Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Magazin 2016/02

Mit Sicherheit

Europa und Internationale Zusammenarbeit

BSI INTERNATIONAL

ANSSI: Portrait einer Zusammenarbeit

BSI INTERNATIONAL

eIDAS-Verordnung: Europaweit einheitliche Rahmenbedingungen

DAS BSI

25 Jahre BSI

EDITORIAL

„Digitalisierung und Cyber-Sicherheit sind zwei Seiten derselben Medaille.“

Liebe Leserinnen und Leser,

1990 wurde das Internet für die kommerzielle Nutzung freigegeben – ein Meilenstein in der Geschichte der IT. Seitdem hat sich das weltweite Netz zu einem Massenphänomen entwickelt, das aus unserer Lebens- und Arbeitswelt nicht mehr wegzudenken ist. In positiver wie negativer Hinsicht.

Denn im Zuge der kommerziellen Internetnutzung hat sich auch die Cyber-Kriminalität zu einem Phänomen entwickelt, das uns heute mehr denn je in Atem hält.

In Deutschland gab es eine frühe und wegweisende Antwort auf die Bedrohungen, die die neue Informationstechnologie möglicherweise mit sich bringen könnte: 1991 wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) gegründet. In den folgenden 25 Jahren hat es sich zu Deutschlands Cyber-Sicherheitsbehörde als dem zentralen Ansprechpartner für alle Themen rund um IT-Sicherheit entwickelt. Zu diesem Jubiläum lassen wir in der vorliegenden Ausgabe des BSI-Magazins Persönlichkeiten zu Wort kommen, die die Geschichte dieser Behörde geprägt und begleitet haben.

Wir feiern in diesem Jahr noch ein weiteres Jubiläum, das die rasante Entwicklung der Cyber-Kriminalität spiegelt: Vor fünf Jahren wurde das Cyber-Abwehrzentrum gegründet. Diese zentrale Kooperationsplattform bündelt die Kräfte der Sicherheitsbehörden in Deutschland. Demnächst kommen auch alle über die Betreiber der Kritischen Infrastrukturen Aufsicht führenden Stellen hinzu. Denn Cyber-Angreifer interessieren sich nicht für Verwaltungsstrukturen oder behördliche Zuständigkeiten. Darum sind Kooperationen bei der Gefahrenabwehr das A und O.

Das gilt auch über Ländergrenzen hinweg. Deshalb arbeiten Frankreich und Deutschland seit vielen Jahren im Bereich der Cyber-Sicherheit zusammen. Diese enge Kooperation mit der französischen Behörde für Sicherheit und Schutz von Informationssystemen ANSSI, basiert auf Vertrauen und gemeinsamen Ansichten zu strategischen Fragen, einer gemeinsamen Positionierung hinsichtlich der defensiven Ausrichtung und einem vergleichbar hohen technischen Know-how.

Sicher, die Allgegenwärtigkeit der Cyber-Bedrohungen kann so manches Unternehmen abschrecken, an der digitalen Transformation zu partizipieren, und so manchen Internetnutzer verängstigen. Aber auch das ist unsere Aufgabe als BSI: Ängste ernst zu nehmen und aufzuklären, wie wir uns wappnen und Schutzmaßnahmen umsetzen können. Denn Digitalisierung und Cyber-Sicherheit sind zwei Seiten derselben Medaille. Deshalb gestaltet das BSI als die nationale Cyber-Sicherheitsbehörde Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Wir unterstützen Sie bei einem sicheren Umgang mit Informationstechnologien.

Ich wünsche Ihnen eine anregende Lektüre.

Bonn, im September 2016

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik

INHALT

AKTUELLES

BSI und VW

Gemeinsam für mehr Cyber-Sicherheit

Das BSI und die Konzernsicherheit der Volkswagen AG haben eine Zusammenarbeit im Bereich der Cyber-Sicherheit vereinbart. Kern der Kooperation ist die Intensivierung des Austauschs von Informationen über Cyber-Gefährdungen. Diese Informationen fließen in das Lagebild des BSI ein. Damit tragen sie zur Darstellung der aktuellen Gefährdungen im deutschen Cyber-Raum bei und bilden eine Grundlage für Handlungsempfehlungen. Ziel ist es, gemeinsam das Lagebild Cyber-Sicherheit zu verbessern, um im Kampf gegen Cyber-Kriminelle wirkungsvoller agieren zu können. Außerdem trat die Volkswagen AG der Allianz für Cyber-Sicherheit bei.

ECSM

Europäischer Monat der Cyber-Sicherheit

Im Oktober 2016 unterstützt und koordiniert das BSI wieder den European Cyber Security Month (ECSM) in Deutschland. Unter dem Motto „Ins Internet – mit Sicherheit“ informiert das Bundesamt über die alltäglichen Gefahren der Cyber-Welt. Eigene Aktionen sowie gemeinsame Aktivitäten mit Partnern sensibilisieren Bürgerinnen und Bürger sowie Unternehmen für den verantwortungsbewussten Umgang mit dem Internet.

Seit 2012 bieten die Mitgliedstaaten der Europäischen Union unter Federführung der europäischen IT-Sicherheitsbehörde ENISA (European Union Agency for Network and Information Security) Veranstaltungen, Informationen und Aktionen zum ECSM an.

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

Ranking

BSI erneut unter den Top-Arbeitgebern

Bei der Wahl zu den besten Arbeitgebern im Bereich Informationstechnologie in Deutschland wurde das BSI auf den 15. Platz gewählt und ist damit erneut unter den Top-Arbeitgebern der Branche. Seit 1999 befragt das Forschungsinstitut trendence 5.700 Studierende der IT an 69 Hochschulen in Deutschland nach ihren Wunscharbeitgebern und Karriereplänen und hält die Ergebnisse im trendence Graduate Barometer fest.

Aktuell bietet das BSI verschiedene Bewerbungsmöglichkeiten für Fachkräfte aus den Bereichen Informatik und Mathematik sowie Ingenieurs- und Naturwissenschaften. Informationen zu aktuellen Stellenangeboten des BSI sind unter *https://www.bsi.bund.de/jobs* zu finden.

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

ViS!T in Bern

Stippvisite in der Schweiz

Das BSI hat in diesem Jahr am 8. Symposium ViS!T in Bern teilgenommen. Unter dem Motto „IT-Sicherheit in der konkreten Anwendung“ trafen sich Mitarbeiter der öffentlichen Verwaltung aus Österreich, der Schweiz, Luxemburg und Deutschland, um Themen der IT-Sicherheit multilateral zu diskutieren. Gemeinsames Ziel der beteiligten Länder ist, ein vergleichbares und wenn möglich verbindliches IT-Sicherheitsniveau erreichen zu können.

Das Symposium „Verwaltung integriert sichere Informationstechnologie (ViS!T)“ findet alle zwei Jahre abwechselnd in den beteiligten Ländern statt.

Ransomware

Bedrohungslage unverändert hoch

Im Rahmen der Allianz für Cyber-Sicherheit hat das BSI eine Umfrage zur Betroffenheit der deutschen Wirtschaft durch Ransomware durchgeführt. Die Ergebnisse verdeutlichen, wie verwundbar viele Unternehmen in Deutschland für Cyber-Angriffe sind. Demnach waren ein Drittel (32 Prozent) der befragten Unternehmen aller Größenordnungen in den letzten sechs Monaten von Ransomware betroffen. Mit teilweise erheblichen Auswirkungen: In jedem fünften der betroffenen Unternehmen (22 Prozent) kam es zu einem erheblichen Ausfall von Teilen der IT-Infrastruktur, 11 Prozent der Betroffenen erlitten einen Verlust wichtiger Daten.

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/ransomware-umfrage-2016-04.html

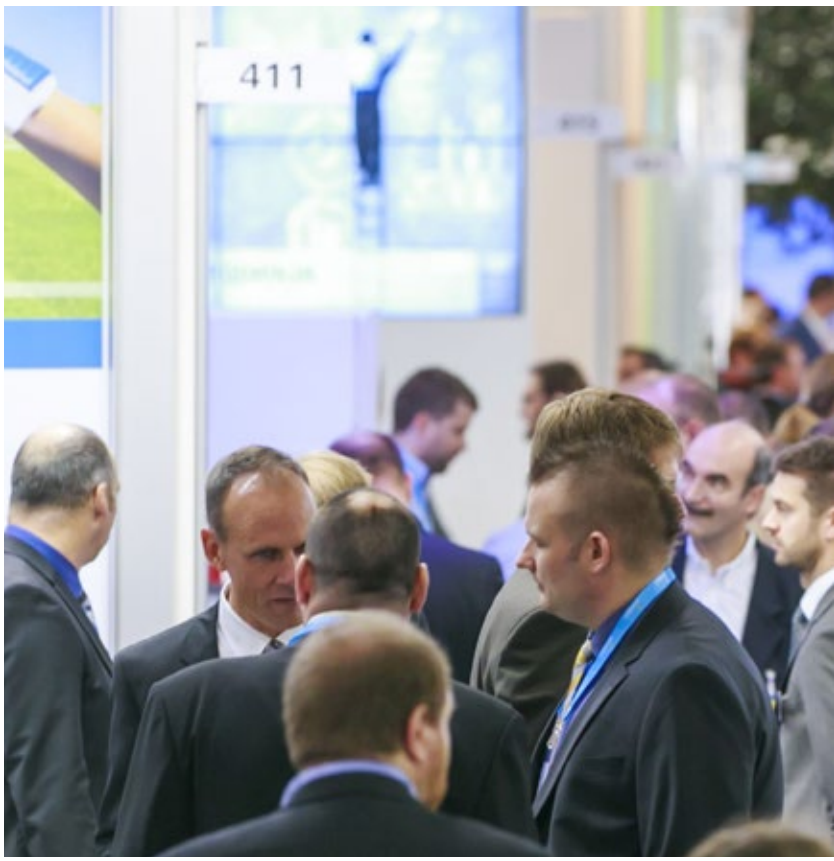
CSCG

Cyber Security Challenge Germany

Die IT-Fachkräfte von morgen zu finden und frühzeitig zu fördern ist eine der Aufgaben der Cyber Security Challenge Germany, die das BSI unterstützt. Der Wettbewerb richtet sich an Schülerinnen und Schüler sowie Studierende im Alter zwischen 14 und 30 Jahren und ist Teil einer europaweiten Initiative. Neueinsteiger und Erfahrene sind gleichermaßen gefragt. Ende September stellten die Nachwuchs-Talente im Landesfinale in Berlin ihr Können unter Beweis. Die Sieger wurden zum europäischen Finale, der European Cyber Security Challenge (ECSC), im November nach Düsseldorf eingeladen.

https://www.cscg.de

it-sa 2016



von Thomas Philipp Haas, NürnbergMesse

Das internationale Schaufenster der IT-Sicherheitsbranche

Vom 18. bis 20. Oktober 2016 steht das Messezentrum Nürnberg wieder ganz im Zeichen der IT-Sicherheit: Zur achten Ausgabe der Fachmesse it-sa werden rund 480 Aussteller erwartet, so viele wie nie zuvor. Darunter finden sich nicht nur Unternehmen und Organisationen aus Deutschland, Österreich und der Schweiz, sondern auch aus Malta, Israel und Südkorea. Die Wachstumskurve zeigt steil nach oben: So sind allein in den letzten drei Jahren etwa 100 neue Aussteller hinzugekommen. Eine wertvolle Ergänzung zur it-sa ist das Kongressprogramm Congress@it-sa. Das BSI unterstützt die it-sa als ideeller Träger von Beginn an und veranstaltet auch dieses Jahr den IT-Grundschutztag am zweiten Messetag.

„Die it-sa deckt alle Facetten der Cyber-Sicherheit ab“, so Frank Venjakob, Executive Director it-sa. IT-Sicherheitsexperten informieren sich auf der it-sa zu Produkten und Dienstleistungen und tauschen sich bei Congress@it-sa zu aktuellen IT-Sicherheitsfragen aus. Thematisch deckt die Veranstaltung von der Authentifizierung bis zur Zertifizierung das komplette ABC der verfügbaren IT-Sicherheitstechnologien ab und ist Bühne für Beratungs- und Schulungsunternehmen. Sonderflächen für Start-ups, zur IT-Sicherheit bei Planung, Bau und Betrieb von Rechenzentren sowie zu Identity und Access Management komplettieren das Ausstellungsangebot. Damit ist die it-sa nicht nur europaweit führend, sondern hat sich zu einer der weltweit bedeutendsten IT-Sicherheitsveranstaltungen mit zuletzt über 9.000 Besuchern entwickelt.

GEMEINSCHAFTSSTÄNDE AUS ISRAEL UND FRANKREICH

Die diesjährige Messe zeigt einmal mehr ihre internationale Bedeutung: Erstmals beteiligen sich Israel und Frankreich mit Gemeinschaftsständen. Das Nachbarland rangiert, gemessen am Importvolumen, an dritter Stelle der bundesdeutschen Außenhandelsbilanz. Die Start-up-Nation Israel repräsentieren insgesamt 17 Unternehmen auf der it-sa.

GRÜN, ROT UND BLAU: UMFASSENDES FORENPROGRAMM ZU ALLEN SICHERHEITSTHEMEN

Grün, rot und blau – seit der Erstveranstaltung 2009 stehen diese Farben für die offenen Foren im Rahmenprogramm der it-sa. In über 230 Sessions und Themenblöcken informieren Unternehmen, Verbände und Organisationen auf drei Vortragsbühnen, die sich mitten im Messegeschehen befinden. Dabei stehen aktuelle Entwicklungen der IT-Sicherheit im Mittelpunkt. Auch das BSI ist am 19. Oktober mit einem Referenten zum Thema Cyber-Sicherheit in der Wirtschaft vertreten. Die Präsentationen im Forum Blau setzen den Schwerpunkt auf praxisbezogene Lösungen und Technologien für einer sichere IT- und Daten-Infrastruktur. CEOs, CIOs und IT-Verantwortliche finden Antworten auf strategische und wirtschaftliche Fragen im Forum Rot. Zu den Höhepunkten im Forenprogramm zählt die Paneldiskussion zu aktuellen Entwicklungen bezüglich des FIDO (Fast IDentity Online)-Authentifizierungsstandards und ein Schwerpunkt zur EU-Datenschutz-Grundverordnung.

IT-GRUNDSCHUTZTAG GEHT AUF DER IT-SA IN DIE NÄCHSTE RUNDE

Abseits des lebhaften Messegeschehens bietet das begleitende Kongressprogramm den Rahmen für intensive Expertendialoge. Auch der 4. IT-Grundschutztag findet wieder in Nürnberg und unter dem Dach von Congress@it-sa statt. Vorgestellt werden am 19. Oktober unter anderem die Bausteine der 15. Ergänzungslieferung der IT-Grundschutz-Kataloge. Außerdem auf der Agenda: die Modernisierung des IT-Grundschutzes. ■

DAS BSI AUF DER IT-SA

Vom 18. bis 20. Oktober 2016 im Messezentrum Nürnberg

Mehr Informationen über alle Aussteller, ihre Produkte, den Hallenplan, die App und zu allen Kongress- und Forenvorträgen finden Sie online unter: https://www.it-sa.de

BSI INTERNATIONAL

eIDAS

von Jens Bender, Leiter des Referats eID-Technologien und Chipkarten

Um einen echten europäischen Binnenmarkt auch im digitalen Raum herzustellen, hat die EU mit der eIDAS-Verordnung einheitliche Rahmenbedingungen geschaffen. Elektronische Geschäfts- und Kommunikationsprozesse zwischen Bürgern, Unternehmen und Behörden können nun auch länderübergreifend vertrauenswürdig, rechtsverbindlich und vor allem sicher durchgeführt werden.

Mehr Vertrauen in den digitalen Binnenmarkt

Seit dem 1. Juli 2016 können Verbraucher europaweit leichter elektronische Verträge im Internet unterschreiben: Mit der neuen EU-Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS-Verordnung) werden grenzüberschreitende digitale Vorgänge einfacher. Denn elektronische Signaturen, Siegel und Zeitstempel sowie die Zustellung elektronischer Einschreiben und die gegenseitige Anerkennung elektronischer Identifizierungsmittel sind nun für den gesamten Europäischen Wirtschaftsraum (EWR) einheitlich geregelt. Hinzu kommt eine neue Kategorie von qualifizierten Webseitenzertifikaten.

Die eIDAS-Verordnung setzt das deutsche Signaturgesetz nicht außer Kraft, sie besitzt jedoch Vorrang. Um hier mehr Klarheit zu schaffen, plant das Bundesministerium für Wirtschaft und Energie (BMWi) ein Vertrauensdienstegesetz (VDG), um das bekannte Signaturgesetz abzulösen.

MEHR VERTRAUENSDIENSTE

Als Vertrauensdienste werden verschiedene Dienste zusammengefasst, die das Vertrauen der Bürger und der Wirtschaft in die technische und juristische Sicherheit grenzüberschreitender digitaler Prozesse sicherstellen sollen. Dazu gehören qualifizierte elektronische Signaturen und Zeitstempel. Neu sind qualifizierte elektronische Siegel für Unternehmen und Behörden, die qualifizierte Zustellung elektronischer Einschreiben (wie etwa De-Mail) sowie qualifizierte Zertifikate für die Webseitenauthentifizierung.

Die Einordnung von Vertrauensdiensten und der verschiedenen Methoden zur elektronischen Identifizierung in verschiedene Vertrauensniveaus hat das BSI in der TR-03107-1 „Elektronische Identitäten und Vertrauensdienste im E-Government – Vertrauensniveaus und Mechanismen“ beschrieben.

Mit der eIDAS-Verordnung über diese Vertrauensdienste soll das Handeln im elektronischen Binnenmarkt rechtssicher und auf dem gleichen Vertrauensniveau wie traditionelle papierbasierte Verfahren möglich werden. Die Voraussetzungen dafür sind geeignete Sicherheits- und Interoperabilitätsstandards, die Überprüfung der Einhaltung der Vorgaben durch Audits, Zertifizierungen und Aufsicht über die Anbieter sowie die Festlegung der Rechtswirkung der verschiedenen Dienste.

Während die Rechtswirkung der Dienste in der Verordnung selbst festgelegt ist, werden die Standards den Normungsorganisationen (CEN, ETSI, ISO, ...) überlassen. Für viele Bereiche stellt das BSI eigene technische Richtlinien bereit (z.B. die TR-03145 „Secure CA Operation“) und nimmt aktiv an der Standardisierung teil.

Die Aufsicht über die Vertrauensdiensteanbieter wird durch nationale Stellen übernommen. Hier hat das BMWi die Bundesnetzagentur für die Bereiche Signatur, Siegel, Zeitstempel und Zustelldienste an die EU-Kommission gemeldet, für Webseitenzertifikate das BSI. Anwender erkennen die qualifizierten Vertrauensdienste am einheitlichen EU-Vertrauenssiegel auf den Anbieter-Webseiten.

FERNSIGNATUREN UND WEBSEITENZERTIFIKATE

Bisher war für eine qualifizierte elektronische Signatur in Deutschland immer eine Signaturkarte notwendig. eIDAS ermöglicht nun auch eine sogenannte *Fernsignatur* (oder *Serversignatur*). Diese erlaubt es, den persönlichen Signaturschlüssel bei einem Vertrauensdiensteanbieter zu verwahren und durch diesen Dokumente signieren zu lassen. Davon profitieren besonders Anwender, die nur selten Signaturen nutzen.

Um den Sicherheitsanforderungen (z. B. die Authentizität des Anwenders sicherzustellen) gerecht zu werden, erstellte das Europäische Komitee für Normung (CEN) unter Mitarbeit des BSI entsprechende Richtlinien und Schutzprofile für die Vertrauensdiensteanbieter. Als eine Komponente wird hier eine sichere 2-Faktor-Authentisierung gefordert – in Deutschland bietet sich dafür die eID-Funktion des Personalausweises an.

Weiterhin wird für SSL/TLS-Webseitenzertifikate die Kategorie der *qualifizierten Webseitenzertifikate* eingeführt, um ein höheres Vertrauen in die Zertifikate zu erreichen.

DER PERSONALAUSWEIS ÜBERWINDET GRENZEN

Auch bei der elektronischen Identifizierung zielt die eIDAS-Verordnung auf die einfache, grenzüberschreitende Nutzung. Bereits seit Langem ermöglicht der Personalausweis das grenzüberschreitende Reisen innerhalb Europas – aber auch die Online-Ausweisfunktion ist eine sichere Grundlage für die Nutzung elektronischer Dienste.

Anderseits existieren auch in anderen EU-Mitgliedsstaaten bereits nationale eID-Systeme. Daher werden diese nicht durch ein einheitliches ersetzt, sondern die eIDAS-Verordnung zielt darauf ab, Interoperabilität zwischen den nationalen Systemen zu schaffen.

Die eIDAS-Verordnung regelt die für die gegenseitige Anerkennung erforderlichen Rahmenbedingungen. Die Mitgliedsstaaten können ihre nationalen eID-Systeme bei der Kommission notifizieren. Während die Notifizierung auf freiwilliger Basis erfolgt, ist die Anerkennung notifizierter eIDs (für den öffentlichen Sektor) ab dem 29. September 2018 verpflichtend.

Dabei richtet sich die Wahl der Identifizierungsmittel nach dem jeweils benötigten Vertrauensniveau eines Dienstes. Je höher dieses Niveau, desto sicherer muss das eID-System sein.

Die grenzüberschreitende Interoperabilität wird durch das *Interoperability-Framework* realisiert, welches von den Mitgliedstaaten – Deutschland vertreten durch das BSI – spezifiziert wurde. Es kann sicher und flexibel in die jeweiligen Systeme der Mitgliedsstaaten integriert werden und zwischen diesen übersetzen.

Deutsche Behörden müssen nun die Voraussetzungen dafür schaffen, dass Bürger und Unternehmen aller EWR-Staaten die heimatlichen (notifizierten) eIDs gegenüber deutschen Verwaltungsdienstleistungen nutzen können.

Auf der anderen Seite können sich Inhaber des elektronischen Aufenthaltstitels oder Personalausweises künftig mittels der eID-Funktion auch gegenüber Behörden und Diensteanbietern anderer EWR-Staaten einfach und sicher elektronisch identifizieren. Hierbei erfüllt die eID-Funktion des Personalausweises alle Voraussetzungen für die Notifizierung auf höchstem Vertrauensniveau.

Das BSI hat – zusammen mit Partnern aus der Industrie – die technischen Vorarbeiten für die Integration des Personalausweises in die Systeme anderer Mitgliedstaaten geleistet. Die ersten Testprojekte mit anderen EU-Ländern laufen bereits. ■

https://www.bsi.bund.de/eidas-vo

https://www.personalausweisportal.de/DE/Verwaltung/eIDAS_Verordnung_EU/eIDAS_Verordnung_EU_node.html

GEMEINSAM FÜR EIN SICHERES DIGITALES EUROPA

von Dr. Guillaume Poupard, Generaldirektor der französischen Cyber-Sicherheitsbehörde ANSSI

Frankreich und Deutschland kooperieren bei Cyber-Abwehr

In den letzten Jahren haben sich komplexe Cyber-Attacken immer mehr gehäuft. Frankreich beschloss daher bereits vor etwa zehn Jahren, seine technischen und operativen Fähigkeiten auszubauen, um diesen Bedrohungen sowohl auf nationaler als auch internationaler Ebene entgegentreten zu können.

2008 erfolgte die Veröffentlichung eines Weißbuchs zur Verteidigung und nationalen Sicherheit, das konstatierte, dass Informations- und Kommunikationssysteme unverzichtbar seien für das reibungslose Funktionieren der Gesellschaft. Aufgrund der wachsenden Abhängigkeit von diesen Systemen rückten in der Folge Prävention und Reaktion auf Cyber-Attacken in der Organisation und Planung der nationalen Sicherheit deutlich stärker in den Fokus.

Diese strategische Neuorientierung resultierte 2009 in der Gründung der Agence nationale de la sécurité des systèmes d'information (ANSSI). Als nationale Behörde für Sicherheit und Schutz von Informationssystemen lautet ihr Ziel, koordinierte, umfassende und proaktive Reaktionen auf die Cyber-Bedrohungen des Landes voranzutreiben.

Die erzielten Erfahrungen und die Zusammenarbeit mit wichtigen Netzbetreibern bewogen die französische Regierung, 2013 ein gesetzliches Rahmenwerk zum Schutz kritischer Informationsinfrastrukturen zu verabschieden. Zielsetzung war, in allen wichtigen Bereichen ein gemeinsames Mindestmaß der Cyber-Sicherheit zu etablieren. Das Gesetz betrifft heute mehr als 200 öffentliche und private Betreiber und legte fest, dass bestimmte Sicherheitsmaßnahmen zum Schutz der wichtigsten Informationssysteme zu treffen sind. Außerdem durften nur zugelassene Service-Provider mit Audits sowie der Aufdeckung, Bearbeitung und Behebung von Vorfällen beauftragt werden.

Die Cyber-Sicherheit der öffentlichen Verwaltung und der Netzbetreiber genießt weiterhin hohe Priorität in Frankreich. Allerdings haben die letzten Jahre gezeigt, dass das Thema heute nicht mehr nur Regierungen und Großunternehmen, sondern vielmehr Unternehmen aller Größen in allen Bereichen der Wirtschaft sowie die Bürger selbst betrifft. Wir sind heute gefordert, auch das digitale Leben der Bürger, ihre Privatsphäre und ihre persönlichen Daten zu schützen. Entsprechend startet Frankreich in Kürze eine neue Plattform zur Unterstützung der Opfer von bösartigen

Kurzprofil Dr. Guillaume Poupard

Dr. Guillaume Poupard ist seit März 2014 Generaldirektor der französischen Cyber-Sicherheitsbehörde ANSSI (Agence nationale de la sécurité des systèmes d'information). Zuvor war der promovierte Kryptograph im französischen Verteidigungsministerium sowie in der Beschaffungsbehörde DGA im Bereich Cyber-Security tätig.

Cyber-Angriffen. Diese öffentlich-private Partnerschaft soll verschiedene Aufgaben erfüllen, sei es die Unterstützung der Bürger sowie kleinerer und mittlerer Unternehmen und regionaler Behörden beim Erkennen ihrer Sicherheitsprobleme, die Bereitstellung einer Liste mit Service-Providern oder die Sensibilisierung der Öffentlichkeit.

Aktuell erarbeiten die 500 ANSSI-Experten eine breite Palette von regulatorischen und operativen Aktivitäten. Dies reicht von der Veröffentlichung von Vorschriften und der Überprüfung ihrer Genehmigung über die Zertifizierung und Akkreditierung von Produkten und Service-Providern bis hin zur Überwachung von Netzwerken und der Reaktion auf schwerwiegende Vorfälle.

ZUSAMMENARBEIT IM CYBERSPACE ENTSCHEIDEND

In einer zunehmend vernetzten Welt ist es für einen Staat wenig sinnvoll, seine digitalen Sicherheitsprobleme allein bewältigen zu wollen. Die neue französische Strategie für die digitale Sicherheit, die der französische Premierminister im Oktober 2015 vorgestellt hat, unterstreicht den Willen des Landes, den Dialog mit multilateralen Organisationen und vertrauenswürdigen Partnern zu intensivieren. Damit soll einerseits ein Beitrag zur globalen Stabilität des Cyberspace geleistet, aber auch die Cyber-Sicherheit des eigenen Landes gestärkt werden.

Deutschland ist in vielen Bereichen, einschließlich Cyber-Sicherheit, einer der stärksten und selbstverständlichsten Verbündeten Frankreichs. Die langjährige und enge bilaterale Zusammenarbeit zwischen ANSSI und BSI basiert auf Vertrauen und wird erheblich erleichtert durch gemeinsame Ansichten zu zahlreichen strategischen und politischen Fragen, eine gemeinsame Positionierung hinsichtlich der defensiven Ausrichtung und ein vergleichbar hohes technisches Know-how. Das 25-jährige Jubiläum des BSI ist beispielhaft für die lange Geschichte, die wir auf dem Gebiet der Cyber-Sicherheit bereits gemeinsam hinter uns gebracht haben.

Die digitale Sicherheit beschäftigt immer mehr Akteure. Auch unsere tägliche Arbeit hat sich erweitert und ist nicht mehr auf die Entwicklung technischer und operativer Kapazitäten beschränkt. Vielmehr geht es heute darum, effiziente Governance-Modelle zu definieren, angemessene Regelungen einzuführen oder auch den Dialog mit den zuständigen öffentlichen Einrichtungen und privaten Interessengruppen zu führen. Auch die Zusammenarbeit mit anderen Ländern und multilateralen Organisationen, angefangen bei der Europäischen Union (EU), zählt dazu. In anderen Worten: Alle verfügbaren Hebel müssen bewegt werden, um die digitale Sicherheit des Landes als Ganzes zu sichern.

Die kürzlich erfolgte Verabschiedung der EU-Richtlinie für Netz- und Informationssicherheit (Network and Information Security – NIS) ermöglicht in diesem Sinn ein gemeinsames Mindestsicherheitsniveau für digitale Technologien, Netze und Dienste in allen Mitgliedstaaten und gewährleistet somit das reibungslose Funktionieren des EU-Binnenmarkts.

Unterstützt vom französischen Präsidenten François Hollande und Bundeskanzlerin Angela Merkel arbeiten ANSSI und BSI in vielen Bereichen zusammen, etwa bei der Zertifizierung der Sicherheit des Cloud Computings und der Schaffung eines gemeinsamen Labels für sichere Cloud-Service-Provider auf Basis internationaler IT-Sicherheitszertifikate (CCRA

und SOG-IS) oder beim Erkunden industrieller Synergien im Rahmen eines Meetings am Rande des letzten Internationalen Forums für Cyber-Sicherheit in Lille (Forum International de la Cybersécurité – FIC). Um auf diesen Erfolgen aufzubauen, werden wir in Zukunft noch intensiver zusammenarbeiten, um die Cyber-Sicherheit in Frankreich und Deutschland und innerhalb der Europäischen Union weiter zu verbessern.

AUF DEM WEG ZUR STRATEGISCHEN AUTONOMIE EUROPAS IM DIGITALEN BEREICH

Auch wenn die Mitgliedstaaten in erster Linie selbst für ihre nationale digitale Sicherheit verantwortlich sind, teilen Frankreich und Deutschland die Vision, dass viele Herausforderungen am besten durch gemeinsame und koordinierte Anstrengungen auf europäischer Ebene angegangen werden.

Über die Entwicklung der Kapazitäten und Kooperationen der EU-Mitgliedstaaten hinaus muss die EU erkennen, dass die digitale Sicherheit Europas an vielen Fronten herausgefordert wird. Dies erfordert kollektive Anstrengungen, um die digitale Souveränität Europas zu gewährleisten. Drei Herausforderungen haben sich hier herauskristallisiert:

1. Die Fähigkeit der EU und der Mitgliedstaaten, die Institutionen, die Verwaltungen, die kritischen Infrastrukturen, die Unternehmen und die allgemeine Öffentlichkeit im Cyberspace zu schützen und zu verteidigen, muss gewährleistet sein.

2. muss die EU aktiv die Entwicklung einer nachhaltigen europäischen Industrie auf dem Gebiet der digitalen Sicherheit unterstützen und die Fähigkeit der Mitgliedsstaaten gewährleisten, die Sicherheit von digitalen Produkten und Dienstleistungen zu bewerten und zu genehmigen.

3. muss die EU ihre Fähigkeit bewahren, autonom zu entscheiden, wie Daten und damit verbundene Dienstleistungen in Europa geschützt werden sollen.

Mit gleichgesinnten Mitgliedstaaten werden Frankreich und Deutschland eng zusammenarbeiten, um die strategische Unabhängigkeit der EU im digitalen Zeitalter als langfristigen Garant für einen Cyberspace zu fördern, der sicher ist und unsere Werte respektiert.

AKTUELLE ERKLÄRUNG DES DEUTSCH-FRANZÖSISCHEN VERTEIDIGUNGS- UND SICHERHEITSRATS (DFVSR) (4.7.16):

Deutschland und Frankreich verfolgen gemeinsam das Ziel der strategischen Unabhängigkeit der EU im digitalen Zeitalter, die sich auf folgende Schritte gründet:

1. Stärkung der Fähigkeit der Mitgliedstaaten und der EU insgesamt, ihre Netze zu schützen und ihre digitale Resilienz zu erhöhen, und zwar durch den gemeinsamen Aufruf, die NIS-Richtlinie [Network and Information Security] schnell umzusetzen;

2. Entwicklung einer unabhängigen, innovativen, wirksamen und diversifizierten europäischen Industrie insbesondere im Bereich Vertrauensbildung im digitalen Umfeld und Cyber-Sicherheit;

3. Gewährleistung der Fähigkeit der Europäer, unabhängig über die Sicherheitsstufe ihrer Daten zu entscheiden, insbesondere im Zusammenhang mit der Aushandlung von Handelsabkommen.

Deutschland und Frankreich haben auf diesem Gebiet mehrere Initiativen ergriffen, etwa durch gemeinsame Anstrengungen bei der Zertifizierung der Sicherheit von Cloud Computing oder der Sicherheit von E-Mails, die Organisation eines „Speed-Datings“ zwischen deutschen und französischen im Bereich Cyber-Sicherheit tätigen KMU am Rande des Internationalen Forums für Cyber-Sicherheit in Lille im Januar 2016 oder auch durch ihre gemeinsame Arbeit zur internationalen Cyber-Sicherheit auf diplomatischer Ebene, insbesondere in den Vereinten Nationen, der OSZE, der EU und der NATO.

ANSSI IN ZAHLEN

500 Experten aktuell – **100** neue Mitarbeiter geplant für 2016

Veröffentlichung von über **20** technischen Publikationen in 2015

150 Veranstaltungen zur Sensibilisierung in 2015

Bearbeitung von knapp **30** großen IT-Angriffen in Frankreich in 2015

Schulung von **1.500** staatlichen Angestellten im Umgang mit IT-Sicherheitsproblemen jährlich

Weitere Informationen:
http://www.ssi.gouv.fr/en/

Der Weg zum neuen ANSSI-BSI Cloud Label

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

Wie auf der Basis von Vertrauen und Expertise eine neue europäische Initiative entsteht

ANSSI (Agence nationale de la sécurité des systèmes d`information) und das BSI haben sich in den letzten Jahren sehr intensiv mit der Sicherheit von Cloud Computing beschäftigt. Beide Behörden gelangten zu einem sehr ähnlichen Verständnis für die Anforderungen an Cloud-Sicherheit und initiierten jeweils neue Nachweise für ein sicheres Cloud Computing, da die existierenden Zertifizierungen die Anforderungen nicht ausreichend abdeckten. Allerdings haben beide Behörden unterschiedliche Wege eingeschlagen.

AUDITIERUNG DURCH WIRTSCHAFTSPRÜFER

Das BSI entwickelte den Cloud Computing Compliance Controls Catalogue (C5). Dieser Katalog, eng an erprobte Standards angelegt, definiert Anforderungen für die sichere Erbringung geschäftskritischer Dienste, die der Cloud-Anbieter alle erfüllen muss. Zudem muss er wichtige Parameter seines Angebots transparent machen, wie die Lokalisation der Datenverarbeitung und der Unterauftragnehmer. Die Auditierung richtet sich nach dem international anerkannten Standard ISAE 3000. Der Audit-Bericht lehnt sich an Standards wie ISAE 3402 und SOC 2 an. Wirtschaftsprüfer und Cloud-Experten führen diese Auditierung durch und vergeben ein Testat, für das der Wirtschaftsprüfer haftet. Der C5 enthält zusätzlich Anforderungen für höheren Schutzbedarf und lässt sich individuell – zum Beispiel für eine bestimmte Branche – erweitern. Das BSI stellt die Anforderungen auf und legt Kriterien für die Auditierung fest, hat aber keine weitere Aufsicht über konkrete Verfahren.

ANSSI ZERTIFIZIERT SELBST

Ganz anders die ANSSI. Das Référentiel SecNumCloud, das sich stark an der Norm ISO/IEC 27001 orientiert und diese um einige Vorgaben erweitert, definiert die Anforderungen an sicheres Cloud Computing. Im Référentiel gibt es zwei Niveaus: sécure und sécure plus, wobei letzteres höhere Sicherheitsanforderungen stellt und die Service-Erbringung auf Frankreich beschränkt. Darauf aufbauend hat die ANSSI eine komplett neue, eigene Zertifizierung entwickelt und in Frankreich etabliert. Cloud-Anbieter bekommen ein Zertifikat, das von der ANSSI ausgestellt wird und auf einem Audit-Bericht von ANSSI-zertifizierten Auditoren basiert.

EIN GEMEINSAMES CLOUD LABEL ENTSTEHT

Das von BSI und ANSSI angestrebte Sicherheitsniveau ist sehr ähnlich, die beiden sehr unterschiedlichen Ansätze zur Zertifizierung und Testierung scheinen sich jedoch konträr gegenüberzustehen.

Motiviert durch deutsch-französische Wirtschaftskonsultationen und basierend auf dem großen, gegenseitigen Vertrauen entstand daher die Idee, ein neues Cloud Label zu schaffen. Es steht für die gemeinsamen Anforderungen zur Cloud-Sicherheit und einen geeigneten Nachweis. Dem Label zugrunde liegt ein gemeinsamer, kurzer Katalog mit Sicherheitszielen („core rules“). Die Testierung nach C5 des BSI und die ANSSI-Zertifizierung genügen natürlich diesen Ansprüchen. Ein Anbieter, der bereits eine der beiden Zertifizierungen hat, kann dieses Label erhalten, und damit auf beiden Märkten sehr leicht mit dem Sicherheitsniveau seines Produkts werben.

Das Cloud Label wird von ANSSI und BSI explizit als europäische Initiative gesehen, in die auch Zertifizierungen anderer Länder aufgenommen werden können. Expertise und Unabhängigkeit von BSI und ANSSI und die vertrauensvolle Zusammenarbeit werden so für ganz Europa gewinnbringend. ■

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

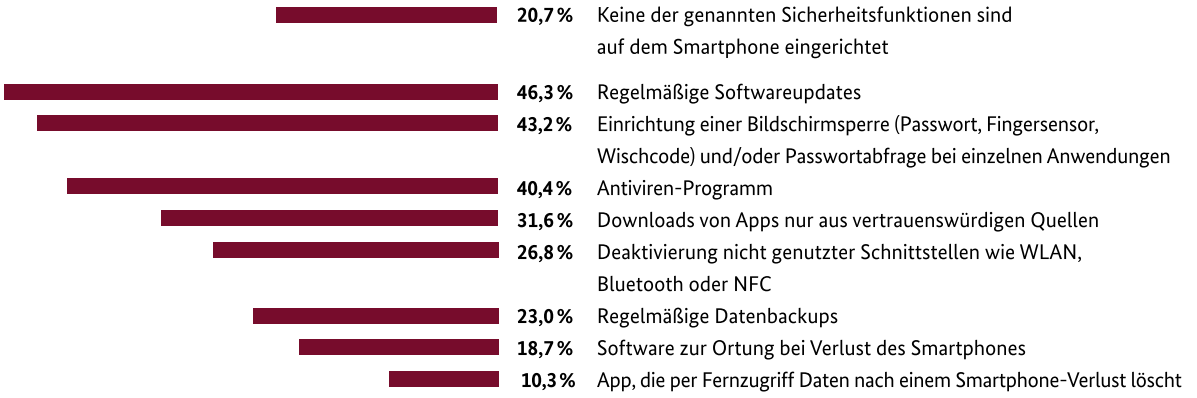
CYBER-SICHERHEIT

Der gläserne Smartphone-Nutzer

Mehrheit der Deutschen setzt sich Sicherheitsrisiken aus

JEDER FÜNFTE SMARTPHONE-NUTZER OHNE SICHERHEITSSCHUTZ

Welche Sicherheitsfunktionen nutzen Sie auf Ihrem Smartphone?



JÜNGERE GENERATION IST VORSICHTIGER BEIM UMGANG MIT SMARTPHONES

92,5 %

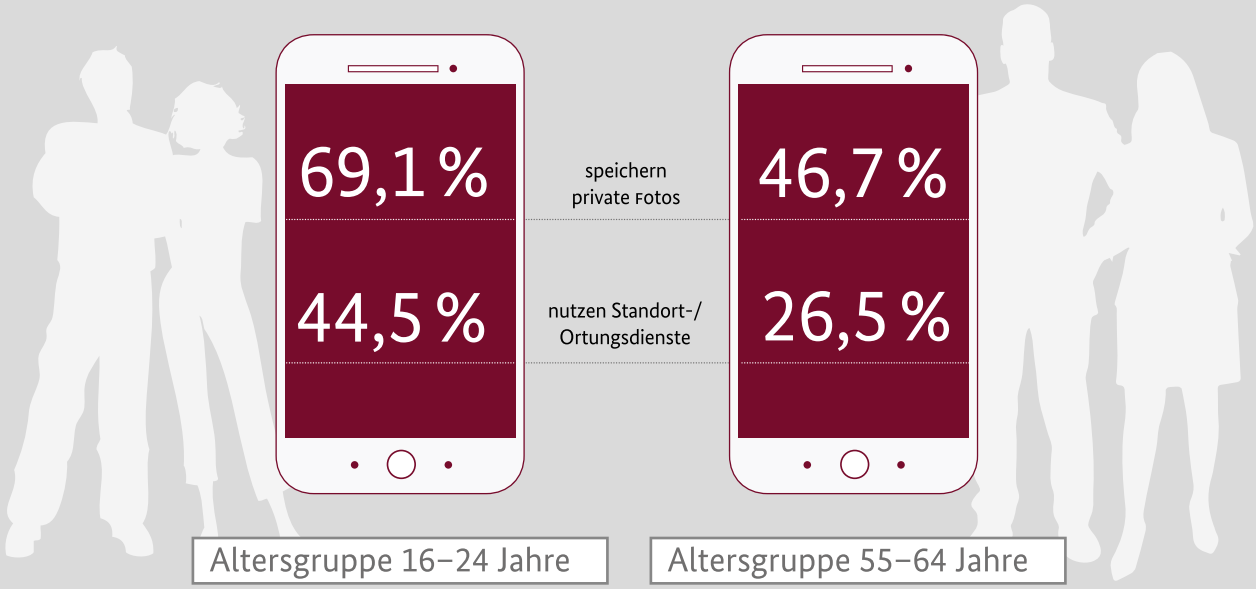
der 16- bis 24-Jährigen bestätigen, dass sie eine oder mehrere der genannten Sicherheitsfunktionen einsetzen

66,8 %

der 55- bis 64-Jährigen bestätigen, dass sie eine oder mehrere der genannten Sicherheitsfunktionen einsetzen

Quelle: Repräsentative Online-Befragung durch TNS Infratest GmbH im Auftrag des BSI.

JE JÜNGER DER SMARTPHONE-NUTZER, DESTO MEHR SENSIBLE DATEN WERDEN AUF DEM SMARTPHONE GESPEICHERT



SENSIBLE DATEN

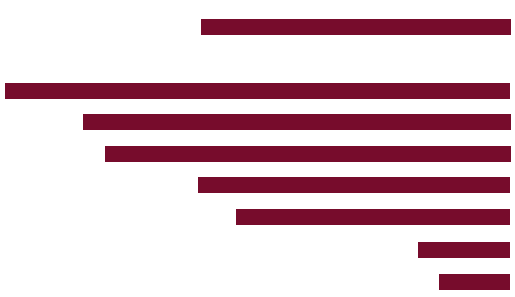
Welche Daten speichern Sie auf Ihrem Smartphone?

FRAGILE

25,4 %	Keine sensiblen Daten auf dem Smartphone
57,8 %	Private Bilder und/oder Videos
47,9 %	Kontaktdaten und private Adressen
30,4 %	Standort-/Ortungsdienste
29,8 %	Direktzugriff auf private Nutzerkonten (z.B. E-Mail-Programme/ Facebook/Cloud) ohne eingerichteten gesonderten Login
19,7 %	Apps, mit denen persönliche Daten erfasst werden (z.B. zu Sportaktivitäten oder Gesundheit)
11,5 %	Passwörter
7,3 %	Zugangsdaten zum Onlinebanking

FREIWILLIGE ÜBERWACHUNG DURCH DAS SMARTPHONE

Was, denken Sie, weiß Ihr Smartphone über Sie?



29,4%	Nichts
48,0 %	Standortdaten
40,6 %	Freundschaften
38,5 %	Lieblingswebseiten
29,6 %	Persönliche Interessen und Hobbies
26,0 %	Vollständiges Bewegungsprofil
8,7 %	Gesundheitszustand
6,7 %	Höhe des Gehalts / Vermögenssituation

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

„Das deutsche Prüfschema genießt weltweit einen exzellenten Ruf“

Interview mit Dr. Markus Mackenbrock

Nicht nur das BSI begeht 2016 sein 25-jähriges Jubiläum. Auch Zertifizierungen kommen seit einem Vierteljahrhundert aus dem Haus. Zwischen dem ersten erteilten Zertifikat und dem heutigen Tag liegen über 1.000 abgeschlossene Zertifizierungsverfahren. Dr. Markus Mackenbrock, Leiter des Referats für die Anerkennung sachverständiger Stellen und Qualitätsmanagement im BSI, hat Einblick in diesen speziellen Aufgabenbereich des BSI gewährt.

Das BSI fungiert als zentrale Zertifizierungsstelle für die IT-Sicherheit in Deutschland. Das klingt nach sehr viel Arbeit. Wie ist das BSI hier aufgestellt?

Das BSI ist für die Prüfungsverfahren zum Glück nicht allein zuständig. Vielmehr übernehmen die Prüfung der Produkte nach den definierten Prüfschemata derzeit bundesweit neun Prüfstellen, die gemäß den Vorgaben des BSI ein Anerkennungsverfahren durchlaufen haben und speziell im Bereich Common Criteria (CC) für das BSI diese Aufgaben wahrnehmen. Common Criteria ist eine anerkannte internationale Norm zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten. Der Ruf unserer Zertifikate ist weltweit exzellent, sodass viele ausländische Produkthersteller die CC-Zertifizierung bei uns beantragen – auch weil wir besonders zügig und kundenorientiert arbeiten.

Neben Common Criteria existieren weitere Standards. Wie unterscheiden sich diese, wo liegen die Anwendungsgebiete?

Common Criteria bezieht sich ausschließlich auf Sicherheitseigenschaften von

Kurzprofil Dr. Markus Mackenbrock

Dr. Markus Mackenbrock ist seit 1993 beim BSI beschäftigt und hat die ersten 10 Jahre der Entwicklung der Common Criteria (CC) maßgeblich mitgestaltet. Heute ist er für die Anerkennung von CC- Prüfstellen sowie für die Ausbildung von CC-Evaluatoren verantwortlich.

Produkten, bei den Technischen Richtlinien stehen die Funktionalität und Interoperabilität im Fokus. Die internationale Norm ISO/IEC 27001 beschreibt ein ISMS (Managementsystem für Informationssicherheit) für einen in sich abgeschlossenen Verbund wie ein Rechenzentrum oder eine IT-Abteilung. Darüber hinaus zertifizieren wir auch Auditoren und IT-Sicherheitsdienstleistungen. Hier gibt es viel Entwicklungspotenzial, da der Markt für IT-Sicherheitsdienstleistungen in Zeiten steigender Cyber-Bedrohungen stark wächst.

In 25 Jahren hat sich in der IT-Welt ja sehr vieles grundlegend verändert. Das trifft sicherlich auch auf die Zertifizierungen zu?

Verändert hat sich vor allem die Komplexität der zu zertifizierenden Produkte und damit einhergehend die geforderte Prüftiefe. Wir haben es heute oft mit zusammengesetzten Produkten zu tun, deren einzelne Komponenten zertifiziert werden sollen, also beispielsweise Hardware, Betriebssystem und Anwendung. Ziel ist dann ein Zertifikat für das komplette zusammengesetzte Produkt. In der Anfangszeit war das anders, da ging es im Wesentlichen nur um das Betriebssystem oder die Anwendung. Auch der Aufwand für die Prüfungen selbst hat sich vergrößert, da heute höhere Prüftiefen gefordert sind; das hängt unter anderem mit den vielfältigeren Möglichkeiten, ein Produkt anzugreifen, zusammen. Trotz allem vergeben wir heute viel mehr Zertifikate, etwa hundert im Jahr – in Anfangszeiten waren es allenfalls eine Handvoll.

Gibt es auch einen Wandel bei der Art der Produkte, die Sie zertifizieren?

Sogar einen sehr großen: In der Anfangszeit wurde noch keine Hardware zertifiziert, das hat sich insbesondere mit der Einführung von Smartcards geändert. Und wir zertifizieren heute auch Endverbraucher-Produkte wie Smart Meter oder den elektronischen Personalausweis. Früher ging es – aus Verbrauchersicht – um exotische Nischenprodukte.

Derzeit dreht sich alles um die Digitalisierung. Welchen Einfluss haben diese Umwälzungen auf Ihre Arbeit und auf die Bedeutung von Zertifizierungen?

Wir entwickeln derzeit viele neue Prüfvorschriften in den Bereichen Energiewirtschaft, Gesundheit, Automotive und Kritische Infrastrukturen. Dabei sind wir in die Sicherheitsvorgaben involviert, die bereits im Entwicklungsprozess von Produkten mitgedacht werden müssen. Eine hohe Bedeutung kommt hier dem ISMS zu, da beispielsweise im Gesundheitswesen die gesamte Infrastruktur von der elektronischen Gesundheitskarte über das Lesegerät bis hin zur verschlüsselten Übertragung der sensiblen Informationen berücksichtigt werden muss. Zudem gibt es immer mehr spezialgesetzliche Forderungen nach einer BSI-Zertifizierung, etwa bei Ausweisen und der Gesundheitskarte sowie Smart Metern und digitalen Tachografen. Diese Zukunftsthemen nehmen einen wesentlichen Teil unserer Arbeit ein.

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

NEUES FUNDAMENT FÜR DEN IT-GRUNDSCHUTZ

von Katrin Alberts, Referat IT-Grundschutz

Schneller, sicherer, weiter: Das BSI macht das bewährte Managementsystem fit für die neuen Sicherheitsanforderungen

Grund genug für noch mehr Schutz: Der IT-Grundschutz ist das zentrale Managementsystem für Informationssicherheit, das das BSI bereits seit 20 Jahren der öffentlichen Verwaltung und der Wirtschaft zur Verfügung stellt. Das BSI überarbeitet die bewährte Methodik nun grundlegend. Damit soll der IT-Grundschutz künftig noch effizienter und schneller umsetzbar sein.

Grundsätzlich kann es jedes Unternehmen treffen: Ein Anbieter von Online-Spielen wird Opfer eines Hacker-Angriffs. Die Täter gelangen an vertrauliche Daten von Millionen Nutzern weltweit. Aus Sicherheitsgründen wird die Gaming-Webseite für mehrere Tage vom Netz genommen und der Vorfall untersucht. Für das Unternehmen bedeutet der Hacker-Angriff einen Imageschaden und finanzielle Einbußen.

Oder: Ein mittelständisches Unternehmen muss auf einer Fachmesse feststellen, dass ein von ihm patentiertes sehr hochwertiges Produkt von einer asiatischen Firma als ein billiges Plagiat kopiert und vorgestellt wird. Da die Umsatzschäden durch Plagiate die Existenz des Unternehmens gefährden können, ordnet die Geschäftsführung eine Überprüfung der Informationssicherheit an. Dabei werden diverse Schwachstellen entdeckt und behoben, um zukünftige Ausspähversuche abzuwenden.

VIELFÄLTIGE HERAUSFORDERUNGEN FÜR UNTERNEHMEN

Beide Szenarien haben eines gemeinsam: Sie bilden die Alltagsrealität der Informationssicherheit in Deutschland ab. Die Ursachen für die mitunter gravierenden Informationssicherheits-Vorfälle sind vielfältig: Zum einen erfolgen Weiterentwicklungen in der Informationstechnik in kürzer werdenden Innovationszyklen. Zum anderen zeichnen sich die heutigen technischen Systeme durch eine steigende Komplexität aus. Zugleich sind immer mehr Bereiche des öffentlichen Lebens sowie in der Wirtschaft einer wachsenden Abhängigkeit von funktionierender Informationstechnik ausgesetzt. Diese Umstände führen dazu, dass Cyber-Sicherheit für viele Unternehmen und Institutionen nicht mehr eine rein technische Frage des IT-Betriebs ist, sondern eine Management-Aufgabe: Auch Führungspersonen müssen sich inzwischen mit der Frage befassen, welche Auswirkungen ein Cyber-Angriff für die Institution mit sich bringt. Daneben können auch Kunden, Lieferanten und Geschäftspartner betroffen sein. Daher ist ein geplantes und organisiertes Vorgehen aller Beteiligten notwendig, um ein angemessenes und ausreichendes Sicherheitsniveau aufzubauen und aufrechtzuerhalten.

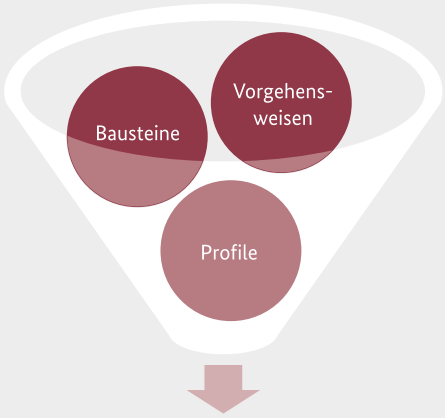
Der IT-Grundschutz trägt als etabliertes Managementsystem für Informationssicherheit den gestiegenen sowie dynamischeren Anforderungen an die Absicherung von Informationen Rechnung: Die bewährte Methode wird derzeit grundlegend überarbeitet. Ziel ist es, zu einer signifikanten Steigerung der Informationssicherheit in Verwaltung und Wirtschaft beizutragen.

IM FOKUS: MITTELSTAND

Aufgrund der sich rasant verändernden Bedrohungslage für IT-Systeme rückt das Thema Cyber-Sicherheit verstärkt in den Fokus des IT-Grundschutzes. Daher wird dort ein noch größeres Gewicht auf die Detektion von Cyber-Angriffen und die geeignete Reaktion gelegt. Zugleich sollen

künftig alle IT-Grundschutz-Veröffentlichungen – wie die bewährten Bausteine – innerhalb der gesamten IT-Grundschutz-Methodik flexibler und zügiger erstellt und veröffentlicht werden können. So wird sichergestellt, dass der IT-Grundschutz jederzeit dem Stand der Technik entspricht. Neben Behörden und größeren Wirtschaftsunternehmen sollen künftig auch kleine und mittelständische Unternehmen (KMU) stärker angesprochen werden. Aufgrund fehlender personeller und finanzieller Ressourcen sind KMU bei Informationssicherheit häufig schlechter aufgestellt als größere Institutionen.

KERNASPEKTE DER MODERNISIERUNG



NEUE VORGEHENSWEISEN ERLEICHTERN DEN EINSTIEG

Institutionen können künftig zwischen drei Vorgehensweisen auswählen:

1. Bei der Basis-Absicherung handelt es sich um eine grundlegende Absicherung der Geschäftsprozesse und Ressourcen einer Institution. Sie ermöglicht einen ersten Einstieg in den Sicherheitsprozess, um schnellstmöglich die größten Risiken zu senken. Im nächsten Schritt können die tatsächlichen Sicherheitsanforderungen im Detail analysiert werden. Diese Vorgehensweise ist daher besonders für KMU geeignet.
2. Die Kern-Absicherung dient als weitere Einstiegsvorgehensweise dem Schutz der essenziellen Geschäftsprozesse und Ressourcen. Diese Vorgehensweise unterscheidet sich vom klassischen IT-Grundschutz durch die Fokussierung auf einen kleinen, aber sehr wichtigen Teil eines Informationsverbundes.
3. Die vom BSI präferierte Standard-Absicherung entspricht in den Grundzügen der bekannten IT-Grundschutz-Vorgehensweise nach dem aktuellen BSI-Standard 100-2. Bei der Neukonzeption des IT-Grundschutzes ist zudem vorgesehen, ein noch breiteres Themenspektrum abzudecken. Dazu wurden u.a. Automatisierungs-, Prozesssteuerungs- und Prozessleitsysteme (Industrial Control Systems, ICS) sowie Detektion und Reaktion aufgenommen.

ZIEL: SICHERHEITSSTANDARDS FÜR BRANCHEN

Eine weitere Neuheit stellen die sogenannten IT-Grundschutz-Profile dar. Mit ihnen stellt das BSI ein flexibles Angebot bereit, mit dem Anwendergruppen den IT-Grundschutz an ihre konkreten Bedürfnisse anpassen und anschließend für weitere interessierte Nutzer veröffentlichen können. Im nächsten Schritt liefern die IT-Grundschutz-Profile die Grundlage, um branchenspezifische Sicherheitsstandards entwickeln und stetig fortschreiben zu können. Neben der Weitergabe von Know-how können sich Unternehmen und Behörden mit denselben Sicherheitsthemen vernetzen und gegenseitig von den Erfahrungen anderer Institutionen profitieren. Die neuen Angebote des IT-Grundschutzes können künftig von Institutionen jeder Größenordnung zur Absicherung ihrer Informationsverbünde genutzt werden.

TEAMWORK: ANWENDER SIND WICHTIGER TEIL DES ITERATIVEN PROZESSES

Während des komplexen Modernisierungsprozesses der IT-Grundschutzmethodik sind bereits erste Bausteine veröffentlicht worden. Diese werden nun in einem neuen Veröffentlichungsprozess als sogenannte Community Drafts auf der IT-Grundschutz-Webseite zur Kommentierung durch die IT-Grundschutz-Anwender zur Verfügung gestellt. Mit dem Input aus der Praxis können die Inhalte bis zum fertigen Baustein noch weiter optimiert werden. Die ersten Community Drafts, unter anderem zu Server-, Client- und Personalsicherheit, sind bereits zur Kommentierung veröffentlicht. Bis Ende 2016 sind rund 70 weitere Bausteine geplant. Die vielschichtige Modernisierung soll im Jahr 2017 abgeschlossen sein. Auch der modernisierte IT-Grundschutz wird weiter die Zertifizierung nach ISO 27001 unterstützen. Das BSI wird die IT-Grundschutz-Community frühzeitig darüber informieren, welche Übergangsfristen für Zertifikate gelten werden. Der Wechsel von der alten auf die neue IT-Grundschutz-Vorgehensweise wird vom BSI so konzipiert, dass die Anwender ihren individuellen Wechsel gut planen und gestalten können.

Der IT-Grundschutz des BSI leistet zur Informationssicherheit einen elementaren Beitrag zur Erhöhung des Sicherheitsniveaus in Deutschland. ■

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

GEMEINSAM ERFOLGREICH

Fünf Jahre Nationales Cyber-Abwehrzentrum

Cyber-Angreifer kümmern sich nicht um Verwaltungsstrukturen oder festgefügte behördliche Zuständigkeiten. Darum sind enge Kooperation und kontinuierliche Kommunikation bei der Gefahrenabwehr wichtig. Nur so kann im Cyber-Raum aus effektiver Detektion wirksame Prävention werden.

Diese Erkenntnis führte 2011 zur Einrichtung des Nationalen Cyber-Abwehrzentrum (Cyber-AZ). Es ist ein Kernelement der 2011 von der Bundesregierung verabschiedeten Cyber-Sicherheitsstrategie, um die operative Zusammenarbeit in der Cyber-Abwehr zu optimieren und Schutz- und Abwehrmaßnahmen zu koordinieren. Dies geschieht auf Basis eines ganzheitlichen Ansatzes, der die verschiedenen Gefährdungen im Cyber-Raum zusammenführt: Cyber-Spionage, Cyber-Ausspähung, Cyber-Terrorismus und Cyber-Crime. Das Ziel: schneller Informationsaustausch, schnelle Bewertungen und daraus abgeleitete konkrete Handlungsempfehlungen.

ENGE KOOPERATION, KLARE TRENNUNG DER BEFUGNISSE

Der Cyber-Raum umfasst alle durch das Internet weltweit erreichbaren Informationsinfrastrukturen. In Deutschland nutzen alle Bereiche des gesellschaftlichen und wirtschaftlichen Lebens die dort zur Verfügung gestellten Möglichkeiten. Staat, Kritische Infrastrukturen, Wirtschaft und Bevölkerung in Deutschland sind in einer vernetzten Welt darauf angewiesen, dass die Informations- und Kommunikationstechnik sowie das Internet störungsfrei funktionieren.

Im Cyber-AZ werden alle Informationen zu Cyber-Angriffen auf diese Informationsinfrastrukturen zusammengeführt, von denen die Sicherheitsbehörden erfahren. Alle tauschen dort ihre Erkenntnisse aus und bewerten sie. Jede Behörde aus ihrer Sicht und in ihrer Zuständigkeit.

In der zentralen Kooperationseinrichtung deutscher Sicherheitsbehörden zur Abwehr elektronischer Angriffe auf IT-Infrastrukturen arbeiten, neben dem BSI, das Bundesamt für Verfassungsschutz (BfV), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundeskriminalamt (BKA), die Bundespolizei (BPol), das Zollkriminalamt (ZKA), der Bundesnachrichtendienst (BND) und die Bundeswehr (Bw) zusammen. Demnächst kommen auch alle über die Betreiber der Kritischen Infrastrukturen Aufsicht führenden Stellen hinzu. Jede dieser Behörden entsendet eine Verbindungsperson als ihren Mitarbeiter ins Abwehrzentrum. Alle arbeiten kooperativ und auf Augenhöhe zusammen.

Im Cyber-AZ sollen alle Behörden in ihrem jeweiligen Zuständigkeitsbereich von dem gemeinsamen Wissen profitieren. Damit das reibungslos funktioniert, ist das Cyber-AZ mit den Lagezentren und entsprechenden Einrichtungen der beteiligten Behörden vernetzt. So bewertet das BSI einen Cyber-Angriff aus informationstechnischer Sicht, während das BfV, der MAD und der BND ihn aus nachrichtendienstlicher Sicht bewerten. Hinzu kommt die polizeiliche Perspektive vonseiten des BKA, des ZKA und der BPoL. Das BBK schließlich bewertet die Aspekte der Katastrophenvorsorge und Belange der Kritischen Infrastrukturen.

Eine so enge Zusammenarbeit löst verständlicherweise die Frage aus, ob dabei auch die jeweiligen gesetzlichen Aufgaben und Befugnisse beachtet werden. Dies wird durch spezielle Verwaltungsvereinbarungen zwischen den beteiligten Behörden sichergestellt. Sie haben sich in den fünf Jahren seit der Gründung als außerordentlich belastbar erwiesen.

GANZHEITLICHES LAGEBILD, FUNDIERTE HANDLUNGSEMPFEHLUNGEN

So wie die Gefährdungslage sich seit 2011 verändert hat, hat sich auch das Cyber-AZ gewandelt. Es entwickelte sich von einer reinen Informationsdrehscheibe hin zur zentralen Kooperationsplattform der IT-Sicherheitsbehörden.

Dies ist vor allem auf die entwickelten Routinen und Produkte, auf ein wachsendes Vertrauen zwischen den beteiligten Behörden und auf die Mitarbeiterinnen und Mitarbeiter zurückzuführen. Sie haben einen behördenübergreifenden Teamgedanken entwickelt und arbeiten zielgerichtet, hoch integriert und effizient im Rahmen etablierter Prozesse zusammen: in der täglichen Lagebesprechung, in Arbeitskreisen zu speziellen Themen oder in gemeinsamen Terminen bei Betroffenen eines Cyber-Angriffs.

BEDARFSGERECHTE PRODUKTE, VIELFÄLTIGE SYNERGIEN

Auch die Produkte des Cyber-AZ haben sich als zielführend und tragfähig erwiesen. Da ist einmal die Cyber-Lage als tagesaktuelle Erstbewertung. Sie stellt Sachverhalte der Cyber-Security bedarfsgerecht, zielgruppenorientiert und strukturiert dar und weist eine hohe technische, politische und mediale Relevanz auf. Da sind zum anderen die

Informationen des Nationalen Cyber-Abwehrzentrums, mit denen analysebasiert das Ergebnis einer Auswertung wichtiger Sachverhalte vermittelt wird, die in den Gremien des Cyber-AZ erarbeitet wurden.

Beide Produkte zeichnen sich dadurch aus, dass alle beteiligten Behörden mit ihren Fähigkeiten und im Rahmen ihrer Befugnisse mitwirken. Dabei werden nachrichtendienstliche und polizeiliche Informationen gleichermaßen berücksichtigt. Gerade die mit diesen Produkten angesprochene politisch-ministerielle Zielgruppe hat einen Bedarf an konsolidierter Betrachtung. Sie bietet einen erheblichen Mehrwert gegenüber Einzelmeinungen.

Die Produkte sind nur ein messbarer Output der vielfältigen Synergien, die sich insbesondere aus dem regelmäßigen Wissenstransfer im Cyber-AZ ergeben. Die beteiligten Behörden und Institutionen nehmen zwar weiterhin alle operativen Aufgaben je nach Zuständigkeit eigenverantwortlich wahr. Aber weit über die direkt beteiligten Mitarbeiter im Cyber-AZ hinaus hat sich ein tiefes Verständnis für die Erfordernisse und Eigenheiten der jeweiligen Arbeit entwickelt. Es dient nicht nur einer nachhaltigen Cyber-Abwehr. Es ermöglicht, vor die Lage zu kommen und den Angreifer zu kennen. So kann sinnvolle und effektive Prävention betrieben werden.

Dies ist umso bedeutsamer, weil ein weiteres Arbeitselement immer wichtiger wird: die Koordinationsfunktion: Heute koordiniert das Cyber-AZ bei Sachverhalten, bei denen die Zuständigkeit mehrerer Behörden betroffen ist, in jeweils extra eingerichteten Arbeitsgruppen die Fallbearbeitung („Koordinierte Fallbearbeitung [KoFaB]“). Dabei greifen die Cyber-AZ-Mitarbeiter jeweils auf geeignete zusätzliche Ressourcen aus ihren jeweiligen Häusern zurück.

In den vergangenen fünf Jahren hat das Cyber-AZ sowohl seine organisatorische Struktur als auch seine Arbeitsschwerpunkte und Kooperationsmodelle kontinuierlich weiterentwickelt. Es hat sich als flexibel und effizient erwiesen. Und es hat entscheidend zu einer verbesserten Architektur in der Cyber-Abwehr beigetragen. ■

Nationales Cyber-Abwehrzentrum

Das Cyber-Abwehrzentrum ist beim BSI in Bonn angesiedelt.

Weitere Informationen:
https://www.bsi.bund.de/cyber-az

IT-Sicherheitsgesetz ist Pflicht – UP KRITIS ist Kür

von Nora Apel, Referat Kritische Infrastrukturen – Grundsatz

Am 25.07.2015 trat das IT-Sicherheitsgesetz (IT-SiG) in Kraft und räumte dem BSI neue Verantwortung und Befugnisse im Bereich der Kritischen Infrastrukturen ein. Die Kritischen Infrastrukturen stellen wichtige, teils lebenswichtige Güter und Dienstleistungen bereit, ohne die das öffentliche und private Leben in Deutschland nicht mehr in gewohnter Weise funktionieren würde.

Das IT-SiG verpflichtet bestimmte Betreiber Kritischer Infrastrukturen, erhebliche IT-Störungen an das BSI zu melden und ihre IT, die für die Erbringung der kritischen Dienstleistungen notwendig ist, nach dem Stand der Technik abzusichern. Die Identifizierung der konkreten KRITIS-Betreiber, die unter die Neuregelungen fallen, erfolgt anhand einer Rechtsverordnung, die in zwei Teilen (sog. Körben) vom Bundesministerium des Innern (BMI) erstellt wird.

VERORDNUNG TRITT STUFENWEISE IN KRAFT

Der erste Korb trat am 03.05.2016 in Kraft und regelt die Sektoren Energie, Wasser, Ernährung sowie Informationstechnik und Telekommunikation. Anlagenbetreiber, die unter diese Verordnung fallen, müssen bei einer IT-Störung über eine Kontaktstelle Meldungen an das BSI abgeben. Über diese Kontaktstelle erhalten sie auch Warn- und Lagehinweise oder -informationen vom BSI.

Spätestens zwei Jahre nach Inkrafttreten der Verordnung müssen die Betreiber dem BSI die Umsetzung von angemessenen Maßnahmen zur IT-Sicherheit nachweisen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Der zweite Korb der Verordnung regelt die Sektoren Transport und Verkehr, Finanz- und Versicherungswesen sowie Gesundheit und ist für das Frühjahr 2017 geplant.

QUANTITATIVE UND QUALITATIVE KRITERIEN

Die Identifizierung der KRITIS-Anlagen, die unter das IT-SiG fallen, erfolgt anhand quantitativer und qualitativer Kriterien mit der vom BSI entwickelten Methode zur Identifikation Kritischer Infrastrukturen (MIKI). Das qualitative Kriterium ist die Erbringung einer kritischen Dienstleistung. Hierunter fallen für die Bevölkerung wichtige, teils lebenswichtige Dienstleistungen, bei deren Beeinträchtigung erhebliche Versorgungsengpässe, Störungen der öffentlichen Sicherheit oder vergleichbare dramatische Folgen eintreten.

Für das quantitative Kriterium wurde ein Versorgungsgrad angesetzt: Anlagen, die – direkt oder indirekt – 500.000 Menschen oder mehr versorgen (können), fallen unter die Verordnung. Zur leichteren Anwendung wurde der Versorgungsgrad auf anlagentypische Werte, wie die Kapazität einer Anlage oder die pro Jahr erzeugte Menge, umgerechnet.

Beispiel: Der Durchschnittsverbrauch an Strom pro Person pro Jahr liegt in Deutschland bei 7.375 kWh (inklusive des umgerechneten Verbrauchs von Unternehmen). Ein Kraftwerk, das 420 MW oder mehr Netto-Nennleistung erzeugt, versorgt somit 500.000 Personen mit einer kritischen Dienstleistung (Stromversorgung) und fällt unter die Verordnung. Da Ausfälle oder Beeinträchtigungen von Anlagen in dieser Größenordnung kritisch sind und schnell zu einer Versorgungskrise in Deutschland führen können, müssen diese verhindert werden.

UP KRITIS: KOOPERATION VON WIRTSCHAFT UND STAAT

An der Erstellung der Rechtsverordnung sind neben Vertretern des BMI, des BSI und des BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe), der zuständigen Aufsichtsbehörden und Fachressorts auf Bundesebene auch die Betreiber Kritischer Infrastrukturen beteiligt. Die Umsetzung des Gesetzes erfolgt kooperativ im UP KRITIS. Dort arbeiten KRITIS-Betreiber, Behörden und Verbände seit 2007 gemeinsam am Schutz der Kritischen Infrastrukturen. Dieser kooperative Ansatz des UP KRITIS zum Schutz Kritischer Infrastrukturen wird mit dem IT-Sicherheitsgesetz weitergeführt. ■

Weitere Informationen:
https://www.bsi.bund.de/IT-Sicherheitsgesetz

DAS BSI

Grußwort von Bundesfinanzminister Dr. Wolfgang Schäuble

Liebe Leserinnen und Leser,

als ich 1991 als Bundesinnenminister die Gründung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verantwortete, war nicht vorauszusehen, wie rasant die Digitalisierung voranschreiten würde. Auch heute sind die Konsequenzen dieser Veränderung nicht bis ins Letzte klar. Innovative Geschäftsmodelle entstehen. Es ergeben sich neue Chancen politischer und gesellschaftlicher Teilhabe. Zugleich missbrauchen kriminelle und terroristische Netzwerke die digitale Infrastruktur.

Bereits seit nunmehr 25 Jahren reagiert das BSI auf die sich ständig ändernden Gefährdungslagen durch Cyber-Kriminalität – mit Erfolg. Dies liegt sicherlich auch daran, dass neben den technischen Möglichkeiten zur Erkennung und Abwehr von Cyber-Angriffen der rechtliche Rahmen stetig angepasst wurde. So ist das BSI seit der Novellierung des BSI-Gesetzes im Jahre 2009 für die IT-Sicherheit aller Bundesbehörden verantwortlich. Mit dem IT-Sicherheitsgesetz aus dem Jahr 2015 wurde die Informationssicherheit Kritischer Infrastrukturen noch einmal gestärkt. Beide Gesetze sind von zentraler Bedeutung für den Kampf gegen Cyber-Kriminalität.

Die Bundesregierung setzt sich in Europa wie auf internationaler Ebene für die Stärkung der grenzüberschreitenden IT-Sicherheit ein. Durch den hohen Grad weltweiter Vernetzung unserer Anwendungssysteme wirken sich Cyber-Angriffe in anderen Ländern zunehmend auch auf die IT-Sicherheit in Deutschland aus. Gerade hier wird das BSI mit seiner Expertise aus einem Vierteljahrhundert gefragt sein.

Ich gratuliere dem BSI zu seinem 25-jährigen Bestehen – es ist heute wichtiger denn je.

Dr. Wolfgang Schäuble,
MdB, Bundesminister der Finanzen

Grußwort von Bundesinnenminister Dr. Thomas de Maizière

Liebe Leserinnen und Leser,

als das BSI vor einem Vierteljahrhundert gegründet wurde, waren weder die rasanten Entwicklungen in der Informationstechnik noch die daraus erwachsenen Herausforderungen so vorhersehbar.

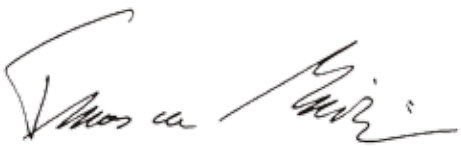
Aber es war spürbar, dass die Digitalisierung unser Leben verändern würde. Und das hat sie. Heute ist die Welt greifbarer, die Menschen einander näher, faszinierende Möglichkeiten und große Chancen haben sich eröffnet.

Digitaler Fortschritt ist nicht risikolos. Vernetzte IT bedeutet nicht nur das Einsparen von Ressourcen und die Optimierung von Prozessen. Komplexität, Abhängigkeiten und Gefährdungen gehen damit ebenso einher. Digitalisierung kann nur gelingen, wenn gleichzeitig hohe IT-Sicherheit gewährleistet ist.

Deshalb war es 1991 goldrichtig, eine unabhängige und fachkundige Instanz zu allen Fragen der IT-Sicherheit zu schaffen. Heute ist das BSI die zentrale Behörde für IT-Sicherheit in Deutschland. Auch international hat es sich einen hervorragenden Ruf erarbeitet und ist hoch anerkannt.

Die digitale Zukunft von Deutschland wird auch weiterhin maßgeblich durch das BSI gestaltet werden. Ich weiß um die hohe Expertise und das große Engagement der Beschäftigten des BSI – das Herz des Amtes. Ihnen gilt an diesem Jubiläum mein Dank.

Ich bin sicher, dass das BSI der wachsenden Dynamik gewachsen ist und es den Anforderungen immer neuer Entwicklungen gerecht werden wird. Für seinen weiteren Weg auf einem echten Erfolgskurs wünsche ich dem BSI weiter viel Erfolg!



Dr. Thomas de Maizière,
MdB, Bundesminister des Innern

25 Jahre BSI

Am 16. September 2016 fand der Festakt „25 Jahre BSI“ in der Stadthalle in Bonn-Bad Godesberg statt. Zu den 400 Gästen zählten neben den BSI-Mitarbeiterinnen und -Mitarbeitern auch Bundesminister des Innern Dr. Thomas de Maizière und Dr. Hans-Georg Maaßen, Präsident des Bundesamts für Verfassungsschutz (BfV).

25 Jahre BSI – im Laufe eines Vierteljahrhunderts hat sich das Amt beträchtlich weiterentwickelt. Die immer rasantere Digitalisierung und die große Abhängigkeit der Menschen von der Informationstechnik haben dem Thema Cyber-Sicherheit zu mehr Bedeutung verholfen. Heute ist das BSI die nationale Cyber-Sicherheitsbehörde, die die Informationssicherheit in der Digitalisierung wesentlich mitgestaltet. Es ist die zentrale Anlaufstelle und führender Kompetenzträger in Fragen der IT-Sicherheit für Staat, Wirtschaft und Gesellschaft.

Das betonte auch der BSI-Präsident Arne Schönbohm in seiner Eröffnungsrede: „Wir haben es geschafft, mit der Entwicklung der Informationstechnologie in den letzten 25 Jahren Schritt zu halten. Unsere Mitarbeiter machen die technische Kompetenz des BSI aus, deshalb sind wir

„Die Zukunftsfähigkeit der Wirtschaftskraft Deutschlands hängt von vielen Faktoren ab – unter anderem auch von der Cyber-Sicherheit. Wir wollen sichere Verkehre, auch im Internet. Das braucht nicht nur die Regierung in ihrer internen Kommunikation, das braucht die Wirtschaft und das brauchen wir als Bürgerinnen und Bürger."

Dr. Thomas de Maizière, *Bundesminister des Innern*

in Deutschland so stark. Wichtig ist, dass wir die Vergangenheit kennen und die Gegenwart verstehen, um die Zukunft gestalten zu können. Nur so können wir Cyber-Gefahren abwehren."

Bundesinnenminister Dr. Thomas de Maizière stellte in seiner Rede heraus, dass Cyber-Kriminalität viele Gesichter habe und es aussehe, als komme jeden Tag ein neues Gesicht hinzu. Ohne eine Institution wie das BSI sei die Digitalisierung auf Dauer nicht geschützt. Er wünsche sich, so der Minister, dass das BSI den kommenden Zukunftstechnologien, dem digitalen Fortschritt, ein sicheres Gesicht gibt.

Einen Eindruck von den Festlichkeiten und Reaktionen der Besucher gibt die Bilderstrecke auf den folgenden Seiten. **>>**

„In den Achtzigerjahren hat das Thema Computersicherheit zunehmend eine Rolle gespielt. Der erste Schritt war, dass man bei der Vorgängerbehörde des BSI eine Abteilung Computersicherheit mit damals insgesamt 60 Stellen eingerichtet hat. Das war relativ viel. Sehr schnell hat sich herausgestellt, dass Computersicherheit nicht nur eine Angelegenheit des Militärs und des Geheimschutzes, sondern der gesamten Gesellschaft ist."

Wendelin Bieser, *ehemaliger Mitarbeiter des BMI*

„Generell bestand die Herausforderung für das BSI darin, sich beim Thema Informationssicherheit unabhängig und neutral zu positionieren. Und damit auch einen ganz neuen Standort für Informationssicherheit in Deutschland aufzumachen."

Andreas Könen, *Leiter der Stabsstelle „IT- und Cybersicherheit; sichere Informationstechnik" im Bundesinnenministerium und ehemaliger Vizepräsident des BSI*

„Die größten Herausforderungen waren, dass das BSI aus unterschiedlichen Behörden und Leuten aus Wissenschaft und Verwaltung zusammengestellt wurde und zusammenwachsen musste. Natürlich kam jeder mit seinem Hintergrund und so war es nicht immer einfach, sich auf eine gemeinsame Linie zu einigen und die Aufgabenschwerpunkte nach dem BSI-Gesetz mit Leben zu füllen."

Marit Blattner-Zimmermann, *ehemalige Mitarbeiterin des BSI*

„Cyber-Sicherheit wurde in den vergangenen Jahren als Thema zu gering geschätzt. Ich bin sehr froh, dass wir mit dem BSI einen starken Partner und dass wir ein gutes Cyber-Abwehrzentrum haben. Ich bin stolz, dass wir die Zusammenarbeit sehr weit vorangebracht haben."

Dr. Hans-Georg Maaßen, *Präsident des Bundesamts für Verfassungsschutz (BfV)*

„Das Highlight war zweifellos die Grün dung des BSI und die Verabschiedung des ersten BSI-Gesetzes. Das wurde sehr heftig zwischen dem Bundesinnenmi-nisterium und den verschiedenen Partei en im Deutschen Bundestag diskutiert. Namentlich mit den Vertretern des Datenschutzes, die den Unterschied zwi schen Datenschutz und Datensicherheit damals noch nicht verstanden hatten. Das waren harte, aber letztendlich sehr erfolgreiche Gespräche."

Eckart Werthebach,
Staatssekretär a.D. im Bundesministerium des Innern

„Ohne Cyber-Sicherheit wird es keine Digitalisierung in Deutschland geben, denn sie ist eine wesentliche Grundlage, damit unser Zusammenleben funktioniert."

Arne Schönbohm, *Präsident des BSI*

„Bei der Behördenberatung haben wir festgestellt, dass immer wieder dieselben Fragen gestellt wurden. Wir haben angefangen, die Antworten in einer modularen Bauweise als Bausteine verpackt aufzuschreiben, was schließlich in dem bekannten IT-Grundschutz mündete."

Isabel Münch, *Referatsleiterin IT-Grundschutz, BSI*

„Der Höhepunkt während meiner Tätigkeit beim BSI war, 2005 deutlich zu machen, dass das BSI tatsächlich eine Behörde ist, die wachsen und sich weiterentwickeln muss. Bis dahin hatte das Amt seit seiner Gründungszeit kein personelles Wachstum verzeichnet. Wenn das nicht geändert worden wäre, wäre das BSI nicht in der Lage, auch nur annähernd die gestellten Aufgaben zu erfüllen."

Horst Samsel, *Leiter der Abteilung Beratung und Koordination, BSI*

„Die Herausforderung bestand darin, dass das Amt überhaupt gegründet wurde. Es war die Phase der Wiedervereinigung, IT-Sicherheit war nicht im politischen Fokus. Wichtig war, dieses parlamentarische Vorhaben durchzuziehen. In der letzten Sitzung des Bundesrates wurde dann am 18. Dezember 1990 entschieden, das BSI zu gründen."

Michael Hange, *ehemaliger Präsident des BSI*

„In meine Zeit beim BSI fiel die Änderung des BSI-Gesetzes im Jahr 2009, bei der dem BSI sehr weitgehend in die Wirtschaft hineinwirkende Kompetenzen eingeräumt wurden. Die erste Herausforderung war auszuprobieren, wie dieses Gesetz wirkt. Wir haben als ersten Fall eine Warnung vor einem sehr weit verbreiteten Produkt ausgesprochen und damit natürlich eine gewaltige Resonanz ausgelöst. Das hat die Stellung des BSI und auch die Wahrnehmung des BSI insbesondere in der IT-Wirtschaft ganz wesentlich verändert."

Horst Flätgen, *ehemaliger Vizepräsident des BSI*

„Die Entscheidung vor 25 Jahren, ein BSI zu gründen, war eine wegweisende Entscheidung. Ohne genau zu wissen, wie sich die Zukunft entwickelt. Diese Einrichtung zu gründen war phänomenal und deshalb feiern wir gerne heute den 25-jährigen Geburtstag. Das BSI ist seitdem ein Ankerpunkt der IT-Sicherheit, ein Vertrauensanker, geworden."

Dr. Thomas de Maizière, *Bundesminister des Innern*

BSI im Dialog

Neue Veranstaltungsreihe gestartet

Das BSI hat mit „BSI im Dialog“ eine neue Veranstaltungsreihe als Forum für Diskussionen und den Austausch mit Akteuren aus Staat, Wirtschaft und Gesellschaft gestartet. Ziel ist es, eine stärkere Visibilität rund um die Themen der Digitalisierung und Cyber-Sicherheit zu erreichen.

Die erfolgreiche Auftaktveranstaltung fand im Juni in Berlin gemeinsam mit dem Bundeskriminalamt (BKA) statt. Im Fokus stand das Thema Ransomware, die Bedrohung durch Schadprogramme, die den Zugriff auf Daten und Systeme verhindern und nur gegen Zahlung von Lösegeld wieder freigeben. Erste Varianten und Konzepte von Ransomware gab es bereits vor dem Jahr 2000, seit 2011 ist Ransomware ein weitverbreiteter Schadprogrammtyp: denn Berichte in Medien über Angriffs-Kampagnen und neue Versionen dieses Schadprogrammtyps sind an der Tagesordnung und Privatpersonen, Unternehmen sowie Verwaltungen sind gleichermaßen betroffen.

In seiner Eröffnung betonte BSI-Präsident Arne Schönbohm die Herausforderung an die IT-Sicherheit von Organisationen und Unternehmen, die aus Ransomware resultiert. Die dadurch verursachten IT-Sicherheitsvorfälle zeigen, wie abhängig jeder von Informationstechnologie ist und welche Auswirkungen ein Cyber-Angriff haben kann. Vervollständigt wurde das Programm durch zwei Impulsvorträge vom BKA und dem BSI über IT-Sicherheitsvorkehrungen in Unternehmen und Verwaltungen, den Faktor Mensch als Schwachstelle sowie die Auswirkungen des IT-Sicherheitsgesetzes. Abschluss der rund zweistündigen Veranstaltung bildete eine rege Diskussion unter den mehr als 30 Teilnehmern.

Das BSI verfolgt mit den Veranstaltungen einen kooperativen, regionalen Ansatz. So soll die Reihe künftig auch in anderen Städten, gemeinsam mit regionalen und überregionalen Partnern des BSI, fortgeführt werden. ■

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

HERAUSFORDERNDE JAHRE

von Arne Schönbohm, Präsident des BSI

Spätestens mit dem Beschluss des IT-Sicherheitsgesetzes hat sich die Rolle des BSI von einer Fachbehörde zu einer unabhängigen Institution gewandelt, die im politisch-wirtschaftlichen Raum agiert. Unsere Aufgaben und Verantwortlichkeiten wurden erneut ausgeweitet. Wir sind und bleiben der zentrale IT-Sicherheitsdienstleister des Bundes und werden auch zunehmend andere staatliche Stellen unterstützen. Aber wir sind auch die zentrale Stelle für Belange der IT-Sicherheit und Digitalisierung in Wirtschaft und Gesellschaft. Insbesondere die Zusammenarbeit mit den Kritischen Infrastrukturen (KRITIS) wurde völlig neu definiert. Kurz gesagt nehmen wir nun die Rolle, die wir seit der Novellierung des BSI-Gesetzes im Jahr 2009 für die Bundesbehörden besitzen, auch für die KRITIS-Betreiber ein.

Das Gesetz ist nicht nur wichtig für das BSI, es reflektiert vor allem die zunehmende Bedeutung der IT-Sicherheit in einer digitalisierten Gesellschaft. Die mit dieser Digitalisierung verbundenen Chancen für den Industriestandort Deutschland sind groß – aber nur, wenn wir uns der damit verbundenen Risiken bewusst sind und sie proaktiv angehen. Unternehmen und Verwaltungseinrichtungen müssen sich auf die Bedrohungen der IT-Sicherheit immer wieder neu einstellen und Maßnahmen der Prävention, Detektion und Reaktion vorbereiten und umsetzen. Das ist aufwendig und erfordert Zeit, Geld und personelle Ressourcen. Einzelne Unternehmen sind bereits seit vielen Jahren sehr aktiv. Andere Unternehmen haben wenig bis gar nichts getan. Das trifft vor allem auf viele kleine und mittelständische Unternehmen zu.

Der positive Trend der letzten Jahre setzt sich weiter fort: Immer mehr Unternehmen beschäftigen sich stärker mit Cyber-Sicherheit. Leider erfolgt dies oft erst, nachdem Probleme aufgetreten sind. Dabei sollten sich die Akteure längst bewusst sein, dass die zunehmende Vernetzung und Digitalisierung aller Lebens- und Arbeitsbereiche ohne IT-Sicherheit nicht zum Erfolg führen wird.

CYBER-SICHERHEIT IN DEN FOKUS RÜCKEN

Ein wichtiges Thema ist für uns in den kommenden Jahren die Unterstützung der Digitalen Agenda der Bundesregierung. Hier können wir als BSI entscheidend dazu beitragen, dass die Digitalisierung in Deutschland erfolgreich ist, durch mehr Sichtbarkeit, durch mehr Dialog, durch mehr Aktivitäten.

- Wir intensivieren den Austausch mit den Vorständen und Aufsichtsräten in den DAX- , MDAX- sowie den kleinen und mittelständischen Unternehmen (KMU).
- Wir wenden uns stärker an die IT-Anwender, führen Gespräche und gründen Arbeitskreise mit ihnen.
- Wir warnen vor Anwendungen mit großen Unsicherheiten und geben Empfehlungen für Sicherheitsmaßnahmen.

„IT-Sicherheit muss schon bei der Entwicklung neuer Produkte und Services mindestens gleichrangig neben ökonomischen und funktionalen Faktoren mitbedacht werden.“

- Wir platzieren das Thema Informationssicherheit in der Chefetage.

Jedes Unternehmen muss künftig einen Digitalisierungs-Vorstand oder CDO (Chief Digital Officer) haben, der seinen Kolleginnen und Kollegen vorrechnet, dass Cyber-Sicherheit bei der Digitalisierung ein Wettbewerbsfaktor ist. Ein IT-Beauftragter reicht dafür nicht. Daher bauen wir in diesem Jahr vor allem den Dialog mit den Entscheidern in den Unternehmen aus, um sie davon zu überzeugen, IT-Sicherheit als Teil des Risikomanagements ihres Unternehmens zu begreifen und sich gerade auch in Bereichen wie Industrie 4.0 oder Automotive entsprechend aufzustellen.

IT-Sicherheit muss schon bei der Entwicklung neuer Produkte und Services mindestens gleichrangig neben ökonomischen und funktionalen Faktoren mitbedacht werden. Denn unser Bericht über die Lage der IT-Sicherheit in Deutschland zeigt, dass die Anzahl der Schwachstellen und Verwundbarkeiten in IT-Systemen nach wie vor auf einem sehr hohen Niveau liegt. Die asymmetrische Bedrohungslage im Cyber-Raum hat sich weiter zugespitzt. Sie kann nur gemeinschaftlich in Schach gehalten werden, wenn Staat, Wirtschaft und Gesellschaft zusammenarbeiten.

KOOPERATIONEN AUSBAUEN

Wir haben die Kooperationsplattformen dafür geschaffen und bauen diese weiter aus.

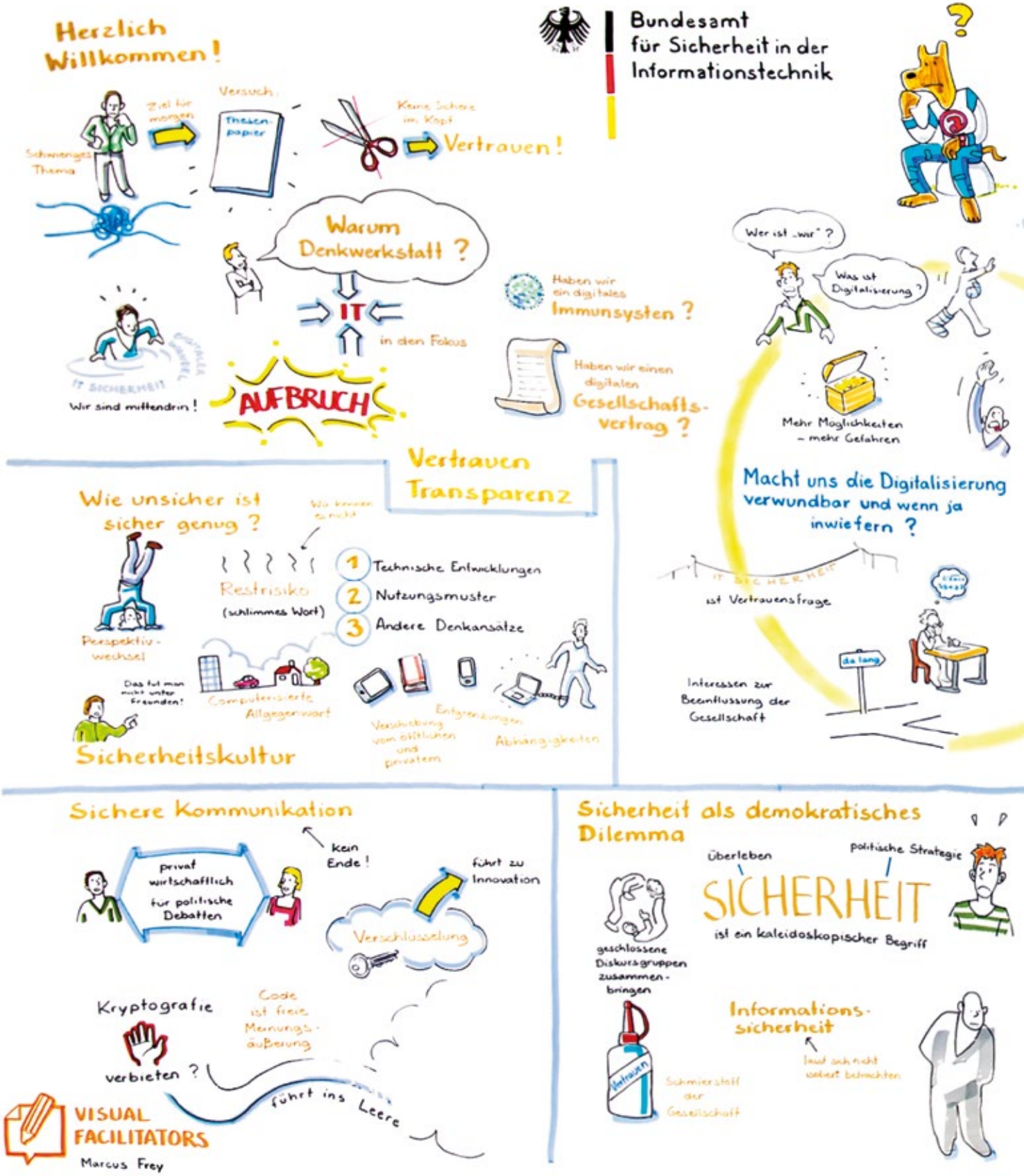
- Die Allianz für Cybersicherheit nimmt seit ihrer Gründung eine sehr positive Entwicklung. Die Zahl der Partner, Multiplikatoren und Teilnehmer steigt stetig an (derzeit 1.980), sodass wir mit den Angeboten der Allianz immer mehr Institutionen regelmäßig und dauerhaft erreichen können.
- UP KRITIS leistet seit ihrem offiziellen Start im Jahr 2007 einen wesentlichen Beitrag zur verlässlichen Bereitstellung der kritischen Dienstleistungen für die Menschen in Deutschland. Der Schwerpunkt liegt dabei auf einem effektiven Zusammenwirken von IT-Sicherheit und der Aufrechterhaltung kritischer Geschäftsprozesse.

Die Zusammenarbeit mit der Wirtschaft ist auch über diese Plattformen hinaus in den kommenden Jahren ein wichtiges Thema für das BSI. Der Fortschritt bei der industriellen Entwicklung führt zu einer kaum übersehbaren Menge neuer Produkte für das Internet der Dinge, Industrie 4.0, Cloud oder Big Data, die auch ein völlig neues Gefahrenpotenzial mit sich bringen. Die Industrie wird zunehmend IT-abhängiger und ihre Funktionsfähigkeit an den Schnittstellen gilt in hohem Maße als gefährdet. Viele etablierte Mechanismen in der Industrie sind nicht an die Digitalisierung angepasst, bei vielen Prozessen in vernetzten Industrieanlagen gilt noch der Grundsatz Safety vor Security. Wir bieten hier schon jetzt zahlreiche konkrete Hilfestellungen und Angebote und werden diese durch weitere Cyber-Sicherheitsempfehlungen ausbauen. Wir setzen dabei auf kooperatives Handeln; dies schließt jedoch eine eventuell notwendige Regulierung nicht aus. Gleichzeitig bauen wir die Anzahl der Zertifikate weiter aus und modernisieren den IT-Grundschutz.

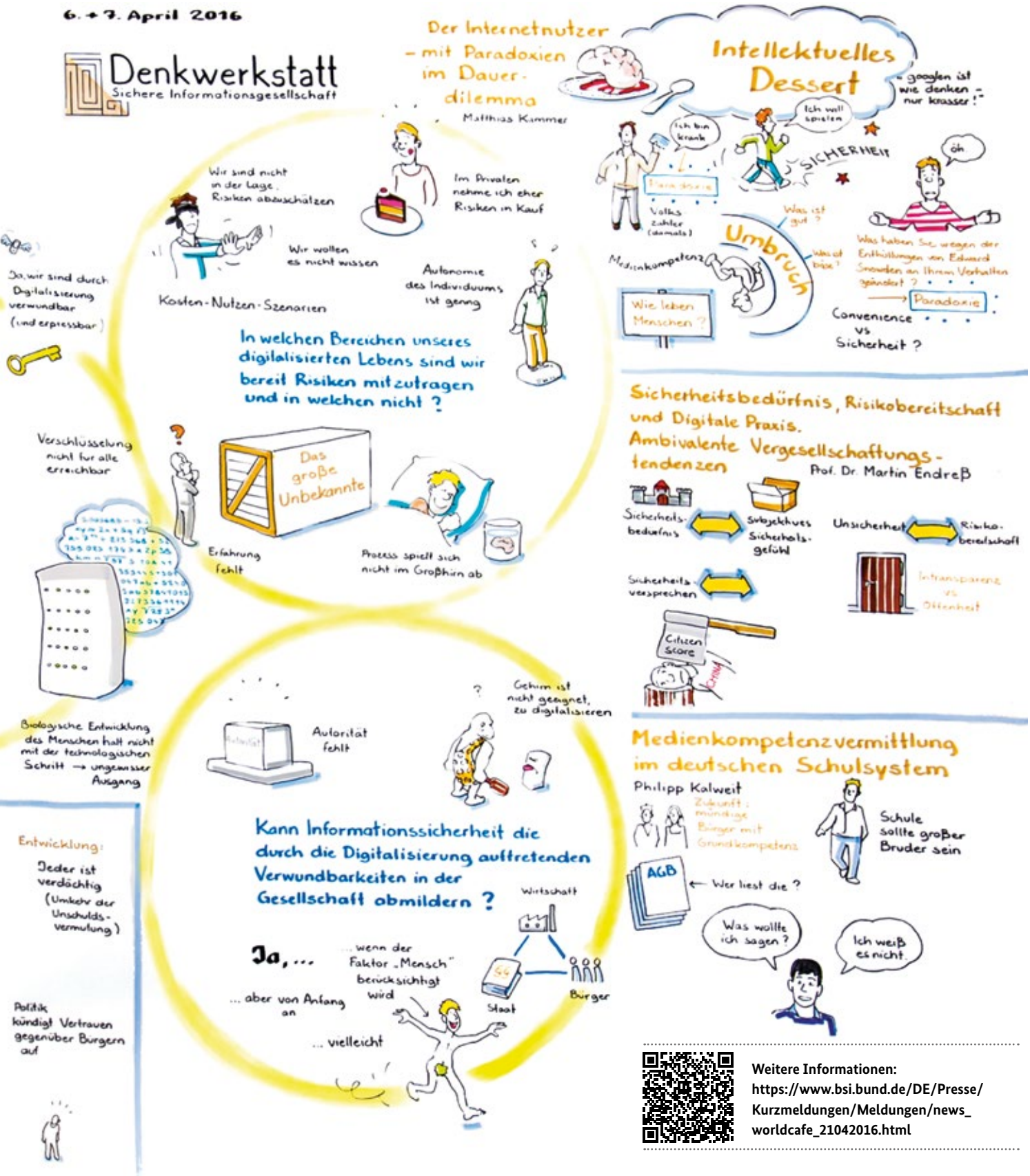
Die Jahre 2016/17 stehen für uns ganz klar im Zeichen der Umsetzung und Operationalisierung des IT-Sicherheitsgesetzes. Der erste Teil der Rechtsverordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) ist seit Anfang Mai 2016 in Kraft. Er bestimmt zunächst Kritische Infrastrukturen in den Sektoren Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung. Bis Anfang 2017 sollen per Änderungsverordnung auch die Betreiber in den Sektoren Transport und Verkehr, Gesundheit sowie Finanz- und Versicherungswesen identifizierbar werden. Sowohl personell als auch organisatorisch müssen wir uns daher hier zügig und gut aufstellen.

Eines wird bleiben: Fortschritte im Bereich der technischen Abwehr von Cyber-Angriffen erfolgen stets Schritt für Schritt – eine Tatsache, die manchmal schwer zu akzeptieren ist. Aber je breiter die Basis wird, also das Bewusstsein für die Bedeutung der IT-Sicherheit für alle Bereiche unseres täglichen Lebens und Arbeitens, die heute vernetzt, online oder digitalisiert vonstattengehen, desto größer können diese Schritte werden. Daran arbeiten wir. ■

Denkwerkstatt für eine sichere Informationsgesellschaft



Im April 2016 diskutierten fünfzig Vertreterinnen und Vertreter aus Zivilgesellschaft, Wissenschaft, Wirtschaft und Verwaltung darüber, wie eine Informationsgesellschaft zugleich smart und sicher sein kann. Als erstes Ergebnis wurden sieben Thesen erarbeitet und im Konsens verabschiedet. Festgehalten wurde die intensive und teils kontroverse Diskussion von Visual Facilitators.



Weitere Informationen:
https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/news_worldcafe_21042016.html

IT-SICHERHEIT
IN DER PRAXIS

„Die Anforderungen an eine moderne und gleichzeitig sichere Bürokommunikation bedeuteten die Geburtsstunde von SINA“

Interview Dr. Rainer Baumgart

Die Essener secunet Security Networks AG entwickelte im Auftrag des BSI die Sichere Inter-Netzwerk Architektur SINA. Diese dient der sicheren Bearbeitung, Speicherung und Übertragung von Verschlusssachen sowie anderen sensiblen Daten und wird bis heute durch secunet stetig weiterentwickelt. Für das BSI-Magazin zog Dr. Rainer Baumgart, Vorstand von secunet, ein Resümee zur langjährigen Zusammenarbeit.

Die Sichere Inter-Netzwerk Architektur SINA ist ein Ergebnis der langen Zusammenarbeit zwischen secunet und BSI. Was macht diese so besonders?

Das BSI und secunet arbeiten praktisch seit der Gründung der secunet auf dem Gebiet der IT-Sicherheit zusammen. Intensiviert wurde die Zusammenarbeit, als secunet die erste Ausschreibung zur technischen Umsetzung des SINA-Konzepts des BSI gewann. Oder anders: Der Umzug der Bundesregierung von Bonn nach Berlin und die gestiegenen Anforderungen an moderne, aber gleichzeitig sichere Bürokommunikation bedeuteten die Geburtsstunde von SINA. Entscheidend für den großen Erfolg von SINA ist die ganzheitliche Sicherheitsarchitektur: Sie umfasst unterschiedliche Gateways, Leitungsverschlüsseler, ein leistungsfähiges Management bis hin zu sicheren Clients und ein Tablet. Seit rund 15 Jahren bewähren sich die Komponenten bei Behörden, Streitkräften und geheimschutzbetreuten Unternehmen und werden dort zur Verarbeitung und Übertragung von Verschlusssachen eingesetzt – bis einschließlich GEHEIM, NATO SECRET und SECRET EU.

Unter Berücksichtigung der besonderen Kundenanforderungen und auch der strengen Zulassungsbedingungen wird SINA stetig in enger Kooperation mit dem BSI weiterentwickelt.

In welchen Themen- und Entwicklungsfeldern der IT-Sicherheit arbeiten BSI und secunet neben SINA zusammen?

Wir haben in nahezu allen Bereichen der IT-Sicherheit Berührungspunkte mit dem BSI. Besonders hervorheben möchte ich, neben den vielfältigen Beratungstätigkeiten, mit denen wir diverse Bereiche des BSI unterstützen, die Zusammenarbeit im Umfeld elektronischer Identitätsdokumente und der Biometrie. Auf dem damals noch jungen Gebiet war echte Pionierarbeit gefragt, als es galt, persönliche physiologische Merkmale aufzunehmen, digital

Kurzprofil Dr. Rainer Baumgart

Dr. Rainer Baumgart ist seit 1997 bei secunet. Seit 1999 ist er im Vorstand der secunet Security Networks AG und übernahm 2001 dessen Vorsitz. Der promovierte Physiker blickt auf eine über 25-jährige Karriere im Bereich IT-Sicherheit mit Stationen bei der RWTÜV AG und der TÜV Informationstechnik GmbH zurück.

umzusetzen und als elektronische Datensätze in Reise- und Ausweisdokumenten zu speichern. Die Ergebnisse der zahlreichen Untersuchungen mündeten in BSI-Standards, die nicht nur nationale Bedeutung haben, sondern auch die Grundlage für internationale Standards für elektronische Identitätsdokumente bildeten. Heute werden fast überall auf der Welt elektronische Reisepässe, die sich an diesen Standards orientieren, ausgegeben und ermöglichen eine schnelle und sichere Identifikation von Reisenden. Zusätzlich kooperieren BSI und secunet gemeinsam mit weiteren Partnern bei der Entwicklung von automatisierten Grenzkontrollsystemen, so genannten eGates.

■ Die digitale Welt verändert sich stetig. Was erwartet uns im Hinblick auf IT-Sicherheit in der Zukunft?

Die zunehmende Digitalisierung schafft zusätzliche Risiken. Unsere Aufgabe ist es, bei der rasanten Entwicklung innerhalb der IT die Bedrohungslage richtig einzuschätzen und mit der geeigneten Sicherheitstechnik darauf zu reagieren. Dabei sind Unternehmen und Behörden gleichermaßen betroffen. Nehmen wir als Beispiel die Kritischen Infrastrukturen – KRITIS. Hier dürfen wir nicht nur auf die großen, offensichtlich betroffenen Branchen schauen, sondern müssen auch im Mittelstand und insbesondere in der Industrie IT-Sicherheit aktiv vorantreiben.

Um aktuelle Lagebilder zu erstellen und bei Sicherheitsvorfällen entsprechende Gegenmaßnahmen einleiten zu können, muss der Austausch der Informationen weiter institutionalisiert werden. Allianzen wie die Allianz für Cyber-Sicherheit sind ein geeignetes Mittel. Allerdings dürfen wir Deutschland nicht isoliert betrachten, sondern müssen den Informationsaustausch wenigstens auf europäischer Ebene ausdehnen, damit in Zusammenarbeit mit allen relevanten Beteiligten ein hohes Maß an Sicherheit gewährleistet werden kann.

Um künftigen Bedrohungen zu begegnen, ist neben guten Konzepten vor allem kompetentes Personal erforderlich. Deutschland ist im Bereich IT-Sicherheit und Kryptografie noch führend in der Welt – das zeigt sich auch in den vielfältigen Aktivitäten der Mitglieder des deutschen Branchenverbands für IT-Sicherheit TeleTrusT. Diese Sicherheitskompetenz ist ein entscheidender Eckpfeiler im Hinblick auf die digitale Souveränität und nicht zuletzt ein Verdienst der Zusammenarbeit zwischen dem BSI, den Bedarfsträgern, der Bundesverwaltung und der deutschen IT-Sicherheitsindustrie. Langfristig die richtigen und kompetenten Mitarbeiterinnen und Mitarbeiter zu bekommen, wird eine der zentralen Herausforderungen der nächsten Zeit sein. ■

Im Jahr 1999 startete das BSI ein Projekt zur Absicherung IP-basierter Netze unter Verwendung kryptografischer Sicherungsmechanismen. Verschlusssachen, die bisher in Tresoren gelagert und nur unter höchster Geheimhaltung von Kurieren transportiert wurden, sollten nun via Internet übertragen und auf PCs und Notebooks gespeichert werden können. Die besondere Herausforderung bestand darin, prinzipiell unsichere PC-Systeme und Netze so abzusichern, dass höchste Sicherheit gewährleistet wird – zu geringen Kosten und bei einfacher Anwendung.

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

Präventivkonzepte gegen Cyber-Kriminalität

Die Polizei rät

Die Verfolgung von Straftaten ist nur eine Möglichkeit, um die Gesellschaft vor Kriminalität zu schützen. Eine andere ist die Kriminalprävention, die mit ihren Konzepten versucht, Kriminalität gar nicht erst entstehen zu lassen. In Deutschland stärkt seit vielen Jahrzehnten das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) die Handlungsfähigkeit von Bürgerinnen und Bürgern im Zusammenhang auch mit Straftaten in der digitalen Welt.

Die präventiven Konzepte, Initiativen und Medien der Polizeilichen Kriminalprävention der Länder und des Bundes entstehen aus dem Anspruch heraus, die Sicherheit der Bevölkerung zu erhöhen. Wesentlich sind die Aufklärung über Kriminalität und die Vermittlung von Handlungsempfehlungen zum Schutz vor Straftaten, Aufklärung vor allem auch über Cyber-Kriminalität und über andere Straftaten mittels Internet.

Plakate, Faltblätter sowie die Pressearbeit über Funk und Fernsehen gehören zum Standardrepertoire der Polizeilichen Kriminalprävention. Der Slogan „Die Polizei rät“ wird in den Gründerjahren und Jahrzehnte darüber hinaus zum Programm – und legt den Grundstein für die kriminalpräventive Arbeit der Polizei von heute. Die Solidargemeinschaft von Bund und Ländern, die hinter der Abkürzung ProPK steht, ist erfolgreich. Über 150 Medien gehören zum Produktportfolio. Sie sind kostenlos online bestellbar oder können über 500 bestell- und lieferberechtigte Polizeidienststellen im Bundesgebiet abgerufen werden. Allein 2015 wurden über 4 Millionen Broschüren, Faltblätter, Plakate und andere Medien an Verbraucher und Experten verteilt.

Darunter sind auch zahlreiche Publikationen, die Sicherheit im digitalen Alltag vermitteln. Inzwischen ist dies ein Schwerpunkt der Präventionsarbeit. Die Polizei setzt darauf, über Straftaten mittels Internet aufzuklären, indem auch konkrete Straftatbestände benannt werden. So soll die Bevölkerung nicht Opfer von Cyber-Kriminellen werden – aber auch selbst nicht zum Täter.

Kurz gefasst klärt das ProPK über Kriminalität auf, zeigt Schutzmöglichkeiten und reduziert dadurch Kriminalitätsursachen. Dabei steht stets der Schutz des Opfers im Vordergrund.

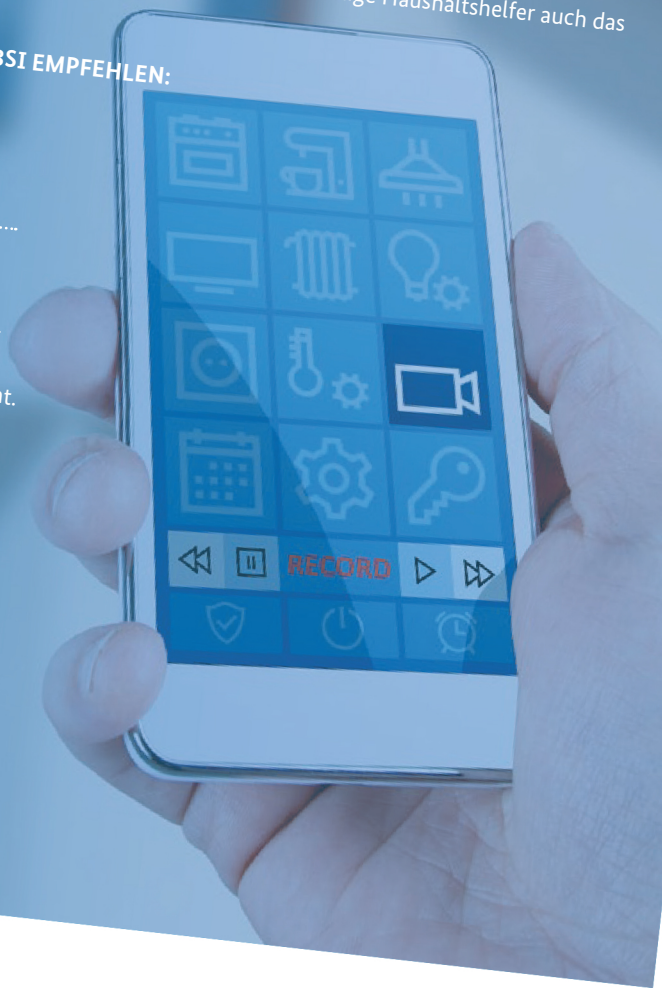
SMART LIVING –

5 TIPPS, DAMIT DAS INTELLIGENTE ZUHAUSE AUCH SICHER IST

Waschmaschine, Alarmanlage, Fernseher – mit Apps und Tablets lassen sich auch diese Geräte bedienen. Dank digitaler Funkübertragung und des Internets sind sie ständig erreichbar, ständig auf Empfang, aber auch ständig ein potenzielles Sicherheitsrisiko. Deswegen gilt für den Smart-TV, die Alarmanlage und andere internetfähige Haushaltshelfer auch das Prinzip „Internetsicherheit".

POLIZEILICHE KRIMINALPRÄVENTION UND DAS BSI EMPFEHLEN:

- ☑ Lesen Sie sorgfältig die Bedienungsanleitung und achten Sie auf die besonderen Sicherheitseinstellungen internetfähiger Geräte.
- ☑ Ändern Sie grundsätzlich bereits voreingestellte Passwörter.
- ☑ Wählen Sie ein Passwort, das mindestens zwölf Zeichen lang ist und nicht im Wörterbuch vorkommt. Es sollte aus Groß- und Kleinbuchstaben in Kombination mit Zahlen und Sonderzeichen bestehen und auf den ersten Blick sinnlos zusammengesetzt sein.
- ☑ Achten Sie auf eine Grundsicherheit Ihres WLAN-Netzes. Drahtlose Funknetzwerke werden teilweise mit nur minimal eingestelltem Sicherheitslevel ausgeliefert. Dem empfohlenen Verschlüsselungsverfahren für WLAN nach sollte das Passwort mindestens 20 Zeichen lang sein.
- ☑ Schalten Sie Kamerafunktionen, zum Beispiel an Ihrem Smart-TV, nur an, wenn Sie diese benötigen.



BSI UND ProPK – EIN KONGENIALES DUO GEGEN CYBER-KRIMINALITÄT

Der Erfolg des Programms beruht auf einer klar geregelten und stetigen Zusammenarbeit zwischen der Polizei aller Bundesländer sowie auf einer gelungenen Bund-Länder-Kooperation. Die Zentrale Geschäftsstelle des ProPK mit Sitz in Stuttgart koordiniert alle länderübergreifenden Aktivitäten innerhalb und außerhalb der polizeilichen Gremien. Eine Projektleitung kümmert sich um die strategische Ausrichtung des Programms, während eine Bund-Länder-Kommission (Kommission Polizeiliche Kriminalprävention) die konzeptionelle Sacharbeit leistet.

Aber der Erfolg ist auch vielen Kooperationspartnern zu verdanken, die polizeiliche Konzepte mit ihrem Fachverstand begleiten und bereichern. Mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) arbeitet das ProPK seit über einem Jahrzehnt zusammen. Beispiele für die gute und notwendige Kooperation sind der Sicherheitskompass, der die wichtigsten Regeln zur sicheren Internetnutzung vermittelt, oder der Film „Verklickt!", der Schülern vielfältige Gefahren des Internets aufzeigt. ■

„Verklickt!" Sicherheit im Medienalltag – Ein Film für Schülerinnen und Schüler ab Klassenstufe 7
Weitere Informationen: http://www.polizei-beratung.de/startseite-und-aktionen/verklickt.html

DIGITALE GESELLSCHAFT

Unter dem Schlüssel der Vertraulichkeit

von Thomas Caspers, Leiter des Fachbereichs Evaluierung und Betrieb von Kryptosystemen

Niemand würde einer Postkarte brisante Details aus dem Privatleben anvertrauen. Zu groß ist die Sorge, dass diese Mitteilung in die falschen Hände gerät. Tatsächlich sind unverschlüsselte E-Mails aber nichts anderes als Postkarten. Im großen Stil. Dennoch versenden entsprechend einer aktuellen bitkom-Befragung nur 15 % aller Nutzer in Deutschland ihre E-Mails verschlüsselt – erstaunlich, wenn man sich die Risiken vor Augen führt.

Das Geschriebene soll nur den Adressaten erreichen und bleibt zwischen Sender und Empfänger vertraulich. Dieser Wunsch ist kein Produkt der neuzeitlichen Digitalisierung. Die Ursprünge moderner Krypto-Verfahren reichen weit in die Geschichte der menschlichen Zivilisation zurück. Höchstwahrscheinlich kodieren Menschen Texte, seitdem sie schreiben, um kritische Informationen von einem unberechtigten Zugriff zu schützen.

GEHEIMSCHRIFT – EIN URALTES REZEPT

Eine der ersten Ideen war dabei: Der Absender verwendet statt der allgemein bekannten Schriftzeichen andere, die nur dem Empfänger bekannt sind, der die Nachricht mithilfe eines Schlüssels entschlüsseln soll. Auch digitale Verschlüsselungsverfahren setzen zu schützende Informationen in für unberechtigte Empfänger nicht mehr zu entziffernde Daten um – mit dem Unterschied, dass Verschlüsselung heute für den Wirtschaftsstandort Deutschland ein wichtiger Wettbewerbsfaktor ist. Denn die Digitalisierung kann ihr Wertschöpfungspotenzial nur entfalten, wenn notwendige Sicherheitsmaßnahmen zum Schutz von Unternehmen und Bürgern ergriffen werden. Daher hat die Bundesregierung das Ziel ausgerufen, Deutschland zum „Verschlüsselungs-Standort Nr. 1“ zu machen. Dazu soll, so die digitale Agenda der Bundesregierung, unter anderem „die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden“.

WER SCHLIESST MIT WELCHEM SCHLÜSSEL?

Grundsätzlich unterscheidet man zwei Verschlüsselungsverfahren: symmetrische und asymmetrische. Symmetrische Verfahren basieren darauf, dass Sender und Empfänger denselben Schlüssel zum Ver- und Entschlüsseln verwenden. Dies ist einerseits einfach, andererseits aber auch die Schwäche des Verfahrens. Denn dazu muss der Schlüssel ausgetauscht werden. Gerät er dabei in falsche Hände, kann die Kommunikation entschlüsselt und mitgelesen werden. Deshalb wurde das asymmetrische Verfahren entwickelt. Hierbei kommen unterschiedliche Schlüssel zum Ver- und Entschlüsseln zum Einsatz. Der Schlüssel zum Entschlüsseln muss dabei nicht mehr herausgegeben werden, was den Austausch der Schlüssel wesentlich einfacher macht: Bei der E-Mail-Verschlüsselung wird nur der öffentliche Teil des Schlüssels ausgetauscht, der zum Verschlüsseln notwendig ist. Den zweiten Dechiffrier-Schlüssel behält jeder Nutzer nur bei sich, damit bleibt er geheim.

DIGITALE SCHLÜSSELBRETTER

Zur Verwaltung dieser Schlüssel gibt es zwei unterschiedliche Konzepte: OpenPGP und S/MIME. S/MIME bietet den Vorteil, dass es nicht nur E-Mails verschlüsselt, sondern auch gleich die Identität des Schlüsselinhabers mittels einer unabhängigen Zertifizierungsstelle bestätigt. Diese Bestätigung bietet OpenPGP nicht, ist dafür allerdings innerhalb weniger Minuten und auch anonym einsetzbar. Unter dem Sicherheitsaspekt sind beide Ansätze gleich effektiv. Im Unternehmensumfeld empfiehlt sich oftmals wegen der zusätzlich verfügbaren Funktionen der aufwendigere S/MIME-Standard, im privaten Umfeld eher die unkomplizierte Lösung OpenPGP.

Doch egal ob S/MIME oder OpenPGP: Bislang sind E-Mail-Anbieter, die von Haus aus Ende-zu-Ende verschlüsseln, noch Mangelware. Die meisten großen Portale

transportieren Nachrichten codiert nur vom Kundensystem zu ihrem Server und dann wieder von ihrem zum Server eines anderen Anbieters, jedoch nicht wirklich durchgehend vom Absender bis zum Empfänger, den beiden Endpunkten der Kommunikation, verschlüsselt. Damit eine solche durchgehende E-Mail-Verschlüsselung Standard wird, sollte sie jedoch ohne Zutun des Nutzers funktionieren – und zwar im Idealfall auf allen Plattformen, die man heutzutage zur E-Mail-Kommunikation nutzt, vom Webbrowser am PC bis zum E-Mail-Client auf dem Smartphone.

AUF DEM WEG ZUM „VERSCHLÜSSELUNGSSTANDORT NR. 1“

Um das Thema Verschlüsselung in Deutschland zu fördern, haben sich Vertreter aus Politik, Forschung und IT-Wirtschaft zusammengeschlossen und sich in der „Charta zur Stärkung der vertrauenswürdigen Kommunikation“ unter Federführung des Bundesministeriums des Innern zu einfachen, transparenten Verschlüsselungslösungen verpflichtet. Diese Anbieter stellen eine „echte“ Ende-zu-Ende-Verschlüsselung – vom Postausgang des Senders bis zum Posteingang des Empfängers – zur Verfügung. Der Anwender muss diesen Schutz nur noch aktivieren beziehungsweise bei sich im E-Mail-Programm einrichten. Weitere Initiativen wie etwa die der „Volksverschlüsselung“ ziehen hier nach – Allianzen, die das BSI begrüßt. Die Behörde legt mit technischen Richtlinien und fachlichen Vorgaben die kryptografischen Grundlagen, auf den die angebotenen Verschlüsselungslösungen zur Gewährleistung einer nach dem Stand der Technik sicheren Verschlüsselung aufsetzen. Sie informiert Unternehmen und Privatanwender darüber, wie sie ihre E-Mail-Kommunikation mit einfachen Mitteln schnell und effektiv schützen können. ■

BSI-LÖSUNG Gpg4win

Mit Gpg4win bietet das BSI eine eigene lizenzkostenfreie Verschlüsselungslösung für Windows-Betriebssysteme an, mit der jeder Nutzer E-Mails, Dateien oder Dateiordner einfach und kostenlos ver- und entschlüsseln kann. Der Quellcode dieser Lösung liegt für jeden offen, sodass seine Funktionsweise auch unabhängig vom BSI überprüft werden kann. Zudem kann durch Gpg4win die Integrität (Unverändertheit) und Herkunft (Authentizität) mittels digitaler Signaturen abgesichert und überprüft werden.

Weitere Informationen:
https://www.bsi.bund.de/Gpg4win

„Wir haben mit der Entdeckung von Gameover Zeus Cybercrime-Geschichte geschrieben“

Interview mit Prof. Dr. Christian Rossow

Der Informatiker Prof. Dr. Christian Rossow beforscht Schadprogramme und findet „Gameover Zeus“ – eine Malware, mit der Cyber-Kriminelle insgesamt mehr als hundert Millionen Dollar stehlen. Durch eine Schwachstelle im Code schleuste sich Rossow in das Botnetz der Kriminellen ein und machte die Malware unschädlich. Das BSI-Magazin hat Rossow zu seiner Arbeit interviewt.

Wie haben Sie Jewgeni Bogatschows Trojaner entdeckt?

Schadsoftware ist seit Jahren ein Kernthema meiner Forschungsarbeiten. Um der täglichen Flut von Malware Herr zu werden, haben wir an der Hochschule eine Analyseumgebung speziell für Schadsoftware erforscht, in der wir das Verhalten der Viren beobachten können. Das Prinzip ähnelt dabei dem Reagenzglas eines biologischen Virenlabors: Wir infizieren virtuelle Maschinen absichtlich mit einer Schadsoftware, um zu beobachten, welche Aktionen diese ausführt. So können wir sehen, wie sich die Schadsoftware im System einnistet, welche Prozesse sie manipuliert, welche Daten gestohlen werden und auch welche Kommunikation mit dem Angreifer stattfindet. „Gameover Zeus“ ist uns in dieser Analyseumgebung aufgefallen, da der Trojaner auffällig viele Kommunikationsverbindungen nach außen aufgebaut hat.

Wann wussten Sie, welchen „Fisch“ Sie „an der Angel“ hatten?

Von der Erkenntnis, einen interessanten Trojaner entdeckt zu haben, bis zur detaillierten Analyse der Schadsoftware vergingen etliche Monate. Wir haben eine Forschergruppe mit Beteiligung von Unternehmen wie Crowdstrike und weiteren Universitäten, zum Beispiel der VU Amsterdam und der Uni Bonn, gebildet, um Gameover Zeus mittels Techniken des „Reverse Engineerings“ zu analysieren. Dieser Prozess ist oft sehr aufwendig, da man lediglich aus dem vorliegenden Maschinencode die gesamte Semantik des doch recht komplexen Programms nachvollziehen muss. Als uns die technischen Details des Trojaners bekannt waren, konnten wir absehen, dass es sich um ein großes und relevantes Botnetz handelt. Spätestens aber seit das FBI in den USA uns um Kooperation bei der Bekämpfung des Trojaners bat, war uns klar, dass wir ein großes Kapitel der Cybercrime-Geschichte schreiben werden.

Wie konnten Sie ihm das Handwerk legen?

Zum ersten Mal hat man befürchtet, eine Schadsoftware vor sich zu sehen, die man nicht mehr „lahmlegen“ kann. Viele Botnetze kann man relativ einfach eliminieren, indem man die zentralen Kommandoserver abschaltet. Gameover Zeus verwendete jedoch ein dezentrales Kommunikationsschema, bei dem es keinen sogenannten Single-Point-of-Failure gab. Heißt: Selbst nach der Abschaltung einzelner Systeme hätte das Botnetz dank seiner Peer-to-Peer-Technologie weiterhin normal operieren können.

Kurzprofil Prof. Dr. Christian Rossow

Prof. Dr. Christian Rossow, Professor für IT-Sicherheit und Leiter der Forschungsgruppe „System Security“ am Center for IT-Security, Privacy and Accountability (CISPA) der Universität des Saarlandes.

An diesem Punkt setzte unsere Forschung an. Wir haben neue Verfahren erforscht, um die dezentrale Kommunikation des Netzwerks so zu manipulieren, dass die einzelnen Bots, also die infizierten Systeme, ihren Kontakt zu den anderen Teilnehmern des Netzwerks verlieren. Nachdem wir einige prototypische Angriffe auf das Botnetz getestet hatten, waren wir uns sicher, dass man das Netzwerk technisch abstellen kann. Dies wurde dann in einer gemeinsamen Operation mit dem FBI im Juni 2014 vorgenommen, wobei das FBI zeitgleich die Hintermänner verfolgte.

Gibt es den perfekten Code?

Gäbe es einen komplett fehlerfreien Code, dann wären einige Probleme der IT-Sicherheit gelöst. Die Praxis zeigt jedoch, dass selbst in Software, die hohen Industriestandards obliegt, nach wie vor Schwachstellen enthalten sind. Nicht umsonst sorgen sich viele Administratoren weltweit über sicherheitskritische Updates, die sich möglichst bald und vollständig auf den Systemen installieren müssen. In der Forschung beschäftigen wir uns deshalb sowohl mit Verfahren, um Schwachstellen aufzuspüren, als auch damit, die Ausnutzung dieser Schwachstellen zu erschweren.

Im Hinblick auf Gameover Zeus lässt sich sagen, dass die von uns für den Angriff auf das Botnetz ausgenutzten Schwachstellen prinzipiell geschlossen werden könnten. Peer-to-Peer-Botnetze wie Gameover Zeus sind zwar relativ komplex und deshalb auch fehleranfällig. Trotzdem ist es realistisch, dass wir zukünftig unzerstörbare dezentrale Botnetze vorfinden werden.

Wie ist der Kampf gegen Cyber-Angriffe mit Viren, Trojanern & Co zu gewinnen? Auf was müssen sich Unternehmen und Bürger in Zukunft einstellen?

Schadsoftware ist nun seit über 30 Jahren bekannt, und noch immer – oder gerade eben in der heutigen Zeit – suchen wir geeignete Gegenmaßnahmen. Die Angriffe werden dabei leider immer ausgefeilter. Ein derzeitiges Massenphänomen ist beispielsweise Ransomware, die Opfer damit erpresst, gesperrte Systeme oder verschlüsselte Dateien erst nach einer Zahlung wieder preiszugeben.

Neben einer auf die Massen ausgelegten Schadsoftware, die weltweit millionenhaft Systeme infiziert, kommt es zunehmend auch zu gezielten und politisch motivierten Angriffen. Diese Angriffe sind deutlich schwerer zu erkennen, da die Angreifer zum einen per Social Engineering zunächst Informationen über die potenziellen Opfer ausspähen, um die Zielpersonen mit einer höheren Wahrscheinlichkeit zu erreichen. Zum anderen sind gezielte Angriffe eben auch nur an sehr wenigen Stellen überhaupt feststellbar und haben somit eine höhere Chance, unerkannt im Hintergrund zu agieren.

Herr Prof. Dr. Rossow, wir danken Ihnen für das Gespräch.

U.S. Department of Justice
Federal Bureau of Investigation

Christian Rossow
Saarland University

In recognition of your outstanding assistance to the FBI in connection with its investigative efforts.

Your cooperation was of immeasurable help to our representatives. I share their gratitude for your support, which assisted them in carrying out their responsibilities. You can take pride in the role you played in the success achieved, and my associates and I congratulate you on a job well done.

June 2014
Date

James B. Comey
Director

Verliehene FBI-Urkunde für Prof. Dr. Christian Rossow

IT-SICHERHEIT IN DER INDUSTRIE 4.0

von Dr. Christian Haas, Leiter der Forschungsgruppe Sichere vernetzte Systeme am Fraunhofer IOSB

Kurzprofil Dr. Christian Haas

Dr. Christian Haas ist seit 2015 für das Fraunhofer IOSB tätig und leitet dort die Forschungsgruppe Sichere vernetzte Systeme. Er studierte Informatik am Karlsruher Institut für Technologie und promovierte dort am Institut für Telematik bei Prof. Zitterbart mit dem Thema Evaluierung der Energieeffizienz von Sicherheitsmechanismen in drahtlosen Sensornetzen. Die Gruppe Sichere vernetzte Systeme beschäftigt sich hauptsächlich mit Forschungs- und Entwicklungsthemen im Bereich Sicherheit für die industrielle Produktion und kritischen Infrastrukturen.

Geeignete Testumgebungen sind unerlässlich

Moderne Produktionsanlagen sind hochgradig vernetzt. Steuerungen und eingebettete Systeme kommunizieren selbstständig miteinander, Planungssysteme aus der Cloud berechnen Auftragsschritte und Maschinenbelegungen, Anlagenführer überwachen und steuern aus der Ferne, Wartungspersonal greift weltweit zu und führt Konfigurationsänderungen aus. Zum Schutz gegen Schäden oder Produktionsausfälle sind geeignete Maßnahmen zur Vermeidung von Sicherheitsvorfällen dringend erforderlich. IT-Sicherheit, im Sinne von Security, der Sicherheit gegen Angriffe, ist eines der erfolgskritischen Themen, die als Voraussetzung für funktionierende und umfassende Industrie-4.0-Lösungen bearbeitet und sichergestellt werden müssen.

Seit einiger Zeit existieren bereits offene Standards (z.B. IEC 62443) und Lösungen, die Betreibern von Produktionsanalagen oder Herstellern von Komponenten und Systemen Vorgehensweisen und technische Lösungen bieten, geeignete Sicherheitsmaßnahmen zu entwickeln und umzusetzen. Dennoch zeigt der Alltag in heutigen Produktionsanlagen, dass in vielen Fällen kaum Sicherheitsmaßnahmen umgesetzt beziehungsweise die vorhandenen Sicherheitsmaßnahmen nicht konsequent genutzt werden. Dies liegt häufig an dem Zusammentreffen unterschiedlicher Kompetenzbereiche, beispielsweise IT (Information Technology) und OT (Operational Technology), aber auch am Fehlen von geeigneten Test- und Schulungsumgebungen, um existierende Sicherheitsmaßnahmen kennenzulernen und auszuprobieren.

Um Unternehmen bei diesen Problemen zu helfen, hat das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB mit dem IT-Sicherheitslabor eine ideale Testumgebung entwickelt, um reale Produktionsszenarien nachzustellen, Sicherheitsmaßnahmen zu testen und Auswirkungen von Angriffen zu untersuchen. Das speziell für Produktions- und Automatisierungstechnik ausgestattete IT-Sicherheitslabor bietet eine gesicherte Umgebung, um die gesamte hierarchische IT-Infrastruktur einer Fabrik mit Büronetz sowie Netzen für Produktionsplanung, -überwachung und -steuerung nachzubilden. Diese wirklichkeitsnahe IT-Netzwerkumgebung ist teilweise aus typischen industriellen Netzelementen aufgebaut sowie in einer Cloud als virtuelle Netzwerkstruktur abgebildet.

Im Rahmen des IT-Sicherheitslabors arbeiten wir unter anderem an der Weiterentwicklung von Werkzeugen und Sicherheitsmechanismen speziell für industrielle Produktionsumgebungen. Die Einrichtungen des IT-Sicherheitslabors werden daneben auch zu Ausbildungs- und Trainingszwecken genutzt, um, beispielsweise im Rahmen von Schulungen, zu vermitteln, wie IT-Sicherheit für Industrie 4.0 schon mit den heute vorhandenen IT-Sicherheitsmechanismen umgesetzt werden kann. ■

Mit Sicherheit
kein Job wie jeder andere

Deutschlands attraktivste Arbeitgeber 2016
TOP 100
trendence ABSOLVENTEN

Wir suchen Sie! www.bsi.bund.de/jobs

IMPRESSUM

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI), 53175 Bonn
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Referat B23 – Öffentlichkeitsarbeit und Presse, Godesberger Allee 185–189, 53175 Bonn Telefon: +49 (0) 22899 9582-0, E-Mail: oeffentlichkeitsarbeit@bsi.bund.de, Internet: www.bsi.bund.de
Stand:	September 2016
Texte und Redaktion:	Stephan Kohzer und Nora Basting, Bundesamt für Sicherheit in der Informationstechnik (BSI); Joachim Gutmann, GLC Glücksburg Consulting AG; Fink & Fuchs Public Relations AG (FFPR)
Konzept, Redaktion und Gestaltung:	Fink & Fuchs Public Relations AG (FFPR), Berliner Straße 164, 65205 Wiesbaden, Internet: www.ffpr.de
Druck:	Druck- und Verlagshaus Zarbock GmbH & Co KG, Sontraer Str. 6, 60386 Frankfurt a.M., Internet: www.zarbock.de
Artikelnummer:	BSI-Mag 16/704-2
Bildnachweise:	Titel: Mopic/fotolia, silvertiger/depositphotos; S. 1: Stephan Kohzer/BSI, S. 4: Matthias Gärtner/BSI (o.l.), ENISA (o.r.), trendence Graduate Barometer (u.l.); S. 5: Informatiksteuerungsorgan des Bundes ISB, Schweiz (o.l.), CSCG (u.r.); S. 6–7: NürnbergMesse; S. 8: blobbotronic/fotolia; S. 9: LOGO eIDAS; S. 10: blobbotronic/fotolia; S. 11: ANSSI (oben.), R.Winkler; S. 12: ANSSI/Picturetank-Gaillardin; S. 13–14: R.Winkler; S. 16–17: R. Winkler; S. 18: BSI; S. 19: Stephan Kohzer/BSI; S. 21: BSI; S. 22: Stephan Kohzer/BSI; S 24: Stephan Kohzer/BSI; Nationales Cyber-Abwehrzentrum; S. 26: Ilja C. Hendel/BMF; S. 27: Henning Schacht/BMI; S. 28–33: Johannes Dominik Weber; S. 34–35; S. 36: Stephan Kohzer/BSI; S. 38–39: Marcus Frey/VISUAL FACILITATORS; S. 41: secunet Security Networks AG; S. 42: ProPK; S. 43: Herrndorff/fotolia; S. 45: gst/shutterstock; S. 47: Prof. Dr. Christian Rossow, S. 48-49: Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB (u.l.); Dr. Christian Haas (o.r.); S. 50: topseller/shutterstock.

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