für den Verschlusssachenbereich unterstützt. Nach zirka zehn Jahren übernahm ich die Referatsleitung für die Entwicklung kryptografischer Verfahren. Anschließend wurde ich Fachbereichsleiter für Kryptografie und wissenschaftliche Grundlagen sowie Abteilungsleiter für die Themenfelder Kryptografie, wissenschaftliche Koordinierung und technische Verschlusssachensicherheit. Seit 1. Januar bin ich nun Vizepräsident des BSI.

Welche Aufgaben haben Sie als Vizepräsident?

Die Schwerpunkte für mein neues Amt lassen sich in drei Blöcke gliedern. Der erste beschreibt meine Aufgabe als BSI-Innenpolitiker. Dieser Bereich umfasst die Umsetzung der Strategie nach innen, die Ausgestaltung von Prozessen sowie die Anpassung der Strukturen des BSI an die gewachsene Größe und an das Anforderungsprofil, das von außen kommt.

Der zweite Block ist meine Rolle als Präsidentenberater. Hier unterstütze ich den Präsidenten bei der Positionierung des BSI, der Strategieentwicklung, der Technologiebewertung als auch dem Abgleich politischer Vorgaben mit den technologischen Umsetzungsmöglichkeiten.

Der dritte Punkt besteht in der Lastenverteilung der Außendarstellung. Dazu zählt die Vertretung des Präsidenten bei externen Terminen und der Präsentation des BSI.

Welche Themen stehen dabei im Vordergrund?

Bei allen drei Aufgabenblöcken gibt es sehr viel zu tun. Im Bereich Innenpolitik steht das starke Wachstum des BSI im Vordergrund. Wir haben für das Jahr 2017 rund 180 zusätzliche Stellen genehmigt bekommen und wachsen damit auf über 800 Mitarbeiter. Die neuen Kollegen müssen gewonnen, eingearbeitet und integriert werden. Damit sind auch die internen Prozesse und Arbeitsweisen an das Wachstum anzupassen. Dies wird begleitet durch einen erheblichen Zuwachs an Aufgaben bei gleichzeitiger Verringerung der Reaktionszeiten aufgrund der steigenden Bedrohungslage.

Die anderen beiden Bereiche stellen dagegen eher laufende Prozesse dar, die sich aus dem Tagesgeschäft ergeben.

Welche Ziele verfolgen Sie dabei?

Wir möchten das BSI bestmöglich für die neuen Gegebenheiten aufstellen. Dazu gehört zum Beispiel die Anpassung der Produkte und Dienstleistungen an die zunehmende Größe des BSI sowie die zusätzlichen Aufgaben und Zielgruppen. Wir waren ursprünglich für die IT-Sicherheit im staatlichen

„Die zunehmende Digitalisierung erfordert eine immer stärkere präventive IT-Sicherheit.“

Kurzprofil Dr. Gerhard Schabhüser

Dr. Gerhard Schabhüser ist seit dem 1. Januar 2017 neuer Vizepräsident des BSI. Er hat damit die Nachfolge von Andreas Könen angetreten, der nun Leiter der Stabsstelle „IT- und Cybersicherheit; sichere Informationstechnik“ im Bundesinnenministerium ist. Der gelernte Diplom-Mathematiker Schabhüser ist bereits seit dem Gründungsjahr 1991 im BSI beschäftigt. Wir sprachen mit ihm über seinen Hintergrund, seine Erfahrungen sowie seine Aufgaben und Ziele in der neuen Position.

Bereich und primär für die Bundesverwaltung zuständig. Selbst hier erweitert sich unser Tätigkeitsbereich durch die zunehmende Nutzung von IT-Technologien in immer mehr Prozessen.

Inzwischen sind wir auch für die Ausgestaltung der Sicherheit Kritischer Infrastrukturen zuständig, die eine viel größere Anzahl von Kunden aus neuen Bereichen nach sich zieht. In Zukunft werden wir auch die Ebenen Länder und Kommunen stärker adressieren, sodass wir bei unseren Dienstleistungen und Produkten zum Schutz von Informationen – inklusive Prävention, Detektion und Reaktion – einen deutlich höheren Skalierungsgrad benötigen. Auch wenn das BSI wächst, werden wir sicher nicht alles selbst machen können. Daher brauchen wir Multiplikatoren, Dienstleister und Hersteller, die wir entsprechend qualifizieren und beauftragen, um Lösungen für Staat, Wirtschaft und Gesellschaft anzubieten.

Welche Trends erwarten Sie für die Zukunft?

Die zunehmende Digitalisierung erfordert eine immer stärkere präventive IT-Sicherheit. Dabei wollen wir als BSI sehr schnell und flexibel auf überraschende neue Anforderungen reagieren. Im Bereich Staat ist dies zum Beispiel die IT-relevante Absicherung von Wahlen. Gerade in diesem Jahr können mit der Bundestagswahl neuartige Herausforderungen auf uns zukommen.

Bei der Zielgruppe Wirtschaft steht vor allem im Zuge des IT-Sicherheitsgesetzes auch das Internet der Dinge mit Industrie 4.0 im Fokus. In Zukunft werden hier weitere Entwicklungen wie das autonome Fahren in vernetzten Autos oder große Digitalisierungsprojekte in Städten eine wichtige Rolle für uns spielen.

Auch für die Gesellschaft wollen wir IT-Sicherheit als wichtiges Kriterium adressieren und mitgestalten. Dazu bauen wir unser Informationsangebot für die Bürgerinnen und Bürger und den Dialog mit Organisationen der Zivilgesellschaft deutlich aus. ■

CYBER-SICHERHEIT AKTIV GESTALTEN

DAS BSI ALS PARTNER FÜR DIE WIRTSCHAFT

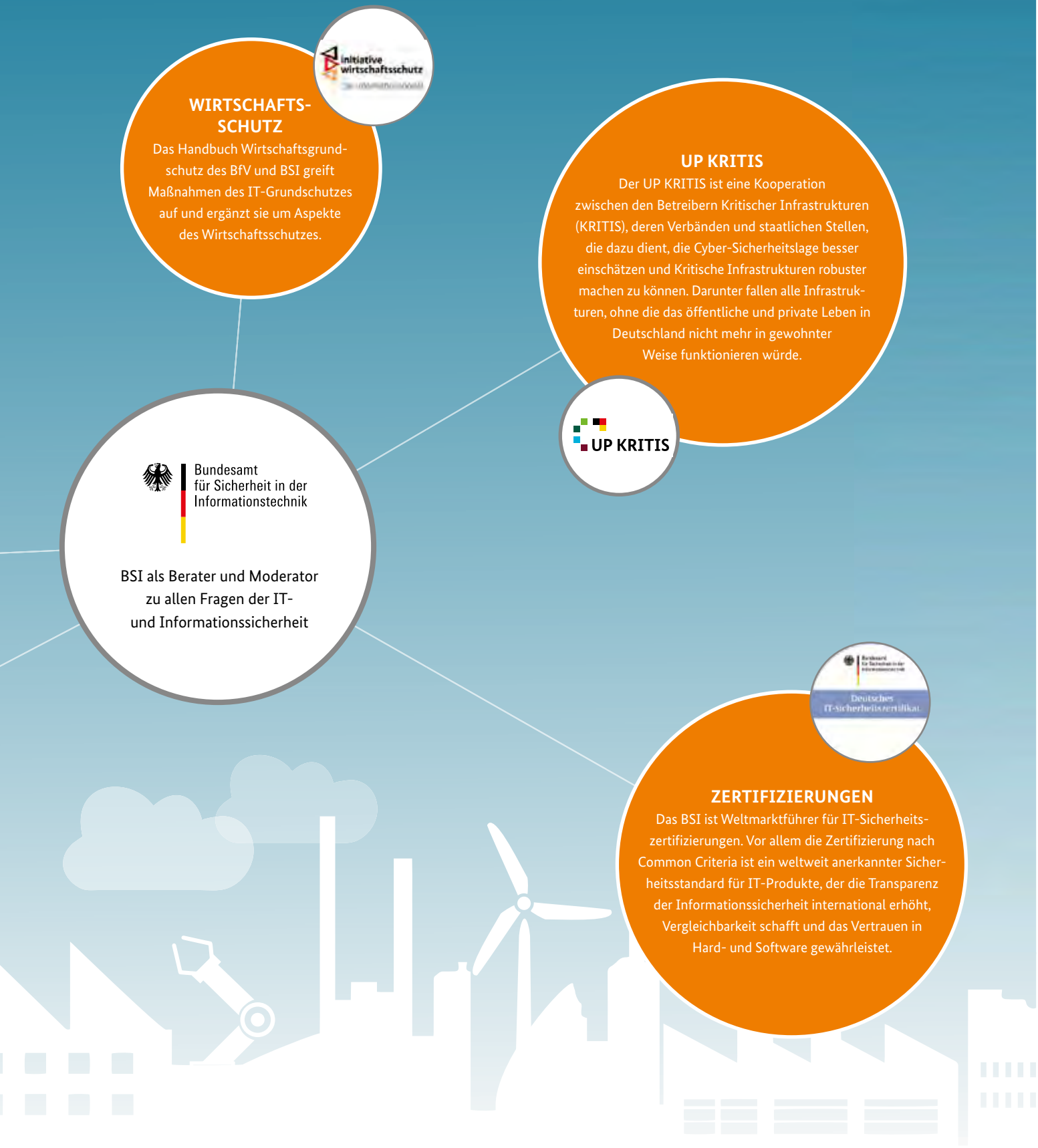
ALLIANZ FÜR CYBER-SICHERHEIT (ACS)

In Zusammenarbeit mit dem Bitkom hat das BSI 2012 die Allianz für Cyber-Sicherheit gegründet. Die größte nationale Kooperationsplattform zum Thema Cyber-Sicherheit bietet rund 2.000 Teilnehmern, 100 Partnern und 45 Multiplikatoren umfangreiche Informationen zur Prävention und Reaktion bei Cyber-Angriffen. Im Fokus steht dabei die Anwendbarkeit der Maßnahmen für den Mittelstand. Teilnehmer profitieren auf Cyber-Sicherheitstagen oder in regelmäßigen Arbeitsgruppen vom offenen Austausch untereinander.

IT-GRUNDSCHUTZ

Mit dem IT-Grundschutz bietet das BSI den meistgenutzten Standard für Informationssicherheit in Deutschland – eine Sammlung grundlegender Maßnahmen und Schutzprogramme zur Prävention und Abwehr von Cyber-Angriffen, die derzeit modernisiert wird.

Deutsche Unternehmen zeichnen sich durch hochwertige, innovative Erzeugnisse aus – und sind daher ein attraktives Ziel von Cyber-Angriffen. Nahezu jede Wirtschaftsbranche und jedes Unternehmen ist betroffen – selten werden Angriffe bemerkt. Gegen diese Gefahr für den Wirtschaftsstandort Deutschland müssen Staat und Unternehmen



ihre Kräfte bündeln. Das BSI als nationale Cyber-Sicherheits-behörde gestaltet als neutrale Stelle Informationssicher-heit in der Digitalisierung durch Prävention, Detektion und Reaktion für die Wirtschaft. Dabei bietet es eine Reihe von Informations- und Kooperationsmöglichkeiten an, um die Cyber-Sicherheit deutscher Unternehmen zu stärken. ■

IT-Sicherheit kennt keine Grenzen

Interview mit Bernd Kowalski

Digitalisierung betrifft alle Bereiche des Lebens, ob Gesellschaft, Wirtschaft oder Politik. Die neuen digitalen Technologien, Produkte und Verfahren werfen dabei wichtige Fragen auf – vor allem bei der IT-Sicherheit. Besonders sichtbar wird die Herausforderung in Bereichen wie IT-Infrastrukturen im Gesundheitswesen, der Energiewirtschaft oder im Automobilsektor beim autonomen Fahren. Bernd Kowalski, Abteilungspräsident Digitalisierung, Zertifizierung und Standardisierung beim BSI, erläutert die hohe Bedeutung von Zertifizierungen für die IT-Sicherheit in der Digitalisierung.

Warum sind Zertifizierungen so wichtig für eine erfolgreiche Digitalisierung?

Mit dem Einzug neuer Technologien, die durch die Dynamik des Marktes getrieben werden, gehen auch immer neue Sicherheitsrisiken einher. Diese Technologien müssen daher bereits vor der Markteinführung sicher gestaltet werden. Geschieht das nicht, kann dieses Defizit später kaum noch beseitigt werden. Geeignete technische Sicherheitsstandards und die Überprüfung mittels Zertifizierung stellen sicher, dass die mit einer neuen Technologie einhergehenden Sicherheitsrisiken schon vor der Markteinführung minimiert worden sind. Denn für die Zertifizierung stellen Unternehmen ihre Produkte dem BSI frühzeitig vor und bringen sie dann nach erfolgter Zertifizierung sicher auf den Markt. Das BSI erteilt IT-Sicherheitszertifikate für eine Vielzahl unterschiedlichster Hard- und Softwareprodukte (z.B. für Smart Meter, Netzkonnektoren im eHealth-Bereich oder auch für hoheitliche Dokumente). Darüber hinaus stellen wir auch Zertifikate nach Technischen BSI-Richtlinien oder nach den Anforderungen des IT-Grundschutzes aus.

Offensichtlich nutzen nicht alle Unternehmen die Möglichkeit der Zertifizierung. Woran könnte das Ihrer Meinung nach liegen?

Eine Zertifizierung ist immer mit einem gewissen Aufwand an Zeit und Kosten verbunden. Sichere, zertifizierte Produkte sind daher in der Regel teurer als solche ohne diese Eigenschaft. Sicherheit ist aber gleichzeitig eine Produkteigenschaft, deren wirtschaftlicher Nutzen für den Kunden nicht unmittelbar erkennbar und der häufig auch mit gewissen Einschränkungen des Bedienkomforts verbunden ist. Anbieter und Nutzer sehen daher oft keinen unmittelbaren wirtschaftlichen Mehrwert in einer Zertifizierung.

Wie lässt sich dieses Dilemma lösen?

Hier kommt dem Staat eine wichtige Aufgabe zu: Er kann durch geeignete Vorgaben und Rahmenbedingungen bis hin zur gesetzlichen Regelung technische Standards und die Zertifizierung der davon betroffenen Produkte vorschreiben. Das hat sich die Bundesregierung mit der Digitalen Agenda u.a. auch vorgenommen. Es gibt eine ganze Reihe von Digitalisierungsbereichen, bei denen wir erkennen, dass ein Bedarf an Regulierung besteht und der Staat gestalterisch tätig werden muss. Neben den bisherigen erfolgreichen BSI-Aktivi-

Kurzprofil Bernd Kowalski

Bernd Kowalski ist seit 2002 beim BSI beschäftigt und verantwortet als Abteilungspräsident die Bereiche Digitalisierung, Zertifizierung und Standardisierung.

täten in den Bereichen Gesundheit, Energie und Ausweissysteme handelt es sich derzeit insbesondere um die Aufgabenfelder Kraftfahrzeugwesen sowie Finanz- und Zahlungsdienstleistungen. Unsere diesbezüglichen Aufgaben sind dazu in den erstgenannten Bereichen bereits in entsprechenden Gesetzesvorschriften verankert. Daneben werden auch gerade die industrie- und gesellschaftspolitisch wichtigen Bereiche der „Industrie 4.0“ oder des „Internet of Things“ in Zukunft eine zentrale Bedeutung erhalten. Hier stellt sich z.B. die Frage, mit welchen Mitteln man dabei – neben einer gesetzlichen Regelung – die Entwicklung geeigneter Standards unterstützen kann.

Welche Hilfestellung kann das BSI dabei leisten?

Die Zertifizierung im BSI deckt heute bereits eine breite Produktpalette an sicherheitskritischen Komponenten ab. Diese werden insbesondere für sichere Identifikations-, Authentisierungs- und Signaturverfahren eingesetzt, für sichere Onlinezugänge und -transaktionen. Hier haben wir uns eine herausragende Weltmarktposition erarbeitet. Natürlich müssen wir im Zuge der steigenden Nachfrage nach zertifizierten Produkten auch neue Verfahren z.B. für Standardprodukte entwickeln, die für den Einsatz im Massenmarkt – also auch außerhalb der regulierten Bereiche – anwendbar sind.

Wie können gegebenenfalls internationale Anforderungen bei der Zertifizierung erfüllt werden?

Bereits heute erwarten Unternehmen von uns Prüfanforderungen und Zertifizierungen, die sie auch im internationalen Geschäft einsetzen können. IT-Sicherheit kennt keine Grenzen. Gerade,

„Sicherheitsvorgaben einhalten, bevor neue Technologien auf den Markt kommen“

wenn wir Technologie sicher machen und Unternehmen zu Investitionen auf diesem Gebiet motivieren wollen, dürfen wir uns nicht auf den deutschen Markt oder Nischenbereiche beschränken. So stimmen wir die Anforderungen, die wir entwickeln, in Normungsgremien wie dem Common-Criteria-Abkommen, aber auch in Fachgremien auf europäischer Ebene wie dem europäischen Komitee für elektrotechnische Normung sowie industriegesteuerten Gremien ab. Damit wollen wir unsere Vorstellungen von IT-Sicherheit einbringen und die mit den Unternehmen hier in Deutschland entwickelten Zertifizierungsanforderungen zu internationalen Standards machen.

Welchen Einfluss haben Gesetzgebungen und Regulierungen auf EU-Ebene?

In der Vergangenheit hatten wir es bei Zertifizierungen vorwiegend mit deutschen Gesetzen wie dem Personalausweis- und Passgesetz oder dem Energiewirtschaftsgesetz zu tun. Heute jedoch haben wir eine steigende Anzahl an Regulierungen auf EU-Ebene. Ein Beispiel dafür ist die eIDAS-Verordnung für eine sichere Identifizierung und digitale Signaturen. Sie verpflichtet die Staaten, entsprechende Standards zu entwickeln und vorzuschreiben und nur solche Technologien zu unterstützen, die diesen Anforderungen genügen. Dabei arbeiten wir eng mit unseren europäischen Partnern zusammen – besonders mit unserer französischen Partnerbehörde ANSSI –, da sie in vielen Bereichen die gleichen Ziele verfolgen wie wir. Deshalb versuchen wir gemeinsam, unsere Vorstellungen von Sicherheitsstandards für Regulierungen auf europäischer Ebene durchzusetzen. Im Gegensatz zu kommerziellen Anbietern, wie beispielsweise einige globale Internet-Marktführer, wollen wir hier in Europa offene Sicherheitsstandards, die allen Anwendungen zugutekommen. Sie sollen den Wettbewerb verschiedener Anbieter sowie die Nutzung der aufwendigen Sicherheitstechnologie durch alle Nutzer und Anwender erlauben und nicht auf ein bestimmtes Geschäftsmodell eingeschränkt sein. Außerdem sollte jedes Land die Sicherheitsstandards entsprechend seiner Gesetzeslage, seiner gesellschaftlichen Wertvorstellungen und seiner Wirtschaftssituation nutzen können. ■

Weitere Informationen: https://www.bsi.bund.de/zertifizierung

180 NEUE KÖPFE FÜR EINE GEMEINSAME MISSION

Digitalisierung sicher gestalten

Wer bei einem Besuch des BSI in Bonn die Gelegenheit hat, hinter die Kulissen zu blicken, wird vielleicht überrascht sein: Die Stimmung dort entspricht keineswegs dem verstaubten Klischee eines „Amtes“. Vielmehr herrscht die rege Betriebsamkeit eines modernen Unternehmens vor, dessen Arbeitsweise von Austausch und Vernetzung der Kollegen/Kolleginnen geprägt ist. Kein Wunder, denn die enge Zusammenarbeit über Zuständigkeits- und Abteilungsgrenzen hinweg ist wesentlich für die erfolgreiche Arbeit des BSI. Angesichts der immer vielfältigeren Aufgaben freuen sich die BSI-Mitarbeiter/-innen bereits auf die vielen neuen Kollegen, die im Laufe des Jahres zu ihnen stoßen werden. Denn mit rund 180 neu zu besetzenden Stellen erwartet das Amt den größten Personalzuwachs seiner Geschichte – rund jedes vierte Gesicht in den Büros, Laboren und Besprechungsräumen wird dann ein neues sein. Jedoch müssen die geeigneten Kandidaten zuvor gefunden und auch überzeugt werden. Im Fokus steht daher die Frage: Was macht das Arbeiten beim BSI denn zu etwas Besonderem?

Die strategische Entscheidung, dem BSI durch eine massive Verstärkung der Personaldecke zu mehr Schlagkraft zu verhelfen, folgt einer offenkundigen Tatsache: Die Gefährdungslage in der digital vernetzten Welt nimmt kontinuierlich zu. Die Digitalisierung eröffnet ungeahnte Chancen – dass dafür immer komplexere Technologien nötig sind, liegt auf der Hand. Sie führen zu einer rasanten Vergrößerung der Angriffsflächen: Weil komplette Geschäftsmodelle und vollständige Prozesse zunehmend ins Internet verlagert werden, steigt der Umfang des Programmcodes und somit die Anzahl möglicher Schwachstellen. Mit der exponentiell zunehmenden Vernetzung im Internet der Dinge – schon heute kommunizieren bereits Milliarden von Sensoren und Geräten miteinander – vermehren sich auch die möglichen Angriffspunkte. Ob Diebstahl geistigen Eigentums von Unternehmen, die Verfügbarkeit von Kritischen Infrastrukturen oder der Missbrauch künstlicher Intelligenz zur Meinungsbeeinflussung durch Social Bots: Digitale Technologien entwickeln sich rasant weiter und werden leider nicht nur zum Guten eingesetzt.

DIE SICHERE DIGITALE ZUKUNFT AKTIV MITGESTALTEN

Digitale Technologien bringen erhebliche Zukunftschancen für Staat, Wirtschaft und Gesellschaft mit sich. Diese sicher zu nutzen, ist ein erklärtes Ziel des BSI. Denn nur wenn der Cyber-Raum sicher gestaltet werden kann, wird auch die Digitalisierung erfolgreich sein. Diese Perspektive bietet für viele Menschen ein hohes Identifikationspotenzial. So entschied sich auch Thomas Gilles, Referent im Bereich „Cyber-Sicherheit für die Digitalisierung von IoT mit Smart Services“, seinen Karriereweg im BSI einzuschlagen. „In unserem Job zählt immer der konstruktive Lösungsbeitrag“, erklärt Gilles. „Hier kann jeder durch gute Arbeit weiterkommen. Und wer Initiative zeigt, kann mit Unterstützung rechnen.“ In seinem inhaltlich besonders fordernden Arbeitsbereich schätzt er vor allem die Dynamik und die Teamarbeit. „Fachlich sattelfest sollte man in einer Umgebung mit so vielen Experten schon sein. Das heißt aber nicht, dass ich alles selber können muss“, so Gilles weiter. Parallel zur vernetzten digitalen Welt vernetzen auch die

„Hier kann jeder durch gute Arbeit weiterkommen. Und wer Initiative zeigt, kann mit Unterstützung rechnen.“ ***Thomas Gilles***

Experten beim BSI ihr Talent und Wissen, um mit probaten Lösungen zu mehr IT-Sicherheit beizutragen. So zieht Gilles je nach Aufgabe die entsprechend spezialisierten Kollegen hinzu – und zwar, entgegen der landläufigen Vorurteile über die behördliche Arbeit – auf dem kürzesten Weg.

SPANNENDE THEMENVIELFALT

Die Ansichten von Thomas Gilles teilt auch Jan-Hendrick Peters, Sachbearbeiter im Bereich „CERT-Bund“. „Beim BSI kann ich zu etwas wirklich Relevantem beitragen“, so Peters. Er betont die Wichtigkeit der IT-Sicherheit im Zeitalter der Digitalisierung: „Ihre enorme Bedeutung reicht von Gebieten des Privatlebens wie Onlinebanking bis zu wirtschaftlich zukunftsrelevanten Themen wie Industrie 4.0.“ Sein Arbeitsalltag besteht aus regen Kontakten mit anderen nationalen und internationalen CERTs, IT-Sicherheitsbeauftragten in Verwaltung und Wirtschaft sowie Bürgern. „Besonders spannend finde ich beim BSI die Themenvielfalt und den raschen technologischen Fortschritt aufseiten der Angriffe wie auch der Gegenmaßnahmen.“ Bei aller Leidenschaft und Faszination für seinen Beruf, schätzt er auch die Menschlichkeit, von der das Arbeiten in der Cyber-Sicherheitsbehörde geprägt ist: „Das BSI achtet auf eine gesunde Work-Life-Balance und nimmt auch Rücksicht auf die persönlichen Belange der Mitarbeiter.“

VEREINBARKEIT VON FAMILIE UND BERUF

Ein angenehmes Arbeitsumfeld, gepaart mit einer fordernden Aufgabe, ist auch Stefanie Euler, Sachbearbeiterin im Bereich Informationssicherheitsberatung, wichtig im Beruf. Die zweifache Mutter war zu Beginn ihrer Karriere vor fast 15 Jahren als Frau noch eine Exotin im technischen Bereich. Sie freut sich umso mehr, dass der Anteil weiblicher Technologieexperten kontinuierlich steigt. Die Vereinbarkeit von Familie und Beruf stellt das BSI durch Möglichkeiten der Telearbeit, verschiedene Teilzeitmodelle und flexible Arbeitszeiten sicher. So bleibt Stefanie Euler trotz Teilzeittätigkeit immer am Ball. „Dadurch konnte ich einen höheren Grad an Flexibilität erlangen“, berichtet Euler. „Das ermöglicht

„Vom BSI habe ich mich jederzeit gut unterstützt gefühlt.“ ***Stefanie Euler***

IT-FACHKRÄFTE GESUCHT

Das BSI wird im Verlauf des Jahres rund 180 Stellen sukzessive ausschreiben. Es werden Informatiker/-innen, Physiker/-innen, Mathematiker/-innen und Ingenieure/-innen gesucht – sowohl Hochschulabsolventen/innen (Bachelor oder Master) als auch berufserfahrene Fachkräfte aus allen MINT (Mathematik-Informatik-Naturwissenschaft-Technik)- Bereichen. Aber auch Interessierte aus anderen Bereichen (beispielsweise Verwaltungs-/Wirtschaftswissenschaften oder Jura) finden hier interessante Stellenangebote. Interessierte Kandidaten finden auf dem neuen Karriereportal unter **https://www.bsi.bund.de/karriere** alle notwendigen Informationen, von den aktuell ausgeschriebenen Stellen bis hin zu Einblicken in die Arbeitswelt der Behörde.

„Beim BSI kann ich zu etwas wirklich Relevantem beitragen. Und das ist ein gutes Gefühl."

Jan-Hendrick Peters

es mir auch, genügend Zeit mit meiner Familie zu verbringen." Doch nicht nur das ist ihr wichtig: „Nebenbei absolviere ich ein Masterstudium, um später einmal die Möglichkeit zu erhalten, mich auf eine Stelle im höheren Dienst zu bewerben", sagt Euler. „Bereits während meines FH-Studiums habe ich mich vom BSI sehr gut unterstützt gefühlt." Wie bei Stefanie Euler fördert das BSI die Kompetenzen und Talente seiner Mitarbeiter, damit diese auch künftig für die steigenden Anforderungen an die IT-Sicherheit gerüstet sind.

VIELFÄLTIGE AUFGABEN

So unterschiedlich die Karrierewege, Tätigkeiten und Hintergründe der Mitarbeiter sind, so vielfältig sind auch die Aufgabenbereiche, in denen das BSI nach Unterstützung sucht. Dabei stehen auch heute noch neue Technologien und Risiken im Fokus – also spannende Aufgaben, um die digitale Zukunftsfähigkeit von Staat, Wirtschaft sowie Gesellschaft nicht nur zu sichern, sondern auch aktiv zu gestalten: sei es in der Beratung, in kooperativen Gremien, in der Informationsbereitstellung, oder in der operativen Cyber-Abwehr. Neu aufgebaut wird zudem das MIRT (Mobile Incident Response Team), um Cyber-Vorfälle in besonders bedeutenden Einrichtungen zu analysieren und bereinigen. Im Bereich der Prävention wird auch die Auswertung vielfältiger Quellen ausgebaut, um über die Cyber-Sicherheitslage in Deutschland stets aktuell im Bilde zu sein – eine wesentliche Voraussetzung für den besseren Schutz von Regierung, Bevölkerung und Unternehmen. Diesem Ziel dient auch die Vernetzung von Behörden und Wirtschaft – sowohl untereinander als auch übergreifend im Rahmen von Initiativen wie der Allianz für Cyber-Sicherheit und dem UP KRITIS. Aber auch bei der hausinternen IT oder der Presse- und Öffentlichkeitsarbeit warten spannende Herausforderungen auf Bewerber. Alles in allem viele gute Gründe für talentierte Köpfe, sich dem BSI-Team anzuschließen. So wie bereits Jan-Hendrick Peters, der es passend auf den Punkt bringt: „IT-Sicherheit finde ich deshalb so spannend, weil sie entscheidend für unsere digitale Zukunft ist." ■

„WIR WOLLEN DEINE DIGITALE SEITE"

Mit neu aufgestelltem Personalmarketing gegen den Fachkräftemangel: Das BSI möchte geeignete Kandidaten auf die beruflichen Chancen bei der Behörde aufmerksam machen. Neben dem neu aufgesetzten Karriereportal hat das BSI eine Anzeigenkampagne gestartet. Die Motive stehen unter dem Motto „Deine digitale Seite". Nicolas Stöcker, Personalgewinner beim BSI: „Sie unterstreichen, dass das BSI für seine Mitarbeiter und ihre herausfordernde und gesellschaftlich bedeutsame Tätigkeit ideale und verlässliche Rahmenbedingungen schafft. Dazu gehören auch die vielfältigen Möglichkeiten, die Arbeit familienfreundlich und flexibel zu gestalten." Doch das BSI ist auch darüber hinaus ein sehr attraktiver Arbeitgeber. Es genießt bundesweit einen exzellenten Ruf und ist international hoch anerkannt. Zukunftsweisende Sicherheitsprojekte gehören für die Mitarbeiter zum Alltag – so leistet jeder täglich einen wichtigen Beitrag zu mehr Cyber-Sicherheit für die Gesellschaft. Neben einem spannenden Arbeitsumfeld bietet das BSI seinen Mitarbeitern auch ein umfassendes Trainings- und Weiterbildungsprogramm. Dazu kommen internationale Projektarbeit und Konferenzen sowie der regelmäßige Austausch mit führenden deutschen und internationalen Sicherheitsexperten. Außerdem eröffnen sich den Mitarbeitern erstklassige Vernetzungsmöglichkeiten in Politik, Wirtschaft und Verwaltung.

Weitere Informationen: https://www.bsi.bund.de/karriere und bewerbung@bsi.bund.de oder unter Tel.: 0228 99 9582 0

Bund-Länder-Kooperationen

von Arne Schönbohm, Präsident des BSI

Gemeinsam für mehr Cyber-Sicherheit in Deutschland

Die Digitalisierung hält in Bundes- und Landesbehörden gleichermaßen in den operativen wie auch administrativen Bereichen des Verwaltungshandelns Einzug. Dies drückt sich unter anderem in Prozessen wie der behördlichen Aktenführung aus, die zunehmend elektronisch umgesetzt wird. Die Vorteile – höhere Effizienz, sinkende Kosten, geringerer bürokratischer Aufwand – liegen auf der Hand. Gleichzeitig steigt jedoch die Abhängigkeit von der ordnungsgemäß funktionierenden Informationstechnik. In der Praxis sind sich viele Behörden der gravierenden Folgen bewusst, die ein Ausfall der IT mit sich bringen kann. Immer mehr Behörden führen daher Informationssicherheitsmanagementsysteme (ISMS) ein.

Jedoch reicht die behördeninterne Sicht auf die Informationssicherheit langfristig nicht aus. Behörden sind keine Inseln und die digitale Transformation stoppt nicht vor Stadt- oder Landesgrenzen. Im Gegenteil, die Vorteile der Digitalisierung können sich erst dann voll entfalten, wenn sie auch behördenübergreifend zum Tragen kommt. Das Ziel ist daher die Etablierung eines Mindestsicherheitsniveaus im Zuge der zunehmenden Vernetzung verschiedener Behörden. Dazu hat der IT-Planungsrat als politisches Steuerungsgremium im März 2013 die „Leitlinie für die Informationssicherheit“ zwischen Bund und Ländern verabschiedet. Bei deren Umsetzung leistet das BSI seinen Beitrag in Form von Beratungen in der Arbeitsgruppe Informationssicherheit (AG InfoSic) sowie in der Unterarbeitsgruppe Informationssicherheitsmanagement (UAG ISMS). So entstand beispielsweise in der UAG ISMS eine Sammlung von Blaupausen und Hilfsmitteln, die unter anderem bei der Bestellung eines IT-Sicherheitsbeauftragten und der Einführung des ISMS unterstützen. Dieser Ansatz gibt Behörden, die am Anfang des Informationssicherheitsprozesses stehen, eine Hilfestellung, wie klare Strukturen der Informationssicherheit etabliert werden können.

Parallel zur AG InfoSic wurde der Verwaltungs-CERT-Verbund (VCV) für den Informationsaustausch auf Ebene der Computer Emergency Response Teams (CERTs) des Bundes und der Länder gegründet. Neben zwei Treffen

„Fest steht, dass durch die Kooperationen zwischen Bund und Ländern eine ‚Win-win-Situation' entsteht, die insgesamt zu einer Erhöhung des Niveaus der Cyber-Sicherheit in Deutschland führt."

pro Jahr, in denen es um den Erfahrungsaustausch auf operativer Ebene geht, steht insbesondere der schnelle Austausch von Warnmeldungen im Vordergrund der Zusammenarbeit. So wurden im vergangenen Jahr rund 2000 Warnungen über den Warn- und Informationsdienst des beim BSI angesiedelten CERT-Bund an die Abonnenten verteilt. Auch im Bereich der Polizeien des Bundes und der Länder gibt es seit dem Jahr 2004 einen regelmäßigen Austausch zum Thema der Absicherung der Informationen in polizeilichen Informationsverbünden. Hier unterstützt das BSI durch den Austausch von Erkenntnissen auf fachlicher Ebene, die zuletzt in die Erstellung von Anforderungen für die sichere Nutzung des Internets am Arbeitsplatz im Bereich der polizeilichen Strukturen eingeflossen sind.

Fest steht, dass durch die Kooperationen zwischen Bund und Ländern eine „Win-win-Situation" entsteht, die insgesamt zu einer Erhöhung des Niveaus der Cyber-Sicherheit in Deutschland führt. Nur ein ganzheitlicher Ansatz kann Cyber-Sicherheit herbeiführen. Dies unterstreicht auch die im November 2016 veröffentlichten Cyber-Sicherheitsstrategie für Deutschland. Vorgesehen ist eine Intensivierung der ebenenübergreifenden Zusammenarbeit und eine engere Einbeziehung der Länder bei der Fortentwicklung der deutschen Cyber-Sicherheitsarchitektur. Konkret drückt sich dies in der geplanten Erweiterung des BSI-Gesetzes aus. Dieses sieht vor, dass das BSI die Länder – auf deren Ersuchen – in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik unterstützt. Das BSI als die nationale Cyber-Sicherheitsbehörde könnte damit seine Angebote und Dienstleistungen für die Länder weiter ausbauen.

Durch den Aufbau eines des Verbindungswesens innerhalb des BSI sollen zukünftig neue Zielgruppen im Bereich der Länder und Kommunen erschlossen und bestehende Verbindungen hinsichtlich der schnelleren und einfacheren Adressierung von Schlüsselpartnern ausgebaut werden. Ziel ist es, Kompetenzen zu bündeln und Wissen für alle Beteiligten zu transferieren und zentral verfügbar zu machen. Denn eine Zersplitterung der Cyber-Sicherheitskompetenzen würde in diesem Zusammenhang eine Bedrohung für die deutsche Sicherheitsarchitektur darstellen.

Die Digitalisierung birgt viele Chancen, die genutzt werden sollten. Dies muss jedoch einhergehen mit Cyber-Sicherheitsmaßnahmen, die durch gebündelte Kompetenzen für Bund und Länder entwickelt und umgesetzt werden. Das BSI wird hierbei als zentrale Wissens- und Beratungsstelle fungieren und seine Aufgabe zur Gestaltung der Informationssicherheit in Deutschland auch gegenüber den Ländern wahrnehmen. ■

15 JAHRE BSI FÜR BÜRGER

Digitaler Sorglosigkeit entgegenwirken

Die Digitalisierung durchdringt immer mehr Bereiche des täglichen Lebens. Gleichzeitig rüsten Cyber-Angreifer kontinuierlich auf und entwickeln ihre Angriffstechniken rasant weiter. Dadurch hat sich Cyber-Sicherheit zu einer der zentralen Herausforderungen unserer Zeit entwickelt. Selbstbestimmtes, sicheres Handeln im Cyber-Raum wird zunehmend wichtiger – und das nicht nur von Staat und Wirtschaft, sondern auch von Bürgerinnen und Bürgern. Ein erster Schritt zur Bewältigung von Cyber-Gefahren ist es, über die Risiken Bescheid zu wissen.

Das BSI versteht es als seine Aufgabe, die Bürgerinnen und Bürger für einen sicheren Umgang mit Informationstechnologien, mobilen Kommunikationsmitteln und dem Internet zu informieren und zu sensibilisieren. Dabei versetzt das BSI Bürger/innen in die Lage, sich verantwortungs- und risikobewusst im Cyber-Raum zu bewegen.

BSI FÜR BÜRGER

INS INTERNET - MIT SICHERHEIT

www.bsi-fuer-buerger.de ▪ www.facebook.com/bsi.fuer.buerger

CD-ROM von 2002

Im **März 2002** startete der Informationsservice BSI für Bürger mit Unterstützung des Bundesinnenminsters Otto Schily mit dem Slogan „Ins Internet – mit Sicherheit!“ als CD-ROM, die bereits im ersten Jahr über 650.000-mal ausgegeben wurde. Aufgrund der großen Nachfrage und des permanenten Aktualisierungsbedarfs entwickelte das BSI kurz danach ein Internetportal: https://www.bsi-fuer-buerger.de.

Der erste Internetauftritt 2003

https://www.bsi-fuer-buerger.de heute

Seit **2003** stehen so vielfältige Informationen als Internetangebot unter https://www.bsi-fuer-buerger.de zur Verfügung. Für technische Laien werden dort Themen wie Onlinebanking, Smartphone-Sicherheit, E-Mail-Verschlüsselung oder Soziale Netzwerke inklusive Handlungsempfehlungen verständlich aufbereitet.

Im **November 2015** wurde die Webseite vollständig überarbeitet. Interessierte Internetnutzer finden nun noch aktuellere Beiträge in moderner und nutzerfreundlicher Struktur vor. Dass das Angebot gut angenommen wird, zeigt der Anstieg der Seitenaufrufe von durchschnittlich über 151.000 Besuchern pro Monat im Zeitraum Juli 2014 bis Juni 2015 auf durchschnittlich über 172.000 Besucher pro Monat im Zeitraum Juli 2015 bis Juni 2016.

- Mit dem „Bürger-CERT“ bietet das BSI einen kostenlosen Warn- und Informationsdienst, der schnell und kompetent über Schwachstellen, Sicherheitslücken und andere Risiken informiert und konkrete Hilfestellungen gibt. Hierfür analysieren BSI-Experten die Sicherheitslage im Internet und verschicken bei Handlungsbedarf die Hinweise an derzeit über 100.000 Abonnenten. Ergänzend liefert der E-Mail-Newsletter SICHER • INFORMIERT vierzehntäglich die wichtigsten aktuellen Sicherheitsnachrichten.

- Über die Facebook-Seite (www.facebook.com/bsi.fuer.buerger) und den seit März 2016 aktiven Twitter-Kanal (www.twitter.com/BSI_Presse) informiert das BSI zu aktuellen IT-Sicherheitsthemen und tritt in den Dialog mit Bürgerinnen und Bürgern. Zum Stichtag 31. Januar 2017 taten dies 28.129 Fans (Facebook) und 4.729 Follower (Twitter).

- Auch telefonisch oder per E-Mail können sich Privatanwender mit ihren Fragen zu Themen der IT- und Internetsicherheit an das Service-Center des BSI wenden – dies tun monatlich rund 400 Nutzer.

Mit all diesen Informationsangeboten versteht sich das BSI als kompetente, unabhängige Anlaufstelle für Cyber- und IT-Sicherheit mit dem Ziel, diese Themen fest im Bewusstsein der Gesellschaft zu verankern, um der digitalen Sorglosigkeit entgegenzuwirken. Als Behörde ist es damit im Vergleich zu sonstigen europäischen Einrichtungen einzigartig.

IT-SICHERHEIT
IN DER PRAXIS

Security by Design:

eID-GATEWAY

Übergreifende Kommunikation bei Industrie 4.0

von Dr.-Ing. Andre Braunmandl, Referat Cyber-Sicherheit für die Digitalisierung in Verkehr und Industrie 4.0
und Dr. Dennis Kügler, Referatsleiter Chip-Sicherheitsanalyse

Das BSI führt jährlich eine Cyber-Sicherheitsumfrage durch. Im Jahr 2016 gaben über die Hälfte der befragten Institutionen an, bereits Opfer erfolgreicher Angriffe geworden zu sein. Fast alle Opfer erlitten dabei nach eigenen Angaben offenkundige Schäden mit zum Teil durchaus relevanten Folgen für die jeweilige Institution.

CYBER-SICHERHEIT VON INDUSTRIE 3.0 ZU INDUSTRIE 4.0

Insbesondere im industriellen Bereich hat die Verfügbarkeit und Vertrauenswürdigkeit von IT-Systemen essenzielle Bedeutung. Bereits Industrie 3.0 ist durch eine hohe IT-Durchdringung charakterisiert, die eine weitgehende Automatisierung ermöglicht. Erfolgreiche Angriffe gegen einzelne IT-Systeme führen somit zu eher punktuellen Ausfällen oder fehlerhaften Produktionsschritten. Mit dem Übergang zur Industrie 4.0 wird eine durchgängige Vernetzung der IT-Systeme vollzogen, sowohl innerhalb der Unternehmen als auch nach außen über das Internet. Diese durchgängige Vernetzung erhöht die Angriffsfläche für Cyber-Kriminelle und Industriespione drastisch. Klassischer Perimeter-Schutz und die gegenseitige Abschottung relevanter Unternehmensbereiche voneinander reichen hier bei Weitem nicht aus. Für die Industrie 4.0 müssen sich die Systeme selbst besser, auch inhärent, schützen können, um wirksame Maßnahmen wirtschaftlich begründbar bei akzeptablen Restrisiken umsetzen zu können.

Im Bereich der Industrie 4.0 rücken damit neben den traditionellen Anforderungen der Verfügbarkeit und Betriebssicherheit der Produktionsanlagen, die klassischen IT-Sicherheitsziele Vertraulichkeit, Integrität und Authentizität für alle vernetzten Produktionskomponenten als Entwicklungsziele mit in den Vordergrund. Damit ergibt sich ein Zielkonflikt, denn diese zusätzlichen IT-Sicherheitsziele schränken prinzipbedingt die Verfügbarkeit ein. Ist beispielsweise ein Schlüssel zur Authentisierung aufgrund abgelaufener Zertifikate nicht mehr nutzbar, ist das System bis zur Erneuerung des Zertifikats nicht oder nur eingeschränkt nutzbar.

STANDARDISIERUNG UND ZERTIFIZIERUNG FÜR INDUSTRIE 4.0

Um ein hohes Sicherheitsniveau und hohe Verfügbarkeit gleichzeitig gewährleisten zu können, ist eine Standardisierung und Zertifizierung von sicherheitsrelevanten Komponenten und Dienstleistung unumgänglich.

Die wesentliche Grundlage hierfür ist die Einführung eines übergreifenden Berechtigungskonzepts auf Basis einer einheitlichen Verwaltung aller beteiligten elektronischen (Maschinen-)Identitäten (eID-Management). Technisch kann diese flexibel und skalierbar durch den Aufbau einer übergreifenden Public Key Infrastructure (PKI) im Zusammenspiel mit der sicheren Speicherung und Verwaltung der eIDs an den betreffenden Maschinen realisiert werden. Hierfür konzipiert das BSI derzeit ein eID-Gateway mit einem generischen Ansatz, der ein durchgängiges Sicherheitskonzept über alle Ebenen der klassischen Automatisierungspyramide (Abb. 1) unterstützt und auf allen diesen Ebenen zum Einsatz kommen soll.

Zentrales Element des eID-Gateways (Abb. 2) ist ein zertifizierter Sicherheitschip (Sicherheitselement, SE), der als

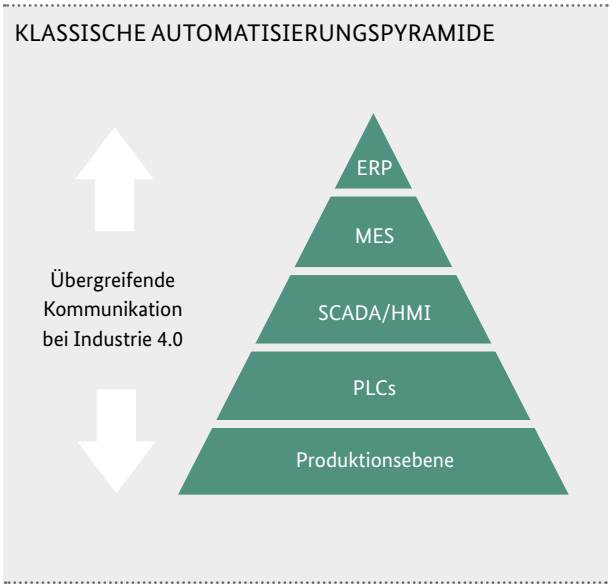


Abb. 1

Hardware-Sicherheitsanker fungiert. Durch die Zertifizierung der Hardware wird eine sichere Erzeugung, Speicherung und Nutzung von Schlüsseln für die eingesetzten kryptografischen Verfahren sichergestellt. Die grundlegenden Anforderungen an geeignete Sicherheitselemente werden derzeit in Technischen Richtlinien und Schutzprofilen des BSI festgelegt. Da diese Chips Einsatzszenarien vom mobilen Endgerät bis hin zum HSM auf Serverebene unterstützen sollen, sind hierbei Mechanismen zur Skalierbarkeit (durch Parallelisierung) und Verfügbarkeit (z.B. durch Redundanz) von hoher Bedeutung. Durch eine klare Separierung von Anwendungs- und Sicherheitsfunktionen in Verbindung mit einem flexiblen Zertifizierungskonzept wird die Nutzung eines einmalig zertifizierten Basis-Sicherheitschips in einem weiten Anwendungsbereich möglich, der neben Industrie 4.0 z.B. Automotive Security, Vehicle2X-Communication oder auch den Einsatz in Registrierkassen umfassen kann. Durch den großen Anwendungsbereich wird der Chip kostengünstig und somit wirtschaftlich einsetzbar sein.

DAS eID-GATEWAY IM EINSATZ

Zur Ansteuerung des eID-Gateways wird seitens des BSI ebenfalls eine einheitliche Schnittstelle (application programming interface, API) spezifiziert. Diese API soll verschiedene Anforderungen erfüllen. Zunächst soll sie den Zugriff auf die Sicherheitselemente und die Software-Kryptobibliotheken über eine einheitliche Schnittstelle ermöglichen, die moderne Industrie-4.0-Kommunikationsstandards wie z.B. OPC UA unterstützt. Der Anwendungsprogrammierer soll sich damit auf die Anwendung konzentrieren können, die ihre Sicherheitsfunktionalitäten unabhängig vom konkret eingesetzten SE über das eID-Gateway aufruft. Damit sollen schließlich so viele IT-Sicherheitsaspekte in den Verantwortungsbereich des eID-Gateway-Administrators verlagert werden wie möglich. Die Rolle des eID-Gateway-Administrators kann dann einem besonderen IT-Sicherheitsspezialisten, beziehungsweise einem zertifizierten Dienstleister übertragen werden. In der Praxis hat sich bislang gezeigt, dass Industrieanlagen-Anwendungsprogrammierung und IT-Sicherheit jeweils so unterschiedliche und anspruchsvolle Wissensbereiche sind, dass sich das entsprechende Expertenwissen nur schwer in einer Person vereinen lässt.

Das eID-Gateway übernimmt damit die Rolle eines universalen Sicherheitsproviders für Industrie 4.0, der die Aufgaben der Authentifizierung und des Vertraulichkeits- sowie Integritätsschutzes für die Maschinenkommunikation (M2M-Kommnikation) im industriellen Umfeld wahrnimmt. Seine Standardisierung ermöglicht ein breites Einsatzfeld und liefert einen umfassenden Sicherheitsansatz zu wirtschaftlichen Bedingungen. ■

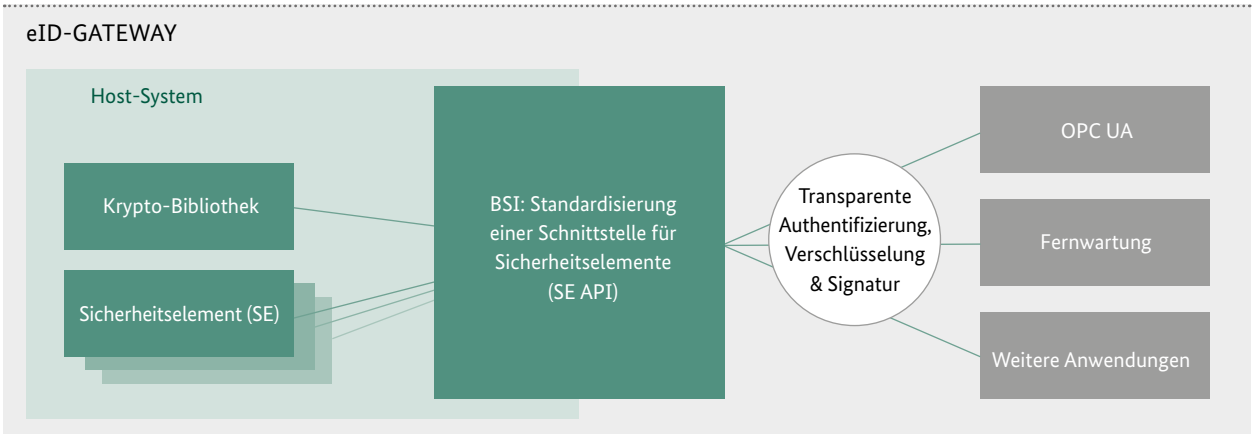


Abb. 2

Mobile Identifizierung sicher gestalten

von Dr. Ulf Löckmann, Referat eID-Anwendungen im eGovernment
und Ingrid Grüning, Referat Cyber-Sicherheit für die Digitalsierung im Gesundheits- und Finanzwesen

Elektronische Überprüfung von Identitätsnachweisen

Ob zur Online-Eröffnung eines Girokontos, zum Kauf einer SIM-Karte oder für einen De-Mail-Zugang: Für viele Dienste in der digitalen Welt ist eine vorherige Identifizierung des Nutzers gesetzlich vorgeschrieben. Damit steigt einerseits der Bedarf und gleichzeitig auch das Angebot an Online-Identifizierungen.

ONLINE AUSWEISEN MIT DEM PERSONALAUSWEIS

Bereits seit 2010 bietet der deutsche Personalausweis eine sichere Methode zur Online-Identifizierung auf hohem Vertrauensniveau. Das Angebot an Diensten zur Nutzung der eID-Funktion ist seitdem allerdings nicht so stark gestiegen wie die Nachfrage nach nutzerfreundlichen Lösungen.

Der steigende Bedarf an Online-Identifizierungen hat dazu geführt, dass sich in Deutschland ein Markt für Fernidentifizierungsdienste gebildet hat. Nach einer Öffnung zur Anwendung nach dem Geldwäschegesetz bieten Identifizierungsdienstleister vermehrt auch Verfahren an, die zur Identifizierung mit dem Personalausweis einen Videochat einsetzen. Viele Banken setzen seither auf die Video-Identifizierung als schnelle Alternative zu traditionellen Verfahren wie PostIdent.

Über einen Videokanal lassen sich allerdings höchstens Sicherheitsmerkmale prüfen, die sich bei bestimmten Lichtverhältnissen unter Bewegung des Ausweises verändern, wie das holografische Porträt oder das Laserkippbild auf der Rückseite. Damit kann aber die Echtheit und Unverfälschtheit eines Ausweises per Video nur eingeschränkt überprüft werden. Und da eine Videoübertragung immer auch anfällig für technische Manipulationen ist, erreichen solche Verfahren aus Sicht des BSI nicht die notwendige Sicherheit, um eine verlässliche Identifizierung zu ermöglichen, wie sie von Angesicht zu Angesicht oder mit der eID-Funktion möglich ist.

GESTIEGENER BEDARF DURCH DIE eIDAS-VERORDNUNG

Um „sichere und nahtlose elektronische Transaktionen zwischen Unternehmen, Bürgern und öffentlichen Verwaltungen zu ermöglichen“, hat die Europäische Union bereits im Jahr 2014 die sogenannte eIDAS-Verordnung erlassen.

Diese regelt seit dem 1. Juli 2016 sogenannte elektronische Vertrauensdienste etwa für qualifizierte elektronische Signaturen und Zeitstempel oder die Zustellung elektronischer Einschreiben. Und genau für solche Dienste ist auch eine verlässliche Identifizierung des Nutzers erforderlich. Es liegt nahe, hier auch medienbruchfreie Verfahren zuzulassen, die ohne Zeitversatz durchgeführt werden können.

Eine Möglichkeit zur Online-Identifizierung bringt die eIDAS-Verordnung gleich selbst mit: Die Mitgliedsstaaten der EU können eigene elektronische Identifizierungssysteme notifizieren, die in den anderen Mitgliedsstaaten anerkannt werden müssen. Dabei wird für jedes Identifizierungssystem das jeweils erreichte Vertrauensniveau angegeben – niedrig, substanziell oder hoch.

ZUKUNFT DER eID-FUNKTION

Für die eID-Funktion des deutschen Personalausweises und des elektronischen Aufenthaltstitels ist eine Notifizierung auf hohem Vertrauensniveau vorgesehen, da sie alle entsprechenden Anforderungen bereits erfüllt. Damit kann die eID-Funktion künftig EU-weit zur sicheren Identifizierung eingesetzt werden.

Um die Marktgängigkeit und Nutzung der eID-Funktion als sicheres Identifizierungsmittel zu fördern, hat das Bundesministerium des Innern einen Gesetzentwurf auf den Weg gebracht. Damit sollen gleichzeitig die Hürden für Diensteanbieter deutlich sinken. So sieht der Entwurf etwa ein vereinfachtes Antragsverfahren für Berechtigungszertifikate vor, und die eID-Funktion wird bei neu ausgegebenen Ausweisen grundsätzlich eingeschaltet sein.

Gleichzeitig stärkt das BSI die technische Nutzbarkeit der eID-Funktion: Mit der mobilen Version der AusweisApp kann die eID-Funktion bequem von einem geeigneten NFC-fähigen Handy aus verwendet werden, ein separates Lesegerät ist nicht mehr erforderlich.

EIGNUNG UNTERSCHIEDLICHER VERFAHREN

Für welches Verfahren zur Identifizierung sich ein Nutzer auch entscheiden mag – wesentlich für das Vertrauen in diesen Vorgang ist eine einheitliche Sichtweise auf das entsprechende Vertrauensniveau, auf das sich Nutzer und Anbieter genauso verlassen können müssen wie Aufsichtsbehörden und der Gesetzgeber.

Um das Sicherheitsniveau unterschiedlichster Verfahren zur Identifizierung einheitlich bewerten zu können, hat das BSI eine Technische Richtlinie verfasst. Damit wird es möglich, aus verschiedenen, gleichermaßen geeigneten Verfahren eines bestimmten Vertrauensniveaus (nach eIDAS-Verordnung) auszuwählen. Die Richtlinie kann als Grundlage für eine einheitliche Prüfung etwa durch akkreditierte Konformitätsbewertungsstellen verwendet werden. Dies schafft Rechtssicherheit für Diensteanbieter und vermeidet anwendungsspezifische Zusatzanforderungen. In entsprechenden Fachgesetzen ist dann nur noch festzustellen, welches Vertrauensniveau für den konkreten Einsatzzweck jeweils erforderlich ist. ■

Die AusweisApp 2 ist als Beta-Version für Android im Google Playstore verfügbar

Weitere Informationen:
https://www.bsi.bund.de/dok/7831034

10 Jahre DsiN: Interview mir Dr. Thomas Kremer, Vorstandsvorsitzender von Deutschland sicher im Netz e.V.

DsiN feierte kürzlich sein 10-jähriges Jubiläum unter dem Motto „Denn Sicherheit kommt von Verantwortung". Was sind die wichtigsten Meilensteine, die der Verein seit seinem Bestehen erreicht hat?

Deutschland sicher im Netz e.V. wurde 2006 auf dem 1. Nationalen IT-Gipfel als gemeinsame Initiative von Wirtschaft, Politik und Gesellschaft gegründet, um Verbraucher und Unternehmen stärker für IT-Sicherheit zu sensibilisieren. Damals nutzte erst jeder zweite Bürger in Deutschland das Internet. Das Smartphone, wie wir es heute kennen, kam erst ein Jahr später auf den Markt – und auch die Internetwirtschaft steckte noch in den Kinderschuhen.

Heute haben wir eine deutlich stärker vernetzte Welt und damit verbunden einen deutlich breiteren Aufklärungsbedarf. Neue DsiN-Angebote zur vernetzten Mobilität sowie zu Schutzwissen in Schulen sprechen für diesen Wandel. Dennoch bleiben auch Standardthemen aktuell: Solange „hallo" oder „12345" zu den am häufigsten genutzten Passwörtern gehören, müssen wir dran bleiben.

Bis zum heutigen Tage haben wir über 10 Millionen Menschen erreicht. Dabei geht es uns vor allem um die Motivation zu Verhaltensänderung und die Einsicht, eine sichere Haltung im Netz einzunehmen. Das erfordert ein professionelles und geduldiges Vorgehen – sowie starke Partner: Unsere Mitglieder und Partner sind die Basis für unsere Initiativen, hier gerade auch die Expertise des BSI sowie auch die Unterstützung der Bundesregierung, allen voran unseres Schirmherren, des Bundesministers des Innern. Sein kraftvolles Bekenntnis zu DsiN auf unserem Jubiläumskongress war für uns ein wichtiges Zeichen.

Auf welchem Fundament ruht die Aufklärungsarbeit des DsiN?

Grundlage unserer Arbeit ist der DsiN-Sicherheitsindex zur Sicherheitslage der Verbraucher in Deutschland. Er fasst die Sicherheitslage in einer Kennzahl zusammen. Zugleich differenziert er die Sicherheitsbedürfnisse nach vier Verbrauchergruppen, die Grundlage unserer Aufklärungsangebote sind: die Fatalisten, die Außenstehenden, die Gutgläubigen und die Souveränen. Die nächste Erhebung kommt Ende Mai 2017 heraus. Jede einzelne Gruppe stellt uns in unserer Aufklärungsarbeit vor unterschiedliche Herausforderungen.

Was sind die Hürden der Aufklärungsarbeit – und wie begegnen Sie diesen?

Es geht darum, Menschen wirklich zu erreichen. Mit den Erkenntnissen aus dem eben schon genannten DsiN-Sicherheitsindex reagieren wir auf ihre konkreten Sicherheitsbedürfnisse sowie Motivationen: So haben wir es bei den Fatalisten mit (vor allem jungen) Menschen zu tun, die unheimlich viel darüber wissen, wie sie sich im Internet schützen könnten, dies aber letztendlich nicht tun, weil sie der festen Auffassung sind, dass dies ja eh nichts bringen würde. Diesem Fatalismus wirken wir mit Angeboten wie dem Jugendwettbewerb myDigitalWorld entgegen, in dem wir junge Menschen motivieren, sich mit ihrem Digitalschutz zu befassen und sogar eigene Ideen dafür zu entwickeln. Bei der Gruppe der Außenstehenden, zu der

„Das BSI ist für uns ein wichtiger Partner, um Aufklärungsangebote mit der notwendigen Expertise zu versehen.“

Kurzprofil Dr. Thomas Kremer

Dr. Thomas Kremer ist Vorstandsvorsitzender von Deutschland sicher im Netz (DsiN) sowie Vorstandsmitglied der Deutschen Telekom. Kleinen und mittleren Unternehmen sowie Verbrauchern bietet DsiN konkrete Hilfestellungen im sicheren Umgang mit dem Internet. In der Cyber-Sicherheitsstrategie der Bundesregierung von 2016 wurde beschlossen, die Aufklärungsarbeit mit DsiN voranzutreiben. DsiN ist ein gemeinnütziger Verein unter der Schirmherrschaft des Bundesministers des Innern mit Sitz in Berlin.

immer noch viele ältere Menschen gehören, ist die Herausforderung weniger das Wollen, sondern eher das noch fehlende Wissen. Hier fangen wir in den Materialien, die der Digital-Kompass für Workshops zur Verfügung stellt, tatsächlich sehr oft bei den Basics an. Die Gruppe der Souveränen wiederum weiß sehr viel und wendet dies auch an. Diese Menschen sind für uns bei DsiN als Multiplikatoren besonders interessant. Wir wollen sie, wie wir es zum Beispiel in der Digitalen Nachbarschaft tun, dafür gewinnen, ihr Wissen und ihre Erfahrungen auch an andere Menschen weiterzugeben.

Kooperationspartnerschaften spielen eine wichtige Rolle bei der Arbeit des DsiN – warum sind diese Partnerschaften so wichtig? Welche Rolle spielt das Bundesamt für Sicherheit in der Informationstechnik dabei?

Das BSI ist für uns ein wichtiger Partner, um Aufklärungsangebote mit der notwendigen Expertise zu versehen. Beispielsweise verweisen wir im Mittelstand häufig auf den BSI-Grundschutz und ziehen hier auch Experten zurate. In diesem Zusammenspiel von DsiN und Partnern wie dem BSI liegt die Zauberformel: Indem wir die Sprache der Verbraucher sprechen und aus ihrer Sicht auf IT-Sicherheit schauen, können wir dazu beitragen, Know-how in die Breite zu tragen und zur Anwendung zu bringen. Grundsätzlich pflegen wir Partnerschaften sowohl zu Experten wie dem BSI oder auch den Fraunhofer-Instituten sowie zu reichweitenstarken Partnern aus der Zivilgesellschaft wie beispielsweise dem Seniorenverband BAGSO oder den IHKs für den Mittelstand – und sind auch stets offen für neue Partnerschaften.

Welche IT-Sicherheitsthemen halten Sie für kritisch und sind Ihrer Meinung nach hier verstärkt aufzuklären? Gerade beim Stichwort Dialog mit Politik und Wirtschaft?

Der DsiN-Sicherheitsmonitor 2016 zeigt, dass die meisten Unternehmen heute über Basisschutzmaßnahmen wie Antivirenschutz verfügen. Zugleich mangelt es an einem Bewusstsein und den Kompetenzen für ganzheitliche Schutzkonzepte. Auch gibt es Defizite in der Umsetzung organisatorischer Maßnahmen, beispielsweise wenn es um Social Engineering als Einfallstor für Cyber-Kriminelle geht. Hier ist noch viel Aufklärungsarbeit zu leisten.

Natürlich gibt es aber auch Grenzen der Aufklärungsarbeit, an denen wir feststellen: Hier müssen wir mit Anbietern der Wirtschaft sprechen – oder auch auf verbindliche Vorgaben für Anwender hinwirken. Ein gutes Beispiel ist die Verschlüsselung: Hier gibt es inzwischen gute Ansätze, dass die Wirtschaft einfache und sichere Lösungen bereitstellt.

Was sind Ihre Pläne für die kommenden 10 Jahre DsiN?

Mit der digitalen Expansion in allen Lebensbereichen steigt auch die Notwendigkeit zur Aufklärung über den sicheren Umgang bei Verbrauchern und Unternehmen. Hier wollen wir unseren Beitrag leisten, Ansprechpartner für praktische Hilfe sein und Orientierungshilfe geben. Natürlich laden wir Unternehmen und Partner dazu ein, diesen Weg auch künftig über gemeinsame Initiativen zu gehen und voranzutreiben. Auch das Bekenntnis der Bundesregierung in der Cyber-Sicherheitsstrategie, die Aufklärungsarbeit mit DsiN voranzutreiben, zahlt auf dieses Ziel ein. ■

DAS SICHERHEISTBAROMETER

Das Sicherheitsbarometer, kurz „Siba“, informiert über die aktuelle IT-Sicherheitslage und gibt Tipps und Hilfestellungen zum Umgang mit Risiken im Netz. Siba kennzeichnet die Gefahren im Internet nach dem Ampelprinzip und hilft Nutzern auf diese Weise, Gefährdungen einzuschätzen. Der Service wird von DsiN in Kooperation mit diversen Partnern, z.B. dem BSI, bereitgestellt.

Siba steht als App in jedem gängigen App-Store sowie unter www.sicher-im-netz.de/siba zum Download bereit.

DIGITALE PIRATERIE

von Joachim Gutmann, Glückburg Consulting AG

Cyber-Angriffe im maritimen Transportwesen

Kurzprofil Joachim Gutmann

Joachim Gutmann ist freiberuflicher Journalist und Buchautor. Seine beruflichen Stationen waren Berlin, Bonn, Düsseldorf, Gummersbach und Hamburg. Dort war er in den letzten 17 Jahren für die Glückburg Consulting AG als Kommunikationsexperte tätig.

In Rotterdam wird ein Containerschiff aus Lateinamerika entladen. Dabei wird ein einzelner Container separat abgeladen, auf einen bereitstehenden Lkw-Anhänger gestellt und sofort abgefahren. Tage später weiß die Reederei: Jemand hatte von außen in das Computerprogramm eingegriffen und den Coup organisiert. Über den Inhalt des Containers darf spekuliert werden.

Ein Beispiel für viele, meint Lars Lange, Generalsekretär der International Union of Marine Insurance (IUMI), des Internationalen Transportversicherungsverbands. „Wir haben heute schon mehr Cyber-Schäden, als wir denken." Ob es die Navigationssysteme auf der Schiffsbrücke, die Antriebssysteme, die interne Kommunikation, die Systeme für Leckagen oder die Dokumente der einzelnen Container betrifft: Mit jedem Neubau kommt mehr Informationstechnologie an Bord.

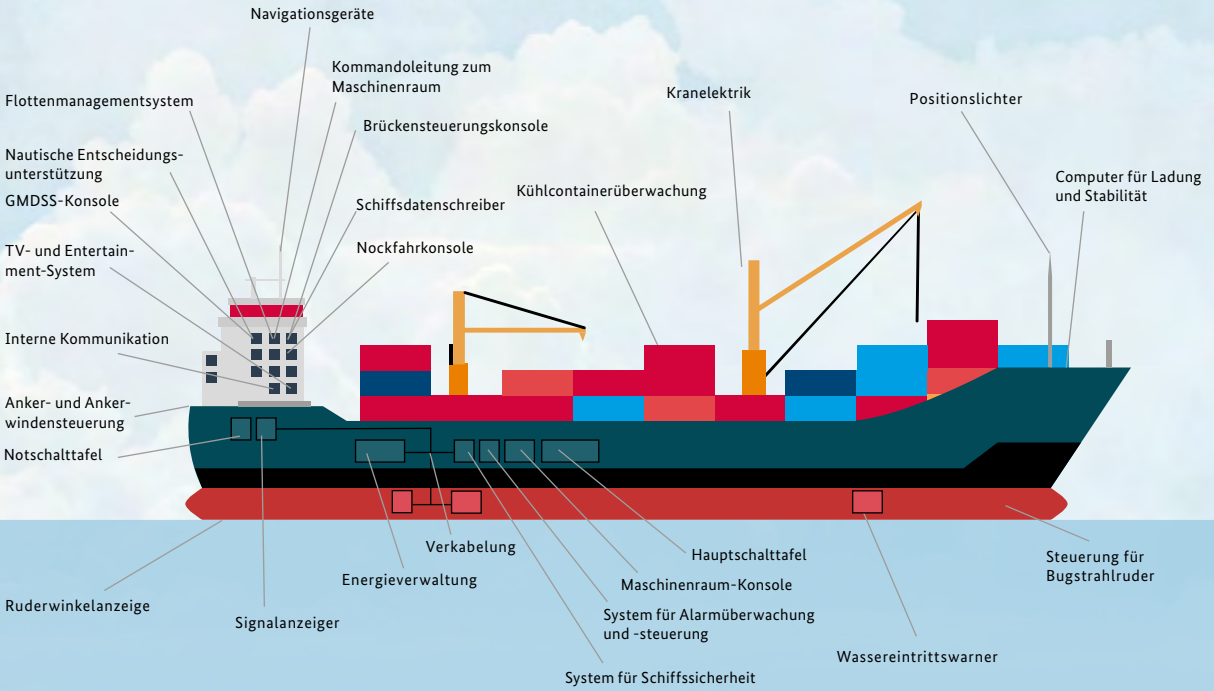
„Ein Schiff ist ein schwimmendes Rechenzentrum", sagt Jan Hinnerk Haul, IT-Experte bei der Klassifikationsgesellschaft DNV GL. Und dieses Rechenzentrum kann angegriffen werden. Insgesamt 26 Angriffspunkte hat das US-Transportministerium gesammelt. Bereits 2013 haben Forscher der Universität von Texas nachgewiesen, dass ein Schiff von außen umgelenkt werden kann. Dafür wurden GPS-Daten manipuliert. Und schon berechneten die Navigationssysteme an Bord die Position falsch. Im Ernstfall ein Super-GAU. Die Gefahr ist durchaus real, denn das an Bord genutzte Navigationssystem ECDIS (Electronic Chart Display and Information System) macht ein Schiff nicht nur anfällig für Störungen, es verbindet es auch mit dem Internet und ist so ein Einfallstor für Computer-Hacker.

Nicht nur auf See, auch an Land lauern Cyber-Gefahren. Die Zutrittsysteme, das Cargo-Handling, die Steuerungssysteme der Kräne, die in vielen Anlagen eingesetzte SCADA-Software machen den Hafen zu einem cyber-physischen System. Und zwar einem schlecht geschützten. Nach einem Bericht des Baltic and International Maritime Council (BIMCO), der weltweit größten Schifffahrtsorganisation, haben IT-Experten bei einer Untersuchung von 20 Containerhäfen festgestellt, dass 16 Standorte „ernst zu nehmende Schwachstellen" aufwiesen.

Auch Reedereien werden ausgespäht, um herauszufinden, welche Schiffe mit wertvoller Ladung und zugleich geringer Bewachung unterwegs sind. Nach einer aktuellen Umfrage des Weltreederverbandes (2016) gaben 21 Prozent der Befragten einen Cyber-Angriff zu, 57 Prozent verneinten und 22 Prozent machten keine Angabe. Sie beklagten Datenverlust (48 Prozent), finanzielle Verluste (21 Prozent) und Einschränkungen der IT-Funktionalität (67 Prozent). Nur 4 Prozent berichteten von einem Angriff auf Schiffssysteme. Und nur jede vierte Reederei hatte sich Gedanken über Abwehrsysteme gemacht. „Das ist zu wenig", sagt Lars Lange. „Die Reedereien wollen das Risiko nicht sehen." Von einem Schiffsverlust durch einen Cyber-Angriff ist bislang zwar auch noch nichts bekannt – aber das dürfte nur eine Frage der Zeit sein.

So lange wollen die maritimen Branchenverbände BIMCO, CLIA, ICS, INTERCARGO und INTERTANKO nicht warten. Sie sind sich einig: Die Zeit ist reif für Cyber Security an

MÖGLICHE ANGRIFFSZIELE FÜR CYBER-KRIMINELLE



Quelle: ICS Security in Maritime Transportation U.S. Department of Transportation

Bord von Schiffen. Anfang 2016 veröffentlichten sie eine Anleitung zur Verbesserung der Cyber Security auf Schiffen – vom Kreuzfahrtschiff über Frachtschiffe bis hin zu Tankern. Die Richtlinie orientiert sich dabei an international anerkannten Rahmenwerken wie dem Cyber Security Framework des NIST und bezieht maritime Sicherheitsstandards wie ISM Code und ISPS Code mit ein. Ihr Ziel: allgemeinverbindliche technische Regelungen zu schaffen und die Crew an Bord regelmäßig zu trainieren.

Diese Regelungen sind zwingend: Je mehr nämlich die Verknüpfung von Steuerungs- und Navigationssystemen mit weiteren Netzen und Entertainment-Systemen voranschreitet, umso mehr erleichtern IT-Schnittstellen entlang dieser Kette Dritten den Zugriff auf Unternehmensnetzwerke. Reeder geben Entwarnung, weil es bislang noch gar nicht überall auf den Meeren möglich ist, per Internet eine stabile Verbindung zu den Schiffen herzustellen. Zudem sollen auf den Schiffen die Systeme für den Betrieb und die Steuerung von denen für die Kommunikation getrennt werden. Das soll die Sicherheit ebenso erhöhen wie Virenscanner und Firewalls in den Kommunikationssystemen an Bord.

Für Prof. Dr. Thorsten Blecker vom Institute of Business Logistics and General Management der TU Hamburg liegt die größte Gefahrenquelle ohnehin woanders, nämlich in den nicht gepflegten Programmable Logic Controllers (PLC), die zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt und auf digitaler Basis programmiert werden – und eben ungeschützt mit dem Internet verbunden sind. Ihre lange Lebensdauer (bis zu 25 Jahre), veraltete Protokolle (z. T. ohne Sicherheitsfeatures) und das Problem, Patches einzuspielen (Verfügbarkeit), machen sie zum Sicherheitsrisiko. „Wir brauchen ein IT-Sicherheitsmanagement auch im maritimen Transportsektor“, fordert Becker.

Mehr Training und mehr Awareness sind dagegen für Jan Hinnerk Haul das Gebot der Stunde. Er beklagt die Mailflut durch die Reedereien an die Schiffe, ein Einfallstor für Malware, ebenso wie den unkontrollierten Einsatz von USB-Sticks und fehlende Antivirussysteme. So fordert die International Maritime Organization, dass Reedereien dringend eine Anweisung für die Mitglieder der Schiffscrew benötigen, wie sie mit sozialen Medien im Internet umgehen sollen. Beklagt wird auch, dass die meisten Schiffe – von den großen Kreuzfahrern abgesehen – weder einen Spezialisten für die Elektronik noch für die Informationstechnologie regelmäßig an Bord haben. Vor dem Hintergrund der aktuellen Bedrohungslage dürfte sich dies bald ändern. ■

Sichere Passwörter

BSI-Basistipp

Passwörter für den E-Mail-Account, Soziale Netzwerke oder den Computer sind wie Schlüssel für das eigene Zuhause: Nur ein sicheres Passwort schützt vor ungewollten Gästen und deren Zugriff auf persönliche Daten, Fotos oder Kontoinformationen.

Dabei gilt für den virtuellen Schlüssel, genauso wie für den Haustürschlüssel – je ausgefeilter, umso schwieriger ist es das Schloss zu knacken.

Umgang mit Passwörtern

- ☑ Passwörter unter Verschluss halten
- ☑ Passwörter in regelmäßigen Zeitabständen ändern
- ☑ Keine einheitlichen Passwörter für Accounts verwenden
- ☑ Voreingestellte Passwörter ändern
- ☑ Passwörter nicht an Dritte weitergeben und nicht per E-Mail versenden

*) ***Die Eselsbrücke:*** *Indem Sie sich jeweils den ersten Buchstaben eines jeden Wortes in einem Satz merken, können Sie sich ganz einfach an ein Passwort mit mehr als acht Zeichen erinnern. Schon sind Sie bestens geschützt. Beispiel: „Am liebsten esse ich Pizza mit vier Zutaten und extra Käse!“ wird zum Passwort: AleiPm4Z+eK! Schon sind Sie bestens geschützt.*

Weitere Informationen: https://www.bsi-fuer-buerger.de/Passwoerter

SPIONAGEABWEHR DURCH ABSTRAHLSCHUTZ

von Dr. Amin Hellerbach, Referat Abstrahlsicherheit

Wer das Schlagwort „IT-Sicherheit“ hört, wird im Allgemeinen zuerst an Malware, Schwachstellen, Hacker, Phishing-Mails und Botnetze denken. Abseits dieser sehr präsenten Gefahren für die IT-Sicherheit existieren jedoch weitere, subtilere Pfade, auf denen kritische Informationen entweichen können. Einer dieser Pfade beruht auf der Ausnutzung physikalischer Effekte und wird als „Kompromittierende Abstrahlung“ bezeichnet.

WAS IST KOMPROMITTIERENDE ABSTRAHLUNG?

Auch wenn wir sie im Alltag nicht wahrnehmen können, sind wir jederzeit und überall von elektromagnetischen Feldern umgeben. Jedwedes elektrisch betriebenes Gerät strahlt sie ab und kann dadurch teils unvorhergesehene Effekte hervorrufen. Dank der konsequenten Umsetzung von Richtlinien zu Funkentstörung und elektromagnetischer Verträglichkeit seitens der Industrie bleibt dies zumeist unbemerkt und folgenlos, wenngleich das Auftreten kurioser Phänomene nicht endgültig ausgeschlossen ist. So können beispielsweise Herzschrittmacher in der Nähe großer elektrischer Anlagen in ihrer Funktion so stark gestört werden, dass die Konsequenzen für den Träger fatal wären. Maßnahmen zur Funkentstörung verringern die Stärke abgestrahlter elektromagnetischer Felder so weit, dass keine Störungen mehr zu erwarten sind; eliminiert werden die Felder dabei jedoch nicht. Somit ist es weiterhin möglich, verarbeitete Informationen aus den Emissionen eines IT-Geräts aufzufangen, auszuwerten und zu rekonstruieren. Werden dabei staatliche Geheimhaltungsinteressen berührt, spricht man von „Kompromittierender Abstrahlung“ oder synonym TEMPEST.

DAS BEDROHUNGSSZENARIO

Bei Vorliegen eines hohen Schutzbedarfs von elektronisch zu verarbeitenden Informationen wird oftmals bewusst auf eine Ankopplung an das Internet verzichtet und somit allen Angriffen aus dem Internet die Grundlage entzogen. Gerade unter solchen Voraussetzungen ist Kompromittierende Abstrahlung ein effektiver, klandestiner und durchaus genutzter Angriffsvektor. Kritische Daten werden dabei aufgefangen, bevor sie verschlüsselt beziehungsweise nachdem sie entschlüsselt vorliegen. Wird beispielsweise eine Textdatei verschlüsselt transportiert, ist sie spätestens auf dem Bildschirm des Bearbeiters im Klartext zu sehen. Eine eventuell vertrauliche Antwort wird, ebenso wie Passwörter, per Tastatur eingegeben. Alle genannten Gerätschaften strahlen ab

Symbolbild einer Abstrahlprüfkabine

und werden somit unbemerkt zum Sicherheitsrisiko. Ein technisch versierter Angreifer kann außerhalb des überwachten Sicherheitsbereiches eine entsprechende Sonde versteckt anbringen, um abgestrahlte Signale aufzufangen. Da diese Art von Lauschangriff rein passiv funktioniert, hat der Angreifer eine Entdeckung kaum zu befürchten.

GEGENMASSNAHMEN DES BSI

Um die Aufwände im vertretbaren Rahmen zu halten, fokussiert sich das BSI auf präventive Maßnahmen zur Minimierung der Risiken durch Kompromittierende Abstrahlung. Handlungsgrundlage sind Verwaltungsvorschriften für den Schutz von Verschlusssachen, die das BSI im nationalen Rahmen federführend erstellt. Als „National TEMPEST Authority“ wirkt das BSI bei deren Gestaltung auch im internationalen Kontext in EU- und NATO-Gremien aktiv mit und ist zuständig für Zulassungsvorgaben. Sollen Verschlusssachen mit einer Einstufung höher als VS-NUR FÜR DEN DIENSTGEBRAUCH verarbeitet werden, müssen die entsprechenden IT-Anlagen zuvor einen erweiterten Zulassungsprozess erfolgreich bestehen. Im Bereich Abstrahlsicherheit umfasst dies praktische Messungen der Emissionscharakteristik eines Geräts. Hierzu verfügt das BSI hausintern über nachrichtentechnische Messlabore für systematische und reproduzierbare Prüfungen. Im Falle großer Objekte, wie beispielsweise Schiffe und Flugzeuge, werden auch Abstrahlprüfungen vor Ort durchgeführt.

PRAKTISCHE UMSETZUNG

Das BSI betreut eine Reihe von Firmen, die marktverfügbares IT-Gerät in handwerklicher Arbeit mit Abschirmmaßnahmen aufwerten. Um die Wirksamkeit dieser Abschirmmaßnahmen zu verifizieren, wird jedes so gehärtete Gerät einer Abstrahlprüfung unterzogen und seine individuelle Emissionscharakteristik („Fingerabdruck“) erstellt. Bei einer erneuten Prüfung, z. B. bei Verdacht auf Manipulation, wird damit eine Erkennung von gegebenenfalls von einem Angreifer vorgenommenen Änderungen möglich. Wenn das Gerät alle Prüfungen erfolgreich besteht, wird es mit Siegeln versehen, die unter anderem als Bestätigung und ebenfalls der Manipulationserkennung dienen. Anschließend ist es im Hinblick auf seine Abstrahleigenschaften für den Einsatz zur Verarbeitung von Verschlusssachen zugelassen.

Die vom BSI betreuten TEMPEST-Gerätehersteller sind berechtigt, Abstrahlprüfungen durchzuführen. Die Zulassung anhand eines Mustergerätes wird ausschließlich vom BSI vorgenommen; die Hersteller führen dann mittels eines vom BSI vorgeschriebenen Messverfahrens die Abstrahlprüfungen für ihre Serienfertigung durch. ■

TL-03305

In der Technischen Leitlinie TL-03305 sind die vom BSI betreuten TEMPEST-Gerätehersteller sowie deren Produkte, die das Zulassungsverfahren bereits bestanden haben, aufgeführt. Ebenso sind maßgeschneiderte Geräte möglich, wenn ein Bedarfsträger dies wünscht oder benötigt. Hierfür kann dieser sich an einen der benannten Hersteller wenden, der sich für alle Zulassungsfragen eng mit dem BSI abstimmt.

Weitere Informationen:
https://www.bsi.bund.de/dok/6800054

QUELLCODEPRÜFUNGEN ALS VERTRAUENSBASIS

von Oliver Zendel, Referatsleiter Evaluierungskoordination und -methodologie und Thomas Caspers, Fachbereichsleiter Evaluierung und Betrieb von Kryptosystemen

Moderne IT-Produkte benötigen einen angemessenen, bedarfsgerechten und damit oftmals immer weiter steigenden Funktionsumfang. Dies hat direkte Auswirkungen auf die Komplexität der Produkte. In der Regel besitzen sie mittlerweile eine so große Komplexität, dass schon allein aus statistischen Gründen mit zahlreichen Fehlern gerechnet werden muss. Zwischen Angreifern und Verteidigern hat sich ein wahres Rennen entwickelt, wer diese Fehler schneller findet. Somit stellt sich beim Einsatz von Software für sicherheitskritische Regierungsanwendungen stets die Frage, wie ein umfassendes Vertrauen in IT-Produkte begründet werden kann. Strategien zur Beantwortung dieser Frage müssen auch darauf zielen, Analysemethoden für die Aufdeckung wissentlich oder unabsichtlich in den Quellcode eingebrachter Fehler und Sicherheitslücken zu finden. Hier kommt als präventive Maßnahme der unmittelbaren Analyse von Quellcodes eine Schlüsselrolle zu, denn ausschließlich auf dieser Ebene liegen sämtliche Funktionen und Verarbeitungsschritte sowie die interne Struktur eines IT-Produktes vollständig und transparent vor.

Viele Hersteller erkennen inzwischen die hohe Bedeutung eines geregelten Zugriffs auf den Quellcode an, um den steigenden Anforderungen an Nachweise zur Vertrauenswürdigkeit gerecht zu werden. Gerade große Hersteller haben daher Verfahren etabliert, Dritten, wie z. B. Regierungsstellen, Quellcodeprüfungen zu ermöglichen (siehe Kasten). Software, die unter Freien Lizenzen steht, gewährleistet jederzeit Quellcodeanalysen beliebiger Tiefe und mit frei gewählten Randbedingungen. Eine Reihe von technischen, organisatorischen und rechtlichen Herausforderungen stellt sich hingegen bei

proprietären Produkten, um aus der Einsichtnahme in den Quellcode überhaupt sinnvolle und verlässliche Schlüsse ableiten zu können.

Für Analysten, die Aussagen zur Vertrauenswürdigkeit treffen sollen, bilden spezifische Kenntnisse der von den Herstellern verwendeten Architekturen und Techniken die entscheidenden Voraussetzungen für erfolgreiche Prüfungen. Darüber hinaus ist es bei komplexen Produkten zwingend erforderlich, Quellcodeanalysen mit technisch fortgeschrittenen und frei wählbaren Werkzeugen durchführen zu können. Rein manuelle Quellcodeinspektionen wie z. B. ein bloßes „Lesen" des Codes lassen bis auf wenige Ausnahmen, etwa die sehr gezielte Überprüfung von spezifischen Produkteigenschaften, keine Rückschlüsse auf das gesamte Produkt zu. Der Einsatz von Analysewerkzeugen, die weitgehend automatisierte Prüfungen erlauben, stößt jedoch nicht bei allen Herstellern proprietärer Produkte unbedingt auf Gegenliebe, denn damit verbundene Anforderungen können in der Praxis technisch sehr anspruchsvoll werden und verursachen hohe Aufwände. Im internationalen Umfeld kommen unter Umständen komplexe rechtliche Rahmenbedingungen hinzu.

Neben dem umfassenden Zugriff auf den eigentlichen Programmcode und der dazugehörigen Dokumentation ist für das BSI die Verfügbarkeit der Quellen für die jeweils letzte stabile Version einschließlich der aktuellsten Sicherheitsupdates von entscheidender Bedeutung. Reproduzierbare Builds schaffen dann einen überprüfbaren Weg von den Quellen bis zu den Binärdateien. Aus diesem Grund spielt die Einbeziehung von Compiler, Linker und Verfahren zur Codesignierung eine zunehmend wichtigere Rolle. Nur so kann sichergestellt werden, dass die Untersuchungen sich auch tatsächlich auf die später eingesetzten Binärdateien beziehen.

In der Regel beschränken IT-Hersteller den Zugriff auf Quellcode, wenn sie ihn nicht unter Freien Lizenzen veröffentlichen, auf Räumlichkeiten, die vollständig unter ihrer eigenen Kontrolle stehen. Auch in solchen Konstellationen ist für die Erreichung einer hinreichend unabhängigen Bewertung der Einsatz eigener Analysesysteme erforderlich. Die Mitnahme und der Einsatz solcher Systeme muss der jeweils prüfenden Stelle durch den Hersteller ermöglicht werden.

Erfahrungen mit Herstellern, die ein echtes Interesse an tiefer gehenden und begründbaren Vertrauensaussagen zu ihren Produkten haben, zeigen, dass erfolgreiche und gewinnbringende Quellcodeanalysen bereits heute umsetzbar sind. Liegen für ein Softwareprodukt keine geeigneten und hinreichend hohen Zertifizierungen etwa nach Common Criteria vor, die bereits verlässliche Aussagen beinhalten, bilden gezielte Quellcodeuntersuchungen einen pragmatischen Ansatz zur Gewinnung von Vertrauensaussagen. Dabei ist naturgemäß nicht nachweisbar (und auch gar nicht das eigentliche Ziel), dass eine Software wirklich vollständig frei von Fehlern und Sicherheitslücken ist. Besonders kritische Aspekte, etwa bei der Erzeugung von Zufallszahlen sowie der Einbindung und Konfiguration von Bibliotheken zur Verschlüsselung oder Authentisierung, sind jedoch bei Verfügbarkeit des Quellcodes ausreichend prüfbar. Dabei entsteht auch ein erheblicher Nutzen für den Hersteller eines IT-Produkts, da verringerte Fehlerzahlen zu sinkenden Kosten im Lebenszyklus des Produkts führen. Alle Anwender des Produkts profitieren zudem von erhöhten Sicherheitseigenschaften. Für den Einsatz in kritischen Umgebungen, wie der in der Regierungskommunikation eingesetzten Informationstechnik, ergeben sich schließlich mit einer konsequenten Umsetzung von Quellcodeanalysen vielversprechende Ansätze für nachvollziehbare Vertrauensaussagen und qualitativ bessere Lösungen. ■

PROGRAMME GROSSER IT-HERSTELLER ZUR QUELLCODEEINSICHTNAHME:

APPLE OPEN SOURCE
https://opensource.apple.com/

CISCO OPEN SOURCE UND TECHNOLOGY VERIFICATION SERVICE
http://opensource.cisco.com/
http://www.cisco.com/c/en/us/about/trust-transparency-center/validation/technology-verification.html

GOOGLE ANDROID OPEN SOURCE PROJECT UND CHROMIUM
https://source.android.com/
https://www.chromium.org/

MICROSOFT OPEN SOURCE UND GOVERNMENT SECURITY PROGRAM
https://opensource.microsoft.com/
https://www.microsoft.com/en-us/twc/government-security-program.aspx

ORACLE SOURCE CODE FOR OSS UND VIRTUALBOX
http://www.oracle.com/technetwork/opensource/index.html
https://www.virtualbox.org/wiki/Downloads

RED HAT OPEN SOURCE
https://www.redhat.com/de/open-source

VMWARE OPEN SOURCE
http://www.vmware.com/de/download/open_source.html

SCHRÖDINGERS KATZE

Es handelt es sich um ein Gedankenexperiment aus der Physik, das 1935 von Erwin Schrödinger vorgeschlagen wurde. Es problematisiert die direkte Übertragung quantenmechanischer Begriffe auf die makroskopische Welt in Form eines Paradoxons. Das Paradoxon besteht darin, dass dem Gedankenexperiment nach eine Katze in einem verschlossenen Kasten mit den Regeln der Quantenmechanik in einen Zustand gebracht werden könnte, in dem sie gleichzeitig „lebendig“ und „tot“ ist. In diesem Zustand verbleibt die Katze, bis die Experimentieranordnung untersucht wird, also der Kasten geöffnet und nachgeschaut wird. Die gleichzeitig tote und lebendige Katze wird erst dann eindeutig auf „lebendig“ oder „tot“ festgelegt, wenn man sie beobachtet, also eine Messung durchführt.

DIGITALE GESELLSCHAFT

Informationssicherheit im Quantenzeitalter

von Dr. Heike Hagemeier und Dr. Manfred Lochter, Referat Kryptografische Vorgaben und Entwicklungen

„Mit der Entwicklung eines Quantencomputers ist in ungefähr 10 Jahren zu rechnen, und das schon seit 30 Jahren." Dieser Witz hält sich hartnäckig, vor allem unter denjenigen, die den Möglichkeiten von Quantencomputern skeptisch gegenüberstehen. Aktuelle Entwicklungen zeigen aber, dass es schon heute Zeit ist zu handeln.

Die Sicherheit digitaler Infrastrukturen beruht heute wesentlich auf Public-Key-Kryptografie. Dabei werden hauptsächlich Verfahren eingesetzt, die sich auf die angenommene Schwierigkeit bestimmter mathematischer Probleme stützen. Beispielsweise basiert das RSA-Kryptosystem auf der Tatsache, dass es im Allgemeinen schwierig ist, große Zahlen in ihre Primfaktoren zu zerlegen.

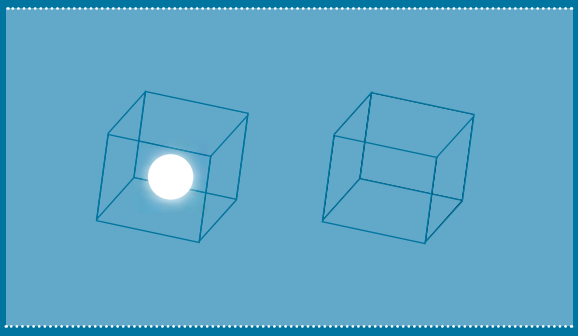
Mit den heute verfügbaren Mitteln sind die (korrekt und mit der richtigen Schlüsselgröße) eingesetzten Public-Key-Verfahren nicht zu brechen.

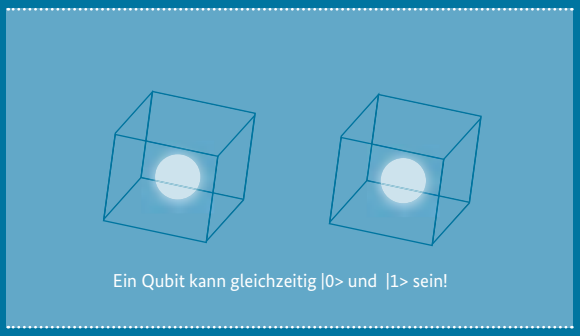
Allerdings wurde bereits 1994 von Peter Shor ein Algorithmus vorgestellt, der die genannten Verfahren auf damals noch rein hypothetischen Quantencomputern leicht brechen und damit der heutigen Public-Key-Kryptografie die Grundlage entziehen würde. Dabei sollte nicht vergessen werden, dass symmetrische Verfahren (wie AES-256) durch Shors Algorithmus nicht gefährdet sind. Bei symmetrischen Verfahren würde sich die benötigte Schlüssellänge durch potenzielle Angriffe mit einem Quantencomputer verdoppeln („Grovers Algorithmus").

Die Idee eines Quantencomputers stammt von R. Feynman (Anfang der 1980er-Jahre) und beruht auf den Gesetzen der Quantenmechanik. Ein Quantencomputer würde sich von den heutigen Computern dadurch unterscheiden, dass er statt mit Bits mit sogenannten Qubits (s. Kasten) rechnet.

Bisher ist noch kein Quantencomputer, der zum Brechen kryptografischer Verfahren geeignet wäre, verfügbar. Es gibt jedoch große Fortschritte bei der Realisierung der dafür benötigten Grundbausteine. In den letzten Jahren hat die Entwicklung von Quantencomputern ein ständig zunehmendes Interesse in Forschung und Industrie erfahren.

BITS UND QUBITS





DEFINITION EINES BITS:
Das Bit ist im Zustand 0, wenn das Teilchen im linken Kasten ist, und im Zustand 1, wenn das Teilchen im rechten Kasten ist.

DEFINITION EINES QUBITS:
Das Qubit ist im Zustand |0>, wenn das Quantenteilchen im linken Kasten ist, und im Zustand |1>, wenn das Quantenteilchen im rechten Kasten ist.

Quantencomputer nutzen die Prinzipien der Quantenphysik. Sie rechnen mit Quantenbits (Qubits), die im Gegensatz zu klassischen Bits zwei Zustände (mit gewissen Wahrscheinlichkeiten) gleichzeitig annehmen können (Superposition). Ein Quantencomputer kann mit n verschränkten Qubits in einem Schritt Berechnungen durchführen, für die ein herkömmlicher Rechner 2^n Operationen benötigt.

Globale IT-Konzerne wie IBM, Google oder Microsoft investieren erhebliche Ressourcen in die Quantenforschung und konnten bereits beachtliche Fortschritte erzielen. Diese Unternehmen sind allerdings eher an gewinnbringenden Einsatzgebieten von Quantencomputern wie beispielsweise Pharmazie oder Materialforschung interessiert. Die EU startet gerade ein Flagship Project im Umfang von einer Milliarde Euro, um Quantentechnologien zu erforschen und wirtschaftlich nutzbar zu machen.

QUANTENSPRUNG FÜR DIE KRYPTOGRAFIE DER ZUKUNFT

In der Kryptografie entwickelte sich parallel zu den technologischen Fortschritten ein neues Forschungsgebiet: die Post-Quantum(PQ)-Kryptografie. Dieses beschäftigt sich mit der Entwicklung und Untersuchung von kryptografischen Verfahren, die auch mit Quantencomputern nicht gebrochen werden können. Dabei ist hervorzuheben, dass diese Verfahren auf „klassischen“ Computern funktionieren und sich damit wesentlich von einem anderen aktuellen Forschungszweig unterscheiden: der Quantenkryptografie. Die Quantenkryptografie versucht, quantenmechanische Effekte für kryptografische Anwendungen zu nutzen. Ein Beispiel dafür ist die quantenbasierte Schlüsselverteilung, die die Eigenschaften von sogenannten verschränkten Teilchen ausnutzt.

In den letzten Jahren hat die Post-Quantum-Kryptografie erheblich an Bedeutung gewonnen: Die NSA hat im August 2015 vor Quantencomputern gewarnt und die Migration zu quantencomputerresistenten Verfahren eingeleitet. Als Begründung gibt die NSA aktuelle Fortschritte in Physik und Technologie an, die die Entwicklung eines kryptografisch relevanten Quantencomputers ermöglichen könnten. Konkrete quantencomputerresistente Verfahren hat die NSA dabei nicht benannt, sondern auf die künftigen Standards des National Institute for Standards (NIST) verwiesen. Dementsprechend hat NIST mit dem Standardisierungsprozess für PQ-Kryptografie begonnen.

Mehrere internationale Forschergruppen beschäftigen sich zur Zeit intensiv mit der Sicherheit und Praktikabilität von PQ-Kryptografie. Im Rahmen des Horizon-2020-Programms finanziert die EU beispielsweise zurzeit die europäischen Projekte PQCrypto und SAFEcrypto.

„Der Einsatz quantencomputerresistenter Verfahren wird früher oder später für die meisten kryptografischen Anwendungen zum Standard werden."

Von den Forschern werden dabei verschiedene Ansätze zur Realisierung von quantencomputerresistenten Verfahren verfolgt. Dies sind beispielsweise gitterbasierte Verfahren, codebasierte Verfahren oder hashbasierte Signaturen. Dabei bilden die hashbasierten Merkle-Signaturen das bisher einzige Verfahren, das bereits allgemein als sicher und gut erforscht angesehen wird und auch vom BSI (etwa für die Signatur von Softwareupdates) empfohlen wird. Zurzeit scheinen sich allgemein die gitterbasierten Verfahren immer mehr durchzusetzen. So wurde beispielsweise der gitterbasierte Algorithmus „New Hope" zum Schlüsselaustausch testweise in Googles Browser Chrome implementiert. Bisher sind allerdings viele der neuen Verfahren noch nicht praktikabel und nur unzureichend erforscht. Die Standardisierung von PQ-Kryptografie steht insgesamt noch am Anfang. Zudem müssen viele der heute verwendeten Sicherheitsprotokolle erst an die Formate der PQ-Verfahren angepasst werden. Es muss damit gerechnet werden, dass sich eine Migration auf grundlegend neue kryptografische Verfahren nur sehr langsam und nicht ohne Reibungsverluste vollziehen wird.

WIE VIEL ZEIT HABEN WIR?

„I estimate a 1/7 chance of breaking RSA-2048 by 2026 and a 1/2 chance by 2031." *Michele Mosca, Nov. 2015*

Solche Schätzungen sind natürlich immer noch vage. Aber für kryptografische Anwendungen mit langen Geheimhaltungsfristen ergibt sich daraus dennoch akuter Handlungsbedarf. Es besteht die Gefahr, dass große Mengen von verschlüsselten Daten auf Vorrat gesammelt werden und in der Zukunft mithilfe eines Quantencomputers entschlüsselt werden können. Aus demselben Grund müssen auch die heute verwendeten Schlüsseleinigungsverfahren entsprechend lange sicher sein.

Signaturen zum Zwecke der Authentisierung dagegen haben in der Regel eine eher kurze Lebensdauer und müssen im Prinzip nur bis zum Zeitpunkt ihrer Prüfung sicher sein. Sollte ein Signaturverfahren in der Zukunft durch einen Quantencomputer gebrochen werden können, so sind die heutigen Signaturzertifikate vermutlich bereits abgelaufen. Nur bei sehr langen Gültigkeitszeiten für Signaturschlüssel ist Vorsicht geboten.

Der Einsatz quantencomputerresistenter Verfahren wird früher oder später für die meisten kryptografischen Anwendungen zum Standard werden. Ein kurzfristiger Einsatz ist aus den genannten Schwierigkeiten (z. B. Praktikabilität, Kompatibilität) dennoch nicht realistisch. Das BSI empfiehlt daher, wenn möglich, vorerst „hybride" Lösungen einzusetzen. „Hybrid" bedeutet hier die Kombination der klassischen Verfahren mit geeigneten quantencomputerresistenten Lösungen. Hierfür sind verschiedenste Ansätze denkbar.

Zudem sollte bei der Neu- und Weiterentwicklung von Anwendungen vor allem darauf geachtet werden, diese möglichst flexibel zu gestalten, um auf alle denkbaren Entwicklungen reagieren, kommende Empfehlungen und Standards umsetzen und möglicherweise in Zukunft geschwächte Algorithmen austauschen zu können. ■

Kurzprofil Dr. Michael Meier

Prof. Dr. Michael Meier ist Leiter der Abteilung Cyber Security des FKIE. Dieser Bereich analysiert Angriffstechniken und entwickelt Monitoring-Prozesse sowie Kontrollmechanismen zum Schutz vor Cyber-Angriffen auf IT-Systeme. Prof. Dr. Meier ist Inhaber des Lehrstuhls für IT-Sicherheit am Institut für Informatik der Universität Bonn, mit dem das FKIE zusammenarbeitet. Seine Forschungsschwerpunkte sind die angewandten Aspekte von IT-Sicherheit, Angriffs- und Malware-Analysen.

VERNETZUNG MIT NEBENWIRKUNGEN

von Prof. Dr. Michael Meier, Abteilungsleiter Cyber Security, Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE

Sicher ins Internet of Things

Das Internet of Things (IoT) macht das Leben in vielen Haushalten smarter: Kameras, Babyfone, Fernseher, Thermostate in Smart Homes werden mit dem Internet verbunden – und müssen vor Cyber-Angriffen geschützt werden.

Alles andere als smart sind hingegen die Sicherheitseigenschaften der meisten IoT-Systeme. Häufig werden Standard-Passwörter verwendet, die – einmal geknackt – Zugriff zu sämtlichen Geräten desselben Typs gewähren. Auch auf Updatestrategien, mit denen Sicherheitslücken in der Gerätesoftware regelmäßig geschlossen werden, verzichten viele Hersteller aus Kostengründen. Cyber-Kriminelle nutzen diese Schwachstellen aus. Sie bringen möglichst viele internetfähige Geräte unter ihre Kontrolle, um sie für ihre Zwecke zu missbrauchen – eine Methode, die im Fall des Mirai-Botnetzes im Oktober letzten Jahres für Furore gesorgt hat. Die Betreiber dieses großen Netzwerks kontrollieren mehr als 400.000 IT-Komponenten, um Denial of Service (DoS)-Angriffe auszuführen: Sie überlasten die Server populärer Internetdienste und erzwingen damit deren Ausfall.

Prof. Dr.-Ing. habil. Jürgen Beyerer, Institutsleiter des Fraunhofer IOSB, und Bundesministerin für Bildung und Forschung Prof. Dr. Johanna Wanka bei der Eröffnung des Lernlabors Cyber-Sicherheit in Görlitz.

HERSTELLER UND NUTZER IN DER PFLICHT

Weil die wirtschaftlichen Schäden dieser Angriffe enorm sind, gilt es, IoT-Geräte dagegen abzusichern. Zum einen müssen bindende Sicherheitsstandards an den Verkauf der Systeme gekoppelt, Standard-Passwörter verboten und Sicherheitsupdates regelmäßig bereitgestellt werden. Zum anderen sollte aber auch den Nutzern die Mitwirkung zur Absicherung ihrer internetfähigen Geräte auferlegt werden. Selbst wenn sie rechtlich nicht für Cyber-Attacken haften, so ist es doch fahrlässig, beispielsweise das Router-Passwort nicht zurückzusetzen, obwohl sämtliche Medien darüber berichten, dass die Geräte für das Mirai-Botnetz geködert werden. Wie bei der Einnahme von Medikamenten müssen Nutzer aufgeklärt werden, dass die Vernetzung im IoT „Nebenwirkungen“ hat, wenn sie ihre IT nicht absichern.

CYBER-SICHERHEIT EINE FRAGE DER QUALIFIKATION

Letzten Endes müssen die Sicherheitsmaßnahmen aber auch so in das Gerätedesign integriert werden, dass sie für den Nutzer einfach umsetzbar sind. Hierfür ist eine Qualifikation der verantwortlichen Mitarbeiter erforderlich. Die Fraunhofer Academy, die Weiterbildungseinrichtung der Fraunhofer-Gesellschaft, entwickelt für ihr Lernlabor Cybersicherheit verschiedene Lernpfade und Module, unter anderem explizit zur IoT-Sicherheit. Das berufsbegleitende Weiterbildungsformat vermittelt aktuelles Know-how aus der Spitzenforschung und befähigt Mitarbeiter – vom Security-Experten über den Entwickler bis zum Management – IoT-Geräte sicher zu gestalten. ■

IoT – aber sicher!

von Arne Schönbohm, Präsident des BSI

Der Cyber-Angriff auf den Internet-Dienstleister Dyn im Oktober 2016 zeigt anschaulich, dass die Digitalisierung ohne Cyber-Sicherheit nicht erfolgreich sein wird. Angreifer durchsuchen das Internet nach verwundbaren Netzwerkgeräten, werden hunderttausendfach fündig und schließen die Geräte zu einem schlagkräftigen Botnetz zusammen. Davon sind mittlerweile nicht nur PCs, Notebooks oder mobile Geräte betroffen, sondern Haushaltsgeräte, die im Zuge des Internets der Dinge (Internet of Things, IoT) immer öfter mit dem Internet verbunden werden. Die Anwender merken oft nicht, dass ihre Geräte übernommen wurden.

Das BSI als Gestalter der IT-Sicherheit durch Prävention, Detektion und Reaktion fordert daher IoT-Hersteller auf, nicht nur funktionale und preisliche Aspekte, sondern die folgenden Sicherheitsanforderungen bei der Produktentwicklung zu berücksichtigen:

- Nutzer sollten die Möglichkeit haben, voreingestellte Zugangsdaten und Passwörter für alle Zugriffsmöglichkeiten auf die Geräte (z. B. via HTTP, TELNET oder SSH) zu ändern.
- Können Passwörter nicht individualisiert werden, sollten IoT-Geräte ihre Nutzer vor der Inbetriebnahme zu einem Passwortwechsel zwingen.
- Nicht genutzte Dienste sollten deaktiviert werden können.
- Die ein- und ausgehende Kommunikation des IoT-Geräts sollte nur mittels kryptografisch geschützter Protokolle wie TLS erfolgen.
- IoT-Geräte dürfen nicht automatisch über Universal Plug and Play (UPnP) eine unsichere Konfiguration im Router herstellen und so Verbindungen zu unsicheren Diensten erlauben.
- Um auch längerfristig Cyber-Angriffe zu erschweren, sollten sich Hersteller dazu verpflichten, regelmäßig Sicherheitsupdates zur Verfügung zu stellen, die kryptografisch geschützt übertragen und installiert werden können.
- Zudem sollte die Produkt-Firmware hinreichend gehärtet sein; dadurch kann beispielsweise das Nachladen von Inhalten aus dem Internet verhindert werden.

Das BSI wird den Dialog mit den Herstellern und Verbänden verstärken, um gemeinsam Lösungsansätze zu entwickeln.

Smart Meter Gateway

von Dennis Laupichler, Referatsleiter Cyber-Sicherheit für die Digitalisierung der Energiewende

Cyber-Sicherheit für die Digitalisierung der Energiewende

Intelligente Messsysteme sind wichtige Bausteine im intelligenten Netz und benötigen „Security & Privacy by Design". Das Smart Meter Gateway ermöglicht als zentrale Kommunikationsplattform des intelligenten Messsystems die sichere Umsetzung vielfältigster Anwendungsfälle und wird zum Treiber für Innovationen der Digitalisierung. In Zusammenhang mit den technischen Standards des BSI schafft das Gesetz zur Digitalisierung der Energiewende verbindliche Rahmenbedingungen für den sicheren und datenschutzkonformen Einsatz von intelligenten Messsystemen in verschiedenen Einsatzbereichen. Die Ausgestaltung von verbindlichen Mindestanforderungen zur sicheren Integration der Ladesäuleninfrastruktur von Elektromobilen in das intelligente Netz wird nun folgen.

DIGITALE TRANSFORMATION DER ENERGIEWIRTSCHAFT

Die mit der rasanten Technologieentwicklung einhergehende Digitalisierung aller gesellschaftlichen Lebensbereiche stellt Staat, Wirtschaft und unsere Gesellschaft vor große Herausforderungen. Im Bereich der Energiewirtschaft werden sowohl die digitale Transformation des Energiesystems als auch die Integration von dezentralen und erneuerbaren Erzeugungsanlagen die bisherige Wertschöpfungskette gravierend verändern. Neue, innovative Geschäftsmodelle entstehen und zugleich nehmen auch bisher branchenfremde Unternehmen als neue Wettbewerber am deutschen Energiemarkt teil.

Die zunehmende Digitalisierung und Vernetzung führt in der Energiewirtschaft auf der einen Seite zu Effizienzsteigerungen und Prozessoptimierungen sowie zu mehr Komfort, indem Produktkomponenten sowie Systeme untereinander kommunikativ verknüpft werden. Auf der anderen Seite steigt zukünftig mit der Digitalisierung und Vernetzung das Bedrohungspotenzial deutlich an, da sich die Anzahl der Angriffspunkte erhöht, die Kommunikationsinfrastrukturen immer komplexer werden und die zu verarbeitenden Datenmengen sich vervielfachen.

Die Wahrscheinlichkeit erfolgreicher Angriffe auf digitalisierte Infrastrukturen wird folglich zunehmend größer. Daher sind nachweislich sichere Produktkomponenten und Systeme im Netz sowie eine sichere Kommunikationsinfrastruktur entscheidend für das Vertrauen der Anwender.

DATENSCHUTZ UND DATENSICHERHEIT

Eine erfolgreiche digitale Transformation kann nur mit der frühzeitigen Entwicklung und Bereitstellung von allgemein verbindlichen Sicherheitsstandards und Maßnahmen zur Sicherung der Vertrauenswürdigkeit digitaler Infrastrukturen gelingen. Elektronische Identitäten und Verschlüsselung spielen hier eine zentrale Rolle für eine sichere und datenschutzkonforme Digitalisierung. Hierzu müssen neue Technologien nicht nur in Deutschland entwickelt, sondern auch erfolgreich eingeführt werden, um in zukünftigen digitalen Märkten eine führende Gestaltungsrolle einzunehmen und letztlich mit dem digitalen Wandel die Energiewende als gesellschaftliches Ziel zu erreichen.

RECHTSRAHMEN UND TECHNISCHE STANDARDS DES BSI

Das Gesetz zur Digitalisierung der Energiewende, welches zum 2. September 2016 in Kraft getreten ist, trägt diesen Kernanforderungen Rechnung und schafft deshalb entscheidende Voraussetzungen für den Aufbau einer intelligenten Infrastruktur für die Energiewende. Gegenstand des neuen Messstellenbetriebsgesetzes (MsbG, Artikel 1 des Gesetzes zur Digitalisierung der Energiewende) enthält unter anderem die Festlegung hoher technischer Standards

„Die zukünftige Integration des Smart Meter Gateways in die Ladesäule ermöglicht ein sicheres und datenschutzkonformes Laden und Abrechnen von Ladevorgängen."

für intelligente Messsysteme in Form von Schutzprofilen (Protection Profiles, PP) und Technischen Richtlinien (TR) des BSI zur Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität.

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 deren 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.

Das Gesetz zur Digitalisierung der Energiewende ermöglicht den kontinuierlichen stufenweisen Ausbau der intelligenten Messsysteme und anderer Komponenten um weitere Anwendungsfälle wie beispielsweise das netzdienliche Einspeise- und Lastmanagement von Erzeugern und Verbrauchern, die Integration von weiteren Sparten (Gas, Wasser, Wärme) und der Ladesäuleninfrastruktur im Bereich der Elektromobilität.

SICHERE INTEGRATION DER LADESÄULEN-INFRASTRUKTUR VON ELEKTROMOBILEN

Der Rechtsrahmen zeigt bereits perspektivisch über § 48 MsbG die Ausgestaltung von verbindlichen Mindestanforderungen zur sicheren Integration der Ladesäuleninfrastruktur von Elektromobilen in das intelligente Netz auf. Die Nutzung der Batterien von Elektromobilen als Stromspeicher und die Erzeugung von Regelenergie, die zum Ausgleich der schwankenden Einspeisung aus Windparks und Solaranlagen gebraucht wird, werden zukünftig eine wichtige Rolle spielen. Zugleich müssen Ladevorgänge von Elektromobilen vorausschauend in Energiemanagementsystemen aufeinander abgestimmt werden, um Netzschwankungen und negative Rückwirkungen in das intelligente Netz zu vermeiden. Die zukünftige Integration des Smart Meter Gateways in die Ladesäule ermöglicht ein sicheres und datenschutzkonformes Laden und Abrechnen von Ladevorgängen. Neben Anforderungen an die Ladesäule und an die Gesamtsystemarchitektur sind daher sichere Authentisierungsverfahren, sichere Administration und Betrieb der Ladepunkte, eine datenschutzkonforme Messwertverarbeitung sowie die Notwendigkeit einer vertrauenswürdigen Kommunikationsinfrastruktur entscheidend.

Das BSI wird hierzu gemeinsam mit dem Wirtschaftsministerium den Dialog- und Abstimmungsprozess zu Verbänden, Interessengruppen und Förderprojekten aufnehmen, um das Ziel einer sicheren Integration der Ladesäuleninfrastruktur von Elektromobilen in das intelligente Stromnetz zu gewährleisten. ■

Weitere Informationen: www.bsi.bund.de/SmartMeter

Spätestens seit den US-Präsidentschaftswahlen sind sie in aller Munde: Social Bots, die hauptsächlich in sozialen Medien wie Facebook oder Twitter ihr Unwesen treiben. Dabei handelt es sich um Computerprogramme, die nach ihrer Aktivierung ohne menschliches Zutun automatisiert im Internet agieren. Das Ziel von Social Bots ist, durch die schiere Masse von Äußerungen wie Tweets, Retweets, Kommentaren und Likes ein bestimmtes Meinungsbild zu erzeugen, das eine vermeintliche gesellschaftliche Realität abbildet. Diese Technik, so sind sich Experten einig, kann folglich geeignet sein, die politische Diskussion zu beeinflussen und damit letztendlich auch der Demokratie großen Schaden zuzufügen.

SOCIAL BOTS

Roboterkampf um die Meinungshoheit im Netz

Nach dem Erfolg von Donald Trump bei den US-Präsidentschaftswahlen war sich ein großer Teil der Beobachter sicher: Nie zuvor haben die sozialen Medien so stark zum Ausgang einer politischen Wahl beigetragen wie in den USA im Herbst 2016. Dabei sind erst wenige Jahre vergangen, seit soziale Medien ihren Siegeszug in der immer stärker digital vernetzten Gesellschaft angetreten haben. Inzwischen nutzt fast jeder dritte Deutsche nach dem „Reuters Institute Digital News"-Report vom Juli 2016 soziale Medien nicht nur, um mit Bekannten in Kontakt zu bleiben, sondern neben Zeitungen und dem Fernsehen auch als Nachrichtenquelle. Besonders vor diesem Hintergrund kommt der zunehmenden Verbreitung von Social Bots eine herausragende Bedeutung zu.

50 JAHRE CHATBOTS

Ihren Ursprung haben automatisierte Dialogsysteme wie Social Bots oder Chatbots bereits in den sechziger Jahren des vergangenen Jahrhunderts, als der Informatiker Joseph Weizenbaum mit ELIZA eine computerbasierte Sprachverarbeitung entwickelte, die als eine geniale frühe Anwendung von künstlicher Intelligenz gilt. Durch die rasanten Technologiesprünge der vergangenen Jahre sind die Datenverarbeitung und damit auch die Entwicklung künstlicher Intelligenz erheblich vorangeschritten. Die Hürden für die Entwicklung und den Einsatz von Social Bots sind deshalb nahezu verschwunden. Mit vergleichsweise geringem Arbeits- und Geldaufwand lassen sich Programme schreiben, die in soziale Netzwerke entsandt werden und dort Kommentare und Postings liken, empfehlen oder kommentieren.

Fortgeschrittene Ausprägungen sind sogar in der Lage, selbstständig Nutzerprofile zu erstellen mit Bild, Namen und einigen weiteren Angaben. Sogar zu längeren Texten und Meinungsaustausch sind bestimmte, komplexere Formen der mit künstlicher Intelligenz ausgestatteten Bots bereits fähig. Die Krux dabei ist: Ein normaler Internetnutzer ist nicht in der Lage, ein solches Bot-Profil oder -Posting von dem eines echten Menschen zu unterscheiden. Der Social Bot wird sich mit anderen falschen und echten Nutzern vernetzen, Nachrichten kommentieren, Postings teilen und liken, und ein Aktivitätsniveau erreichen, das ein echter Internetnutzer im wahren Leben kaum schaffen kann. Für die Deutungshoheit solch aktiver, vernetzter Meinungsroboter sorgen derweil die Algorithmen der sozialen Netzwerke: Je häufiger ein Inhalt gelikt oder geteilt wird, desto prominenter erscheint er auf den Plattformen; wer bereits viele Follower hat, erreicht umso mehr neue Nutzer. Auf diese Weise kann der Effekt von nur wenigen Bots und Nutzern sehr groß sein. Der Manipulation von öffentlichen Meinungsbildern wird dadurch Tür und Tor geöffnet.

KÜNSTLICHE BEEINFLUSSUNG DER BUNDESTAGSWAHL?

Mit der nahenden Bundestagswahl sind die mit Social Bots verbundenen Gefahren weit nach oben auf die Agenda gerückt. Bundesinnenminister Thomas de Maizière erklärte unlängst, er werde „dafür eintreten, dass alle Parteien in Deutschland, die an der nächsten Bundestagswahl teilnehmen, öffentlich erklären, dass sie an solchen Aktionen nicht teilnehmen."

Das BSI beobachtet die Entwicklungen auf diesem Feld sehr genau. Wie im aktuellen IT-Lagebericht dargestellt, hat es bereits Angriffe auf Parteien, Medien und staatliche Einrichtungen entdeckt, welche die Sorge vor einer gezielten Manipulation der öffentlichen Meinung durch Dritte begründen. Dazu gehören auch die Aktivitäten sogenannter Trolle. Im Gegensatz zu Social Bots verbergen sich hinter Trollen echte Menschen, die gegen Bezahlung gezielte Desinformationskampagnen und Falschmeldungen, sogenannte Fake News verbreiten, um das öffentliche Meinungsbild zu beeinflussen. Denn die sozialen Medien sind schnell – und ist eine falsche Nachricht erstmal im Internet und somit in der Welt, ist es sehr schwer, sie wieder zu entfernen oder gar vergessen zu machen. ■

ZU GUTER LETZT

VERANSTALTUNGSÜBERSICHT 2017

15. Deutscher IT-Sicherheitskongress

16.–18. Mai 2017 in Bonn-Bad Godesberg

Die Digitalisierung und Vernetzung vieler Lebens- und Arbeitsbereiche geht rasant voran. Gleichzeitig machen technische Innovationen in Bereichen wie Industrie 4.0, intelligente Verkehrssysteme oder im Rahmen der Energiewende deutlich, dass der Sättigungsbereich des möglichen Einsatzes von Informationstechnologie noch lange nicht erreicht ist. Erfolgreich in der Umsetzung können die genannten Entwicklungen aber nur sein, wenn dabei von Anfang an neben funktionalen und ökonomischen Faktoren auch Aspekte der IT-Sicherheit angemessen berücksichtigt werden. Digitalisierung ohne IT-Sicherheit wird letztendlich nicht funktionieren.

Die Sicherheit von IT-Produkten wird angesichts der rasanten Innovationsgeschwindigkeit und des daraus folgenden ökonomischen Erfolgsdrucks häufig weder von Nutzern noch von Anbietern gleichrangig mitbetrachtet. Die besondere Herausforderung dabei ist, die Sicherheitsziele mit den Nutzeransprüchen in Einklang zu bringen und Produkte zu entwickeln, die den Bedürfnissen der Anwender entsprechen.

Ein Lösungsansatz besteht darin, bei aktuellen Entwicklungen in Bereichen wie Automotive, Industrie 4.0 oder mobilen Anwendungen bereits jetzt Standards zu formulieren, die etablierte Vorgehensweisen und Erkenntnisse in die Produktentwicklung mit einfließen lassen. Nicht zuletzt muss der Verbraucherschutz, also der Schutz der Bürgerinnen und Bürger bei der Nutzung von digitaler Kommunikation und Diensten, eine besondere Rolle einnehmen. Es gilt für Wirtschaft, Staat und Gesellschaft, einen Mittelweg zwischen zu viel Sicherheit und zu hoher Risikobereitschaft zu finden.

Der 15. Deutsche IT-Sicherheitskongresses steht daher unter dem Motto:

„Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis“

Mit über 600 Fachbesuchern (im Jahre 2015) ist der Deutsche IT-Sicherheitskongress, den das BSI alle zwei Jahre ausrichtet, eine feste Größe im Veranstaltungskalender der IT-Sicherheitsbranche. Drei Tage lang diskutieren die Teilnehmer über den Stand der nationalen und internationalen Entwicklung zur IT-Sicherheit. Ziel des Kongresses ist es, das Thema IT-Sicherheit aus unterschiedlichen Blickwinkeln zu beleuchten, Lösungsansätze vorzustellen und weiterzuentwickeln. Eine begleitende Ausstellung ergänzt das Vortragsprogramm.

Informationen zu Teilnahmemöglichkeiten, Vortragsprogramm und begleitender Ausstellung unter: https://www.bsi.bund.de/IT-Sicherheitskongress

WEITERE VERANSTALTUNGEN MIT BSI-BETEILIGUNG:

Hannover Messe Industrie (HMI)

24.–28. April 2017

Das BSI ist auf der Hannover Messe Industrie (HMI) vom 24. bis 28. April 2017 mit einem eigenen Stand (Halle 8, Stand D29) vertreten und informiert dort über aktuelle Herausforderungen der Cyber-Sicherheit und IT-Sicherheitsprojekte mit Bezug zur Industrie. Das BSI präsentiert sein breites Angebot an Fachinformationen zur sicheren Gestaltung der Digitalisierung in Staat, Wirtschaft und Gesellschaft.

Jobmesse konaktiva

9.–11. Mai 2017

Jobmesse ITS.connect

19. Mai 2017

Das BSI stellt sich auf den Jobmessen konaktiva an der Technischen Universität Darmstadt und ITS.connect in Bochum als potenzieller Arbeitgeber vor. Interessierte Studierende und Absolventen erhalten Informationen zum Berufseinstieg, zu Karrieremöglichkeiten und zu den spannenden Aufgabenfeldern, die sich Mitarbeiterinnen und Mitarbeitern im BSI bieten.

it-sa

10.–12. Oktober 2017

Vom 10. bis 12. Oktober 2017 ist das BSI mit einem Stand und diversen Vortragsaktivitäten auf der it-sa in Nürnberg vertreten. Das BSI fungiert gemeinsam mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom e. V.) als ideeller Träger.

Die it-sa ist die einzige IT-Security-Messe im deutschsprachigen Raum und eine der bedeutendsten weltweit. Ob Cloud Computing, IT-Forensik, Datensicherung oder Hosting: Die Messe ist eine einzigartige Plattform für IT-Sicherheitsbeauftragte, Entwickler und Anbieter von Produkten und Dienstleistungen rund um das Thema IT-Security.

Eine aktuelle Vorschau zu Veranstaltungen mit BSI-Beteiligung finden Sie unter:
https://www.bsi.bund.de/Veranstaltungen

Was wir wollen: Deine digitale Seite

Fotos © iStock.com/Grafissimo; © iStock.com/Krasyuk

Bundesamt
für Sicherheit in der
Informationstechnik

Informationstechnik ist die Grundlage des modernen Lebens. Umso wichtiger ist es, dass die Menschen der digitalen Welt vertrauen können. Darum kümmern wir uns. Als nationale Behörde für Cyber-Sicherheit gestalten wir IT-Sicherheit in Deutschland – aber auch in Europa und der Welt. Dazu arbeiten wir mit Wirtschaft und Wissenschaft zusammen. Wir beraten Politik und Verwaltung und stehen im Dialog mit den Bürgern sowie zahlreichen Verbänden. Im internationalen Austausch sind unsere Experten geschätzt und gefragt. Alles für ein gemeinsames Ziel: Informationssicherheit. Wir sorgen dafür, dass die Zukunft aus dem Netz erwachsen kann. Mit rund 650 Mitarbeitern sind wir ein vergleichsweise kleines Team für eine große Aufgabe. Und deshalb brauchen wir Verstärkung.

Weitere Informationen: https://www.bsi.bund.de/karriere und bewerbung@bsi.bund.de oder unter Tel.: 0228 99 9582 0

IMPRESSUM

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI) 53175 Bonn
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Referat B23 – Cyber-Sicherheit für den Bürger und Öffentlichkeitsarbeit Godesberger Allee 185–189 53175 Bonn Telefon: +49 (0) 228 999582-0 E-Mail: bsi-magazin@bsi.bund.de Internet: www.bsi.bund.de
Stand:	März 2017
Texte und Redaktion:	Stephan Kohzer und Nora Basting, Bundesamt für Sicherheit in der Informationstechnik (BSI) Joachim Gutmann, GLC Glücksburg Consulting AG Fink & Fuchs AG
Konzept, Redaktion und Gestaltung:	Fink & Fuchs AG, Berliner Straße 164 65205 Wiesbaden Internet: www.finkfuchs.de
Druck:	Druck- und Verlagshaus Zarbock GmbH & Co KG Sontraer Str. 6 60386 Frankfurt a.M. Internet: www.zarbock.de
Artikelnummer:	BSI-Mag 17/705-1
Bildnachweise:	Titel: Henning Schacht (Foto), BSI (Hintergrund); S. 1: Stephan Kohzer/BSI; S.4 Catharina Frank (o.l.), Sabrina Löhr, Posteo e.K. (Mitte), Stephan Kohzer/BSI (u.r.); S. 5 CSCG, Institut für Internet-Sicherheit – if(is) (o.l.); S. 6–7: R. Winkler; S. 8: MeinUnternehmensfilm GmbH; S. 10: R. Winkler; S. 11 Henning Schacht; S. 12: Karin Berneburg/BILDSCHÖN GmbH; S. 13: Karin Berneburg/BILDSCHÖN GmbH; S. 14: bluedesign/fotolia; S. 16: liuzishan/fotolia; S. 19: Henning Schacht; S. 20: kasto/fotolia (o.l.), Henning Schacht (o.r.); S. 21: Henning Schacht (o.l.), Henning Schacht (o.r.); S. 22–23: R. Winkler; S. 24: Deutsche Cyber-Sicherheitsorganisation GmbH; S. 25: R. Winkler; S. 27: Stephan Kohzer/BSI; S. 28–29: R. Winkler; S. 30-31: Stephan Kohzer/BSI; S. 32: R. Winkler; S. 34: Stephan Kohzer/BSI; S. 35: Stephan Kohzer/BSI (o.l.), Fink & Fuchs Fotos iStock.com/ Grafissimo, iStock.com/Krasyuk (u.r.); S. 36: Henning Schacht; S. 38: Leo Leowald; S. 39: Leo Leowald; S. 41: BSI; S. 42: R. Winkler; S. 44: Deutschland sicher im Netz e.V.; S. 46–47: enanuchit/fotolia; S. 48: dstarky/fotolia (Bild), ICS Security in Maritime Transportation U.S. Department of Transportation (Idee); S. 49: R. Winkler; S. 51: BSI; S. 52: R. Winkler; S. 54: R. Winkler; S. 56: R. Winkler; S. 58: nexusplexus/123 RF Lizenzfreie Bilder (Hintergrund), Fraunhofer (o.l.); S. 59: Fraunhofer (o.l.), Stephan Kohzer/BSI (u.l.); S. 61: Björn Wylezich/fotolia; S. 62: R. Winkler, Herrndorff/fotolia (Hand); S. 64–65: Kwangmoo/fotolia; S.66: Fink & Fuchs, Fotos iStock.com/Grafissimo; iStock.com/Krasyuk

Das BSI-Magazin erscheint zweimal im Jahr. Es ist Teil der Öffentlichkeitsarbeit des BSI.
Es wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

Für die digitale Version des BSI-Magazins scannen Sie den QR-Code
https://www.bsi.bund.de/BSI-Magazin

www.bsi.bund.de