Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Magazin 2017/02

Mit Sicherheit

Informationssicherheit als Voraussetzung für Digitalisierung

CYBER-SICHERHEIT

Das BSI vor Ort im Einsatz

DAS BSI

Cyber-Sicherheit in der Digitalisierung

IT-SICHERHEIT IN DER PRAXIS

Ohne Kooperation geht es nicht

EDITORIAL

Alles aus einer Hand

Die massiven Cyber-Angriffe der jüngsten Vergangenheit haben gezeigt: Die großen Digitalisierungsprojekte in Deutschland, die Nutzung des Internets der Dinge durch die Bürgerinnen und Bürger sind nur dann ein Gewinn für alle, wenn ein angemessenes Sicherheitsniveau gewährleistet ist.

Das IT-Sicherheitsgesetz, die KRITIS-Verordnungen, die Regelungen im Telekommunikations- und im NIS-Umsetzungsgesetz schaffen einen soliden Rahmen für mehr IT-Sicherheit. Sie verpflichten zahlreiche Akteure, für ein angemessenes Sicherheitsniveau zu sorgen und Vorfälle zu melden. Der Fokus des BSI geht darüber hinaus. Als nationale Cyber-Sicherheitsbehörde ist es unser Anliegen, die Informationssicherheit in der Digitalisierung zu gestalten. Daher adressieren wir auch diejenigen, die nicht unmittelbar den genannten Regulierungen unterliegen.

Kein Unternehmen verkündet gern, dass es einem Cyber-Angriff zum Opfer fiel, kein PC-User gibt gern zu, dass Ransomware all seine Daten unwiederbringlich verschlüsselte. Sie müssen der Instanz vertrauen, an die sie sich in solchen Fällen wenden.

Eine repräsentative Umfrage des BSI ergab zuletzt, dass 87 Prozent der Befragten Sicherheit im Internet für wichtig halten, sich aber weniger als die Hälfte nach eigenen Angaben mit diesem Thema auskennt. Zwei Drittel nannten Sicherheitstests, Sicherheitsrichtlinien und klare Haftungsregelungen als Beitrag zu mehr Sicherheit im Cyber-Raum.

„Als nationale Cyber-Sicherheitsbehörde ist es unser Anliegen, die Informationssicherheit in der Digitalisierung zu gestalten.“

Ergänzend ergab eine von DIVSI veröffentlichte Studie, dass vier von fünf Befragten die Einführung eines Sicherheitssiegels für vertrauenswürdige Angebote und Dienstleistungen im Internet befürworten. 85 Prozent der Internetnutzer in Deutschland stimmen der Aussage zu, dass der Staat sich stärker um das Thema Sicherheit im Internet kümmern sollte und 80 Prozent sprachen sich für eine zentral zuständige Stelle in Deutschland für alle Aufgaben im Zusammenhang mit Sicherheit im Internet aus.

Das BSI ist bereits diese zentrale Stelle: Es verfügt in seiner heutigen Gestalt über ein wichtiges Alleinstellungsmerkmal - seine interne Vernetzung. Nirgendwo sonst arbeiten Experten aus den Spezialgebieten der Informationssicherheit so eng und unmittelbar zusammen. Diese Bündelung und Vernetzung von Cyber-Sicherheitsexpertise in einer Behörde gibt dem BSI seine in Deutschland einzigartige Schlagkraft. Darum können Erkenntnisse aus der operativen Cyber-Abwehr ohne Zeitverzug in Prävention, Standardisierung und Zertifizierung eingebracht werden. Darum fließen neue Erkenntnisse aus der Grundlagenarbeit der Kryptografie in die Abwehrfähigkeiten des BSI ein. Darum kann dieses Wissen verständlich aufbereitet und kommuniziert werden. Und darum initiiert das BSI den Dialog mit Staat, Wirtschaft und Gesellschaft und wirbt um Akzeptanz für Themen der Cyber-Sicherheit.

Einige dieser spannenden Themen finden Sie in unserem BSI-Magazin.
Ich wünsche Ihnen eine anregende Lektüre!

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik

INHALT

AKTUELLES

10 Jahre UP KRITIS

„Wir sind UP KRITIS“ – 10 Jahre ganzheitlicher Schutz kritischer Infrastrukturen

Anlässlich des zehnjährigen Bestehens der öffentlich-privaten Partnerschaft fand am 30. Mai 2017 in Berlin eine Tagung von Betreibern Kritischer Infrastrukturen, Behörden und Verbänden statt. Unter dem Motto „Wir sind UP KRITIS!“ tauschten sich rund 200 Teilnehmer über aktuelle Herausforderungen beim ganzheitlichen Schutz der Kritischen Infrastrukturen aus.

Um einen Ausfall der für das Gemeinwohl wichtigen kritischen Dienstleistungen zu verhindern, verfolgt der UP KRITIS dabei den All-Hazards-Ansatz, der mögliche Gefahren sowohl aus der physischen als auch der Cyber-Welt umfasst. Ziel des UP KRITIS ist die Sicherstellung der Versorgung der Bevölkerung mit den essenziellen Gütern und Dienstleistungen der Kritischen Infrastrukturen, beispielsweise Energie, Wasser, Transport oder Ernährung. Auch für die Zukunft ist es Ziel des BSI und der Betreiber Kritischer Infrastrukturen, deren Schutz konsequent weiter zu verbessern.

Weitere Informationen: https://www.bsi.bund.de/UP-KRITIS

Abschlussveranstaltung SuSi

Sichere digitale Gesellschaft

Am 7. September 2017 stellte das BSI in der Kalkscheune Berlin die Ergebnisse des Projektes „Digitale Gesellschaft: smart & sicher“ (SuSi) vor. Mit Vertretern aus Zivilgesellschaft, Wirtschaft, Verwaltung und Wissenschaft wurden die im gemeinsamen Dialog erarbeiteten „Impulse für eine smarte und sichere digitale Gesellschaft“ diskutiert.

Mehr zum Projekt auf Seite 58

ECSM

European Cyber Security Month 2017

Der Oktober steht auch in diesem Jahr ganz im Zeichen der Cyber-Sicherheit: Unter der Federführung der ENISA (European Network and Information Security Agency) werden bereits zum fünften Mal europaweit Aktionen für EU-Bürger/-innen, Organisationen und Unternehmen rund um Cyber- und IT-Sicherheit angeboten. Ziel ist es, für diese Themen zu sensibilisieren und das Bewusstsein für Cyber-Bedrohungen zu schärfen. Das BSI ist die nationale Koordinierungsstelle für den ECSM in Deutschland und ruft Organisationen auf, sich mit eigenen Aktionen für mehr Cyber-Sicherheit zu engagieren.

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

it-sa 2017

Hohe Internationalität in neuen Hallen

Größer und internationaler – unter diesen Vorzeichen belegt die Fachmesse it-sa dieses Jahr zwei Hallen. Rund 580 Aussteller präsentieren vom 10. bis 12. Oktober im Messezentrum Nürnberg IT-Security-Lösungen aus den Bereichen Hard- und Software sowie Forschung und Dienstleistung. Internationale Gemeinschaftsstände aus Frankreich, Israel und der Tschechischen Republik bereichern das Messeangebot. IT-Sicherheitsverantwortliche und Entscheider dürfen sich auch auf vier offene Foren mit Vorträgen und Diskussionsrunden in den Messehallen und das begleitende Kongressprogramm freuen. Auch dieses Jahr findet am 11. Oktober ein IT-Grundschutz-Tag statt, zudem wird im Rahmen der it-sa das fünfjährige Bestehen der Allianz für Cyber-Sicherheit gefeiert.

Weitere Informationen: www.it-sa.de

Secure Pim iOS

BSI ermöglicht sichere Nutzung von iPhones und iPads in der Verwaltung

Das BSI hat bereits 2015 die Lösung SecurePIM Government SDS des Herstellers Virtual Solution vorläufig für den Einsatz in der Bundesverwaltung zugelassen. Nach Fortführung der Sicherheitsevaluierung mit dem Ziel der finalen Zulassung hat das BSI die Einsatz- und Betriebsbedingungen entsprechend den bisherigen Ergebnissen angepasst, sodass sich auch für Länder, Kommunen und Unternehmen im Bereich der Kritischen Infrastrukturen die Möglichkeit ergibt, iPhones und iPads mit SecurePIM in der vom BSI zugelassenen Variante für eingestufte Informationen zu nutzen. Bisher war der Betrieb von SecurePIM nur im Regierungsnetz möglich. Nun ist darüber hinaus auch der Einsatz in anderen Netzen möglich, in denen eingestufte Daten gespeichert, übertragen und verarbeitet werden.

BSI INTERNATIONAL

SOUVERÄNITÄT WAHREN IM ZEITALTER DER DIGITALISIERUNG

von Dr. Martin Aulbach, Referat Vorgaben und Entwicklungen von VS-IT-Systemen

Produktionsprozesse in der globalisierten Welt

Die Handlungsfähigkeit und Souveränität Deutschlands muss auch im Zeitalter der Digitalisierung gewahrt sein. So fordert es eine Leitlinie der Cyber-Sicherheitsstrategie der Bundesregierung. Ein wichtiges Instrument dafür ist eine wettbewerbsfähige nationale IT-Industrie, die an das hiesige Recht gebunden ist. Nur dann können Forderungen an die IT-Sicherheit von Prozessen und Produkten durchgesetzt werden.

In Deutschland gibt es strenge Regelungen zur Speicherung und Verarbeitung personenbezogener Daten. Sie können im Allgemeinen aber nicht angewendet und durchgesetzt werden, wenn zum Beispiel die E-Mail-Dienste oder Cloud-Speicher von im Ausland ansässigen Unternehmen verwendet werden. So hat beispielsweise Yahoo als international agierendes Unternehmen es kürzlich abgelehnt, dem BSI Einzelheiten zu einem Diebstahl von Zugangsdaten zu einer Milliarde E-Mail-Konten mitzuteilen, obwohl auch deutsche Bürgerinnen und Bürger von diesem Vorfall betroffen waren.

Die meisten IT-Produkte beziehungsweise deren Teilkomponenten werden heute nicht mehr in Deutschland oder der EU hergestellt. In der Halbleiterindustrie ist darüber hinaus eine zunehmende Marktkonsolidierung zu beobachten. Dadurch verringert sich die Auswahl an Herstellern für diese Bauteile. Hat man aber über den Herstellungsprozess oder die Lieferketten keine vollständige Kontrolle, können Manipulationen am fertigen IT-System nicht mehr ausgeschlossen werden. Dies ist kein abstraktes Bedrohungsszenario: Aktuelle Medienberichte lassen vermuten, dass auf 700 Millionen weltweit verkauften Android-Geräten eine ab Werk installierte Hintertür in der von einem chinesischen Werbeunternehmen entwickelten Firmware gefunden wurde.

VERTRAUENSWÜRDIGE HERSTELLUNGSPROZESSE

International agierende Unternehmen, deren Firmensitz nationales Recht nicht zur Anwendung kommen lässt; IT-Produkte, die in anderen Ländern entwickelt wurden; Lieferketten rund um die Welt: Das alles sind die logischen Konsequenzen einer globalisierten Industrieproduktion, die Herausforderungen für die IT-Sicherheit mit sich bringen. Auf diese Herausforderungen reagiert das BSI mit verschiedenen Maßnahmen. Sie sollen vertrauenswürdige Herstellungsprozesse ermöglichen und fördern. So positioniert sich das BSI auf strategischer Ebene dafür, Open Source beziehungsweise Freie Software einzusetzen. Durch die uneingeschränkte Einsicht und Weiterentwicklung von Quellcodes wird die IT-Sicherheit gestärkt. Das BSI tritt dabei sowohl als Anwender als auch Anbieter von Freier Software auf. Zu den vom BSI entwickelten oder geförderten Produkten unter freien Lizenzen gehören beispielsweise Gpg4win, OpenVAS und SINA, eine Abkürzung für Sichere-Inter-Netzwerk-Architektur. Diese auf Linux basierende Produktfamilie wird unter anderem zur sicheren Kommunikation zwischen den deutschen Botschaften und dem Auswärtigen Amt verwendet. Mit SINA ist eine sichere Speicherung, Bearbeitung und Übertragung von amtlich geheim zu haltenden Verschlusssachen bis zur Geheimhaltungsstufe GEHEIM möglich.

EIGENENTWICKLUNG ALS ALTERNATIVE

Ist keine freie Einsicht in den Quellcode oder den genauen Aufbau eines IT-Produktes möglich, kann sich das BSI durch eine Kooperationsvereinbarung mit dem Hersteller von der korrekten Funktionalität des Produktes überzeugen. Darüber hinaus kann das BSI die von der Bundesverwaltung benötigten IT-Produkte beziehungsweise deren Teilkomponenten selbst entwickeln. Dies erfolgt im Rahmen von Ausschreibungen. Dafür können sich Unternehmen bewerben, die bereit sind, die Forderungen des BSI hinsichtlich größtmöglicher Transparenz des Entwicklungsprozesses zu erfüllen. Dies war beispielsweise bei der ursprünglichen Ausschreibung von SINA im Jahr 1999 der Fall, bei der die secunet Security Networks AG den Zuschlag erhielt.

Wenn es in einem IT-System zur Verarbeitung von Verschlusssachen keine Alternative zum Einsatz von nicht vertrauenswürdigen Teilkomponenten gibt, kann das Risiko schließlich noch durch eine geeignete Konzeption des IT-Gesamtsystems auf ein akzeptables Maß reduziert werden. In diesem Fall werden beispielsweise von den Experten des BSI die nicht vertrauenswürdigen Bestandteile so stark vom übrigen System isoliert, dass sie keinen Schaden anrichten können. ■

Letzte Untersuchung vor der Hauptsitzung

G20 – Lauschabwehr

Vertraulichkeit sicherstellen

Beratungen zu international relevanten politischen Themen, Vieraugengespräche und das Ringen um Formulierungen in Verhandlungen bestimmen das Geschehen bei politischen Ereignissen wie dem G20-Gipfel in Hamburg im Juli 2017. Die Lauschabwehr des BSI sorgte mit ihrer technischen Expertise dafür, dass all dies in einem vertraulichen und abhörsicheren Umfeld geschehen konnte.

Familienfoto der G20-Staats- und Regierungschefs und der geladenen G20-Teilnehmer

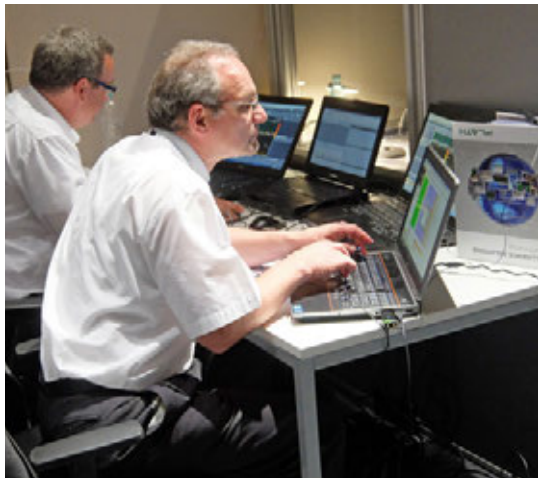


Bild links: Messungen am IT-Netzwerk hinsichtlich Auffälligkeiten mit einem speziellen Analysator

Bild rechts: BSI-Arbeitsplatz zur Überprüfung des Hochfrequenzspektrums, auch hinsichtlich Mobilfunkaktivitäten und IMSI-Catchern, im Konferenzbereich

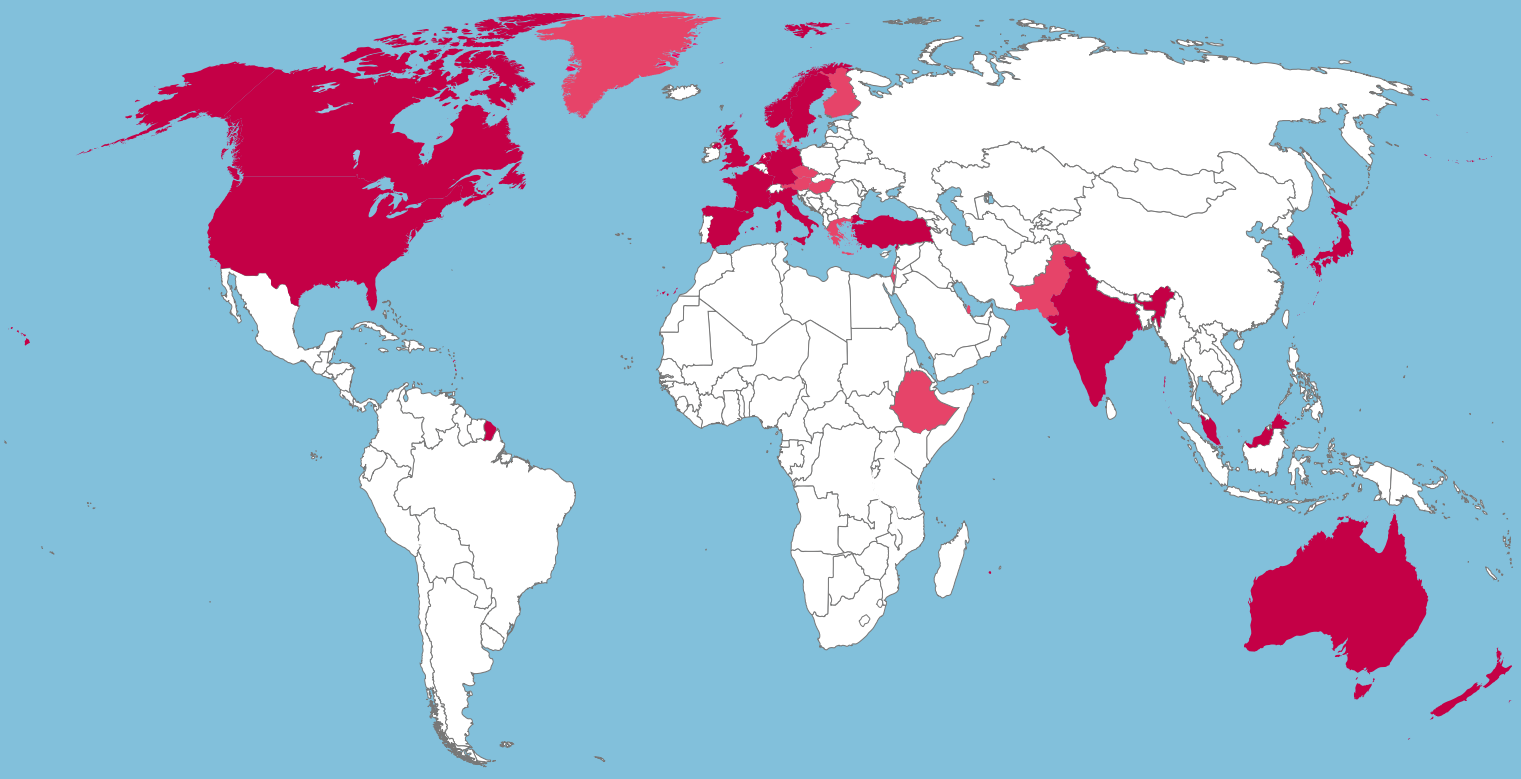
Bild links: Im Messfahrzeug wurden die Sendeaktivitäten durch Mitarbeiter des BSI überwacht und hinsichtlich Auffälligkeiten bewertet

Bild rechts: Die Dolmetscher/-innen wurden gebeten, ihre Mobiltelefone außerhalb der Dolmetscherkabinen zu deponieren, sodass damit keine vertraulichen Gespräche aufgezeichnet oder nach außen übermittelt werden konnten

WELTWEIT ZERTIFIZIERT

von Matthias Intemann, Referatsleiter Zertifizierung von Software und COTS-Produkten

Mehr als 25 Nationen arbeiten zusammen



DIE COMMON CRITERIA – DAS CCRA

Zertifizierende Nationen
Australien, Deutschland, Frankreich, Großbritannien, Japan, Indien, Italien, Kanada, Malaysia, Neuseeland, Niederlande, Norwegen, Schweden, Spanien, Südkorea, Singapur, Türkei, USA

Anerkennende Nationen
Äthiopien, Dänemark, Finnland, Griechenland, Israel, Österreich, Pakistan, Katar, Tschechien, Ungarn

Die Produktzertifikate des BSI nach dem internationalen Standard Common Criteria werden weltweit und speziell in Europa anerkannt. Grundlage dafür sind die beiden Anerkennungsabkommen Senior Officials Group Information Systems Security (SOG-IS) und Common Criteria Recognition Agreement (CCRA). Das BSI trägt aktiv zu beiden Abkommen bei, um den Wert der Zertifikate zu stärken und die nationalen Interessen Deutschlands umzusetzen.

AKTUELLE ENTWICKLUNGEN DES CCRA

Das CCRA ist ein weltweites Abkommen, das derzeit 28 Nationen unterschrieben haben. Zuletzt traten Äthiopien und Katar dem Abkommen bei. Das CCRA ist im Hinblick auf die Prüftiefe anerkannter Zertifikate sehr eingeschränkt, stärkt jedoch die Common Criteria als internationalen Standard. Im April 2017 wurde die neue Fassung in der Version 3.1 Revision 5 veröffentlicht. Parallel finden Arbeiten an der Version 4.0 der Common Criteria in der Arbeitsgruppe/ Working Group 3 (WG 3) des Subkomitees 27 (SC 27) des Internationalen Instituts für Normung (ISO) und der International Electrotechnical Commission (IEC) (ISO SC27 WG3) statt, da die CCRA-Mitglieder ohne weitere Unterstützung die grundlegende Fortschreibung nicht leisten konnten. Auf diese Weise wird die internationale Industrie umfangreich beteiligt.

SOG-IS SOLL IN EUROPA HARMONISIEREN

SOG-IS als europäisches Abkommen hingegen konzentriert sich sehr stark darauf, die Evaluationsmethodologie zu harmonisieren, und unterstützt dadurch nationale und europäische Anwendungsfälle der Zertifizierung. Dem Abkommen sind bislang 13 europäische Staaten beigetreten, zuletzt Polen, Kroatien und Luxemburg. Neben der technischen Domäne im Bereich der „Smartcards and Similar Devices“ wurde der Bereich „Hardware Devices with Security Boxes“ durch Gründung einer Untergruppe für Embedded Devices (JEDS) in der Harmonisierung gestärkt. Hier werden Evaluationsmethodologien und Qualifikationsvoraussetzungen für Prüfstellen zwischen den Teilnehmern harmonisiert und es wird der Stand der Technik dokumentiert. Darüber hinaus findet ein enger Austausch mit Vertretern der europäischen Kommission und der Europäischen Agentur für Netz- und Informationssicherheit (European Network and Information Security Agency, ENISA) statt. So soll Transparenz geschaffen und europäische Vorhaben, etwa die Erstellung eines europäischen IT-Sicherheitszertifizierungsrahmens, unterstützt werden.

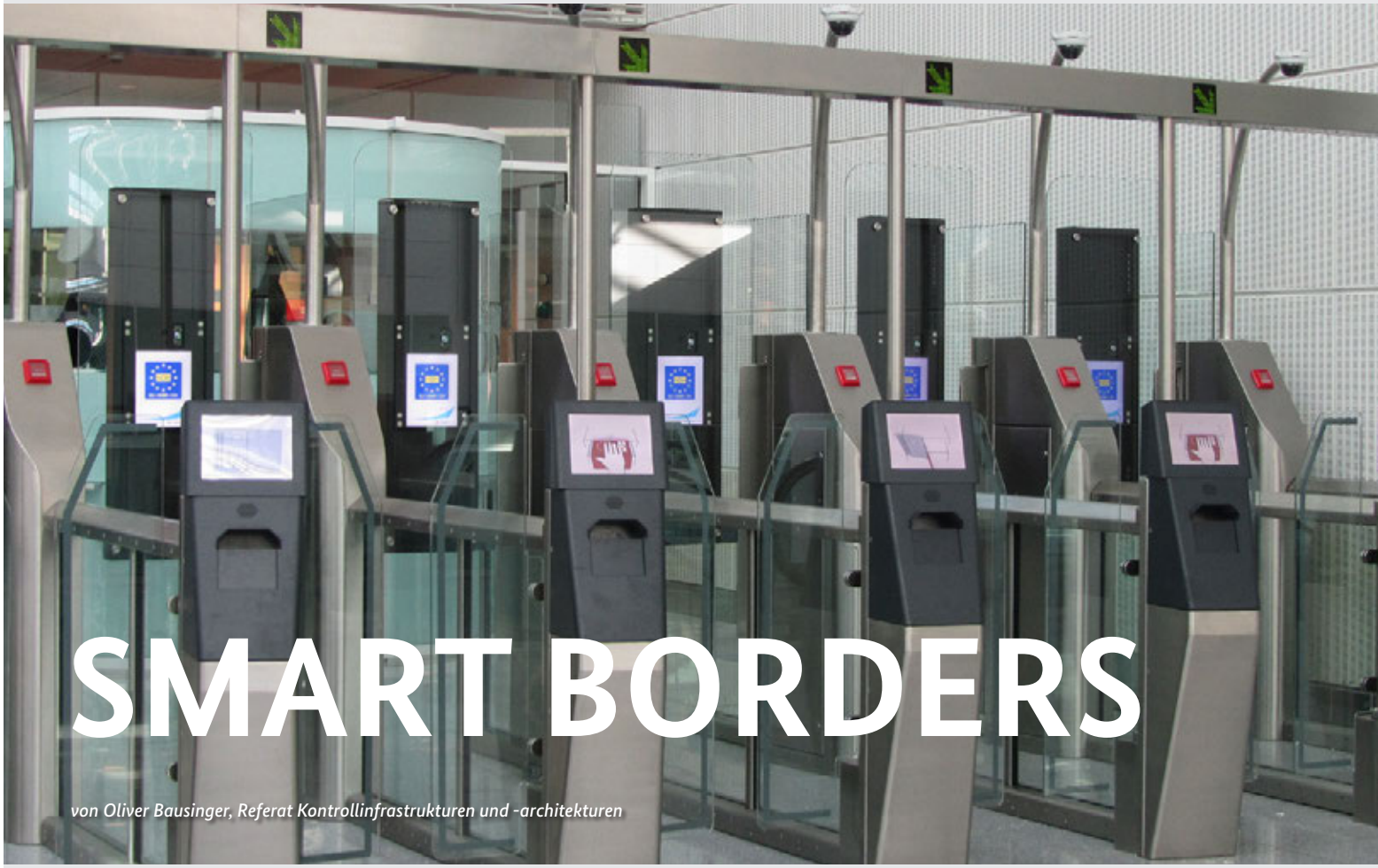
ZIELE UND AKTIVITÄTEN DES BSI

Das BSI tritt für marktgerechte Zertifizierungsoptionen ein. Dieses Ziel wird erreicht durch eine enge Kooperation mit der Industrie und den für die Regulierungen verantwortlichen Institutionen.

Indem dabei gleichermaßen niedrige, mittlere und hohe Prüftiefen unterstützt werden, ermöglicht das BSI, angepasste Zertifikate für unterschiedliche Anwendungsszenarien und verschiedene Zielgruppen auszustellen. So kann ein Hersteller zum Beispiel auch die Beschaffungsanforderungen der USA erfüllen. Diese Position vertritt das BSI auch für Anwendungsfälle in Europa zum Beispiel in Arbeitsgruppen zur Schaffung eines europäischen Zertifizierungsframeworks. Sie trägt damit zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) bei.

Darüber hinaus treibt das BSI proaktiv die Harmonisierung der Krypto-Evaluierungen unter Anwendung der Common Criteria voran – sowohl im CCRA für niedrige Prüftiefen, um eine Alternative zu bestehenden Krypto-Validierungen bieten zu können, als auch im SOG-IS für hohe Prüftiefen. Ferner wird derzeit die Zertifikatsgültigkeit der zertifizierenden Nationen im CCRA und in SOG-IS harmonisiert. ■

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



SMART BORDERS

von Oliver Bausinger, Referat Kontrollinfrastrukturen und -architekturen

EasyPASS-System der Bundespolizei am Flughafen München

BSI pilotiert neues Europäisches Ein- und Ausreiseregister

Nach dem im Verordnungsentwurf vorliegenden neuen Europäischen Ein- und Ausreiseregister (Entry-Exit-System, EES) soll jeder Grenzübertritt eines Drittstaatlers über eine der Schengen-Außengrenzen in einem Europäischen Register für bis zu fünf Jahre gespeichert werden. Neben biografischen Daten sollen auch ein biometrisches Lichtbild und Fingerabdrücke erfasst werden. Das BSI pilotiert seit 2015 gemeinsam mit der Bundespolizei die neuen Prozesse des EES.

Rechts oder links? Das ist die Frage, die sich Reisende stellen müssen, wenn sie aus dem Ausland an einer Grenzkontrolle an einem deutschen Flughafen oder an einer anderen Außengrenze des Schengen-Raums ankommen. Rechts können alle Freizügigkeitsberechtigten aus den derzeit 32 Ländern passieren, die den vereinfachten Ein- und Ausreiseregeln unterliegen. Links heißt es für alle Drittstaatler, die aus anderen Ländern stammen. Manche mussten vorab ein Einreisevisum beantragen, andere dürfen derzeit ohne jede Voranmeldung in den Schengen-Raum einreisen. Der gemeinsame Grenzkodex (benannt nach der Gemeinde Schengen in Luxemburg, wo das erste Abkommen 1985 unterzeichnet wurde) regelt die Aufgaben und Pflichten der Grenzkontrolle bei der Ein- und Ausreise in den gemeinsamen Schengen-Raum und ist dabei für alle beteiligten Staaten unmittelbar geltendes Recht. Ihn einzuhalten ist elementar wichtig, da es innerhalb der Schengen-Staaten im Regelfall keine Kontrollen an Binnengrenzen mehr gibt. So führt Deutschland selbst nur noch an Luft- und Seegrenzen ständige Grenzkontrollen durch, jedoch nicht mehr an den Landgrenzen.

EASYPASS – AUTOMATISIERTE GRENZKONTROLLE FÜR FREIZÜGKEITSBERECHTIGTE

Deutschland hat 2014 begonnen, an allen Großflughäfen automatisierte Schleusensysteme einzusetzen. Das

Unterzeichnung der gemeinsamen Verwaltungsvereinbarungen zwischen BSI, BPOL und BVA (2. Juni 2017 in Frankfurt)

Präsidenten BPOL, BVA und Abteilungsleiter D mit Projektverantwortlichen der einzelnen Behörden vor Smart Borders Pilot Installation am Flughafen Frankfurt

EasyPASS-System erlaubt es, im Regelfall den Grenzübertritt vollständig automatisiert durchzuführen. Dabei wird das digitale Lichtbild aus dem elektronischen Chip des Reisepasses ausgelesen und mit einem live aufgenommenen Gesichtsbild biometrisch abgeglichen. Sofern der Pass als kryptografisch echt und der Identitätsabgleich als erfolgreich bewertet werden, kann der Reisende die Grenze ohne eine weitere manuelle Prüfung durch den Grenzbeamten passieren.

Das BSI prüft in enger Abstimmung mit der Bundespolizei die Systeme regelmäßig auf Schwachstellen, betreibt die notwendige Krypto-Infrastruktur im Rahmen des Nationalen Public Key Directory und sorgt mit seinen Vorgaben dafür, dass sowohl die Dokumentenprüfung als auch die biometrischen Verfahren stets auf dem aktuellen Stand der Technik sind.

NEUES EUROPÄISCHES EIN- UND AUSREISEREGISTER FÜR DRITTSTAATLER

Um auch die Abfertigung von Drittstaatlern mit einem modernen Verfahren auf ein vergleichbar hohes Sicherheitsniveau zu bringen, soll nun ein Europäisches Ein- und Ausreiseregister (EES) eingeführt werden. Nach dem Verordnungsentwurf der EU-Kommission, der voraussichtlich im Herbst 2017 vom Europäischen Parlament beschlossen wird, soll jeder Grenzübertritt eines Drittstaatlers über eine der Schengen-Außengrenzen für bis zu fünf Jahre im EES gespeichert werden. Hierbei sollen nicht nur die üblichen biografischen Daten wie Name, Geburtsdatum etc. gespeichert werden, sondern auch ein biometrisches Lichtbild und vier Fingerabdrücke. Dadurch soll eine deutlich bessere Identifikation des Reisenden ermöglicht werden. Mehrfachidentitäten können dann durch den biometrischen Abgleich aufgedeckt werden. Des Weiteren können Reisende, die ihre berechtigte Aufenthaltsdauer überschritten haben, leicht ermittelt werden.

EFFIZIENZ DURCH SELFSERVICE

Das BSI pilotiert seit 2015 gemeinsam mit der Bundespolizei die neuen Prozesse des EES. Früh stellte sich dabei heraus, dass sich mit seiner Einführung der Gesamtprozess der Grenzkontrolle signifikant ändern muss. Die biometrische Erfassung von Reisenden direkt am Schalter, aber auch die deutlich komplexere technische Anbindung der Flughäfen über mehrere Ebenen bis hin zum zentralen EES stellen die operativen Behörden vor erhebliche Herausforderungen, um sowohl die Kontrolltiefe als auch den zügigen Passagierfluss aufrechtzuerhalten.

Um diesen Herausforderungen zu begegnen, wurden Kiosk-Systeme erprobt, die dem Grenzkontrollschalter vorgelagert sind. Dort kann der Reisende im Selfservice die Dokumentenprüfung, die Erfassung beziehungsweise Verifikation der biometrischen Merkmale und die obligatorische grenzpolizeiliche Befragung durchführen. Im Anschluss geht er zum Grenzkontrollschalter, wo dem Beamten dann bereits alle relevanten technischen Prüfergebnisse vom Kiosk vorliegen. Dieser muss in der abschließenden Bewertung im Normalfall nur noch den Grenzübertritt genehmigen. Das BSI konnte im Rahmen des Pilotprojekts nachweisen, dass der Zeitbedarf im Vergleich zum aktuellen Verfahren ohne EES in etwa gleich bleibt.

DIGITALISIERUNG DER GRENZKONTROLLE

Mit der Einführung von biometrischen Verfahren in die Prozesse der Grenzkontrolle rückt die Sicherheit der eingesetzten Systeme besonders in den Fokus. Das BSI wird in den kommenden Jahren die Technologieentwicklung der Grenzkontrolle mitgestalten, um sicherzustellen, dass die neuen Systeme zuverlässig und sicher betrieben werden. Hierzu wird das BSI eine Projektpartnerschaft mit der Bundespolizei und dem Bundesverwaltungsamt eingehen, um die technologischen Herausforderungen einer sicheren Grenzkontrolle zu gestalten ■

Weitere Informationen: https://www.easypass.de/

CYBER-SICHERHEIT

Das BSI vor Ort im Einsatz

von Stefan Ritter und Timo Steffens, Referat CERT-Bund

Beispiele mobiler Vorfallsbearbeitung bei fortschrittlichen Spionageangriffen

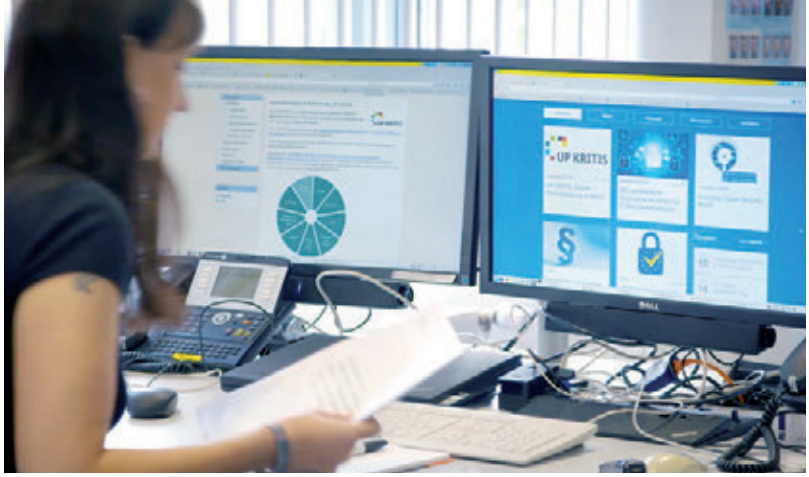
ADVANCED PERSISTENT THREATS (APT)

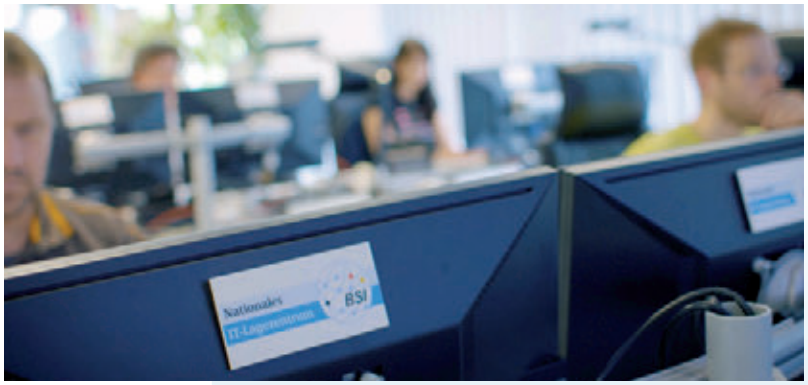
Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer persistenten (dauerhaften) Zugriff zu einem Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

Der Anruf im Lagezentrum des BSI kommt am Nachmittag. Wie eigentlich immer, denn den Vormittag braucht der Betroffene meist, um eigene Maßnahmen zu prüfen, die riesige Herausforderung der Aufgabe zu erkennen und schließlich die Freigabe der Vorgesetzten zu bekommen, sich an das BSI als externen Dritten zu wenden.

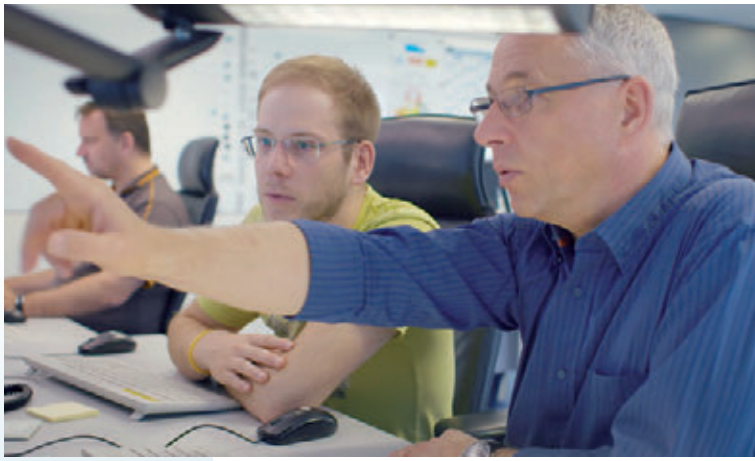
In diesem Fall meldet der IT-Sicherheitsbeauftragte eines großen Mittelständlers einen Angriff auf die zentrale IT des Unternehmens, den die hauseigenen Fachleute nicht in den Griff bekommen. Es geht – wie in den meisten dieser Fälle – um einen schweren Angriff gegen die Kronjuwelen der Firma: Produktionsgeheimnisse, Projektplanungen, Kommunikation von Schlüsselpersonen. Also Angriffe gegen die Vertraulichkeit, hervorgerufen durch sogenannte APTs (Advanced Persistent Threats).

Aber das wissen die Verantwortlichen des Unternehmens im Moment noch nicht, ebenso wenig wie die hinzugezogenen Mitarbeiter des Lagezentrums. Im ersten Telefonat wird deutlich: Auffälligkeiten in der hausinternen IT gibt es wohl schon etwas länger: Eine große unbekannte PST-Datei verstopfte den Mailausgang. Und dann fiel auf, dass der Admin-Kollege, der gerade die Änderung im Netz durchgeführt hat, doch eigentlich seit einer Woche im Urlaub ist. Da beschlossen die Verantwortlichen, sich externen Rat zu holen.





Nationales IT-Lagezentrum des BSI



Der Mitarbeiter von CERT-Bund ruft am frühen Vormittag beim Betroffenen an. Er versucht sich zum IT-Sicherheitsbeauftragten oder einer anderen IT-affinen Managementrolle durchzufragen, die das Problem verstehen und handeln kann. Das persönliche Gespräch am Telefon ist wichtig, um sicherzugehen, dass die Meldung an der richtigen Stelle ankommt, ernst genommen und nachverfolgt wird.

Dem Anruf voraus ging eine Meldung über das SIGINT Support-for-Cyber-Defense-Programm des Bundesnachrichtendienstes: Es wird vermutet, dass ein deutsches Unternehmen Opfer eines APT-Angriffs geworden ist. Wie beim BND werden auch von anderen Nachrichtendiensten Server und Systeme von Angreifern beobachtet und deren Angriffe analysiert. Fällt ein Unternehmen oder eine Behörde aus einem Partnerland durch Kommunikation mit einem solchen System auf, wird dieses Land – hier über BND und dann das BSI – auf geeignetem Wege unterrichtet. In anderen Fällen erfolgt die Meldung aus der internationalen CERT- (Computer Emergency Response Team) und Sicherheitscommunity an CERT-Bund und seine Kontakte. Im ersten Telefonat klärt das BSI mit dem Betroffenen zunächst die Plausibilität und Hintergründe der Meldung und versucht, erste ergänzende Informationen zum Vorfall zu bekommen.

VORFALLSMELDUNGEN

Vorfallsmeldungen kommen auf verschiedenen Wegen ins BSI-Lagezentrum. Primärer Vektor sind die verschiedenen Meldeverfahren für die Bundesverwaltung nach §4 BSI-Gesetz, die meldepflichtigen Kritischen Infrastrukturen nach §8b und die öffentliche Meldestelle der Allianz für Cyber-Sicherheit. Neben derartigen schriftlichen formatierten und unformatierten Meldungen kommen oftmals auch Anrufe an.

EINSATZENTSCHEIDUNG

Nach dem Abgleich der vorliegenden Informationen und dem Austausch der Kontakte wird zwischen den Mitarbeitern des Lagezentrums beziehungsweise CERT-Bund und den Verantwortlichen in der betroffenen Institution ein weiterer zeitnaher Telefonkonferenztermin vereinbart. An diesem nehmen Experten aus verschiedenen Fachbereichen des BSI teil. Im Gespräch werden weitere Details und Hintergründe, Symptome und mögliche Auswirkungen diskutiert. Nach einer Einzelfallprüfung entscheidet dann das BSI, dass die Problemlösung nicht allein durch weitere Beratungen und Hilfen (wie Good Practice-Dokumente, Verweis auf Beratungsunternehmen etc.) oder durch forensische Unterstützung vorangetrieben werden kann, sondern dass ein Termin vor Ort nötig ist, ein sogenannter MIRT-Einsatz (Mobile Incident Response Team). Abhängig von der Dringlichkeit des Einsatzes, den Rahmenbedingungen und der Personalverfügbarkeit wird schnellstmöglich ein Team vor Ort entsendet.

EINSATZ VOR ORT

Die Experten des BSI treffen in diesem Fall auf gute Bedingungen: Das betroffene Unternehmen hat bereits die Rahmenbedingungen für die Unterstützung durch das BSI geschaffen. Hierzu zählen die Verfügbarkeit der richtigen Ansprechpartner, der notwendigen Daten wie Netzübersichten, Logdaten etc. Nach einer Auftaktbesprechung vor Ort, in der nochmal ganz konkret das Problem und die technische Situation besprochen werden, wird dann ein gemeinsamer Einsatzplan für die nächsten Schritte abgesprochen.

Die Experten des MIRT versuchen das Problem zunächst einzugrenzen und die Schadensursache zu isolieren. Auf die Clients werden Tools ausgerollt, die dort nach Angreifer-Signaturen (sogennante Indicators of Compromise, IoCs) suchen. Das BSI bringt hierzu eigene vertrauliche Daten aus dem Schutz der Regierungsnetze mit, mit denen die Signaturen abgeglichen werden. Man sucht nach weiteren Schäden und Auswirkungen des Angriffs und dämmt diese so weit wie möglich ein. Wie weit und tief hat sich der Angreifer im Netz vorgearbeitet? Sind schon zentrale Komponenten gefallen? Hat der Angriff womöglich gar das „goldene Ticket“ des „Master Admins“ und damit die volle Kontrolle über das gesamte Netz? Ist er noch aktiv? Kann man beobachten, was er tut und „wo er steckt“, ohne zu wichtige Daten zu verlieren? Wie verbindet er sich ins Netz? Wie exfiltriert er seine „Beute“? Wo könnte er Hintertüren und Schlupflöcher, zum Beispiel über VPNs, eingerichtet haben? Denn nur wenn man weiß, wie und von wo der Angreifer agiert, kann man ihn sicher aussperren.

Daraus ergeben sich die Möglichkeiten, nach Abschluss der Analysephase einen weitgehend sicheren Übergangsbetrieb hinzubekommen, um eine Basis-Arbeitsfähigkeit in der Institution zu gewährleisten. Parallel erfolgt in Zusammenarbeit mit einem externen Dienstleister die Planung, wie das Netz schnellstmöglich so sicher gestaltet werden kann, dass weitere Angriffe kurzfristig nicht möglich sind. Die Experten des MIRT besprechen sich unterdessen laufend mit den Fachleuten vor Ort wie auch mit weiteren Kollegen im BSI.

Technische und forensische Analysen brauchen Zeit. So wechseln sich in den folgenden Tagen oftmals Analysephasen im BSI und Phasen der Arbeit vor Ort ab. Fortlaufend müssen neue Erkenntnisse in die Untersuchung eingebracht und die Suchläufe neu gestartet werden.

ZUSAMMENARBEIT DES BSI MIT DEN SICHERHEITSBEHÖRDEN UND ANDEREN CERTS

Das BSI steht nicht allein bei der Unterstützung der Betroffenen. Es berichtet pseudonym – also OHNE Nennung des Namens des Betroffenen – und auf hohem Abstraktionsniveau den Sicherheitsbehörden im Cyber-Abwehrzentrum. So sind die anderen Behörden über die Grundzüge des Vorfalls unterrichtet und können vorhandene eigene Informationen einbringen.

Eine Kontaktaufnahme mit dem Betroffenen durch Partnerbehörden des BSI erfolgt ausschließlich nach Absprache. Oftmals lohnt sich dieser Weg der Zusammenarbeit durchaus für die betroffenen Institutionen. Durch Anzeigeerstattung beim Bundeskriminalamt oder den Zentralen Ansprechstellen Cyber-Crime (ZAC) der Landeskriminal-

Links: Mobile Incident Response Teams (MIRT) auf dem Weg zum Einsatzort

Unten: MIRT-Einsatz vor Ort bei der Schadensbegrenzung

ämter können zum Beispiel Ermittlungen eingeleitet werden, um einerseits bessere Erkenntnisse zum Schutz der Netze und Daten zu bekommen und andererseits die Ermittlung der Täter und langfristig deren Verhaftung und Verurteilung zu ermöglichen. Auch die Einbindung des Bundesamtes für Verfassungsschutz kann helfen, weitere Hinweise zum Schutz zu bekommen und die Täter zu ermitteln.

Technische Parameter und IoCs zum Angriff und Täter teilt das BSI auch mit nationalen und internationalen CERT-Partnern – natürlich ebenfalls anonym und unter Weitergabe möglichst weniger Rahmeninformationen zum Betroffenen. Die Hilfen, die das BSI zur Detektion und Analyse des eigenen Vorfalls mitgebracht – und zum Teil auch von den anderen CERT-Partnern erhalten – hat, werden mit Daten vom laufenden Vorfall angereichert beziehungsweise ergänzt und können anderen helfen, so wie sie dem Betroffenen gerade selbst geholfen haben. Es besteht auch die Möglichkeit, dass sich das BSI in Absprache mit dem Betroffenen durch Beratungsunternehmen oder andere externe Fachleute unterstützen lässt, falls die Notwendigkeit dazu besteht.

D-DAY / BEREINIGUNG

Zu einem Zeitpunkt X, „D-Day“ genannt, nach mehreren Wochen bei vollständig kompromittierten Netzen, werden diese zur Bereinigung komplett heruntergefahren und neu gehärtet aufgesetzt, alle Passwörter werden zurückgesetzt und das System geht danach wieder „sauber“ in Betrieb. Es folgt eine intensive Beobachtung, ob es dem Angreifer gelungen war, die Zeit der Bereinigung durch Hintertüren zu „überwintern“ und ob er sich wieder im Netz auszubreiten versucht.

ABSCHLUSSMASSNAHMEN

Unmittelbar nach dem D-Day unterstützt das BSI den Betroffenen dabei, ein internes Projekt aufzulegen, das das Netz und seine Prozesse langfristig resilient gegen Angriffe macht. So sollen in Zukunft erfolgreiche Infektionen einzelner Clients nicht dazu führen, dass das ganze Netz „fällt“. In der Kürze der Zeit der provisorischen zusätzlichen Abwehrmaßnahmen und des Neuaufsetzens war es oft nicht möglich, alle eigentlich erforderlichen Änderungen (zum Beispiel Zwei-Faktor-Authentifizierung für Admins, Segmentierung, APT-Angriffserkennung und Ähnliches) umzusetzen.

In einer Nachbesprechung aller Beteiligten und den folgenden Nacharbeiten im BSI werden die Lektionen und Erfahrungen gesammelt und aufbereitet, um so für den nächsten Einsatz vorbereitet und für andere Betroffene hilfreich zu sein. Hierzu werden zum Beispiel die internen Checklisten überarbeitet oder neue Tools beschafft. Wenn möglich, werden Lektionen weiter ohne Nennung des Namens des Betroffenen mit anderen Sicherheitsteams geteilt. Denn wenn das nächste Mal am späten Nachmittag das Telefon klingelt, müssen die Mitarbeiter des Lagezentrums so gut wie möglich vorbereitet sein. ■

JULI 2015

IT-SICHERHEITSGESETZ TRITT IN KRAFT

MAI 2016

ERSTER TEIL BSI-KRITISVERORDNUNG TRITT IN KRAFT

GESETZLICHE BASIS AKTUALISIERT

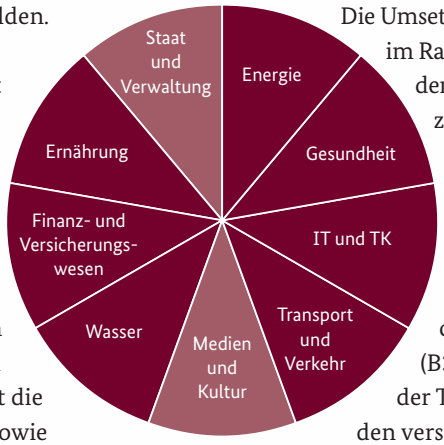
von Nora Apel, Referatsleiterin Kritische Infrastrukturen – Grundsatz

Umsetzung der NIS-Richtlinie schafft weiteren Meilenstein

Ende Juni 2017 trat das NIS-Richtlinien-Umsetzungsgesetz in Kraft. Damit wird die im Juli 2016 verabschiedete europäische Richtlinie über „Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen“ in Deutschland realisiert. Außerdem trat im Juni 2017 der zweite Teil der BSI-Kritisverordnung in Kraft. Damit wird ein Gesetzgebungsprozess abgeschlossen, der mit dem IT-Sicherheitsgesetz im Jahr 2015 begonnen hatte.

ALLE KRITIS-SEKTOREN GEREGELT

Am 25. Juli 2015 trat das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, IT-SiG) in Kraft. Es änderte unter anderem das BSI-Gesetz dahingehend, dass zukünftig bestimmte Betreiber Kritischer Infratrukturen verpflichtet sind, ein Mindestniveau an IT-Sicherheit umzusetzen und gegenüber dem BSI nachzuweisen sowie erhebliche IT-Störungen, die Auswirkungen auf die Kritischen Infrastrukturen haben oder haben könnten, an das BSI zu melden.



Wer genau unter das Gesetz fällt, regelt die gemäß § 10 BSIG erlassene Rechtsverordnung (BSI-Kritisverordnung, BSI-KritisV). Dort wird anhand quantitativer und qualitativer Kriterien näher bestimmt, wer von den Neuregelungen betroffen ist. Die Rechtsverordnung wurde in zwei Teilen, sogenannten Körben, erlassen. Der erste Korb ist am 3. Mai 2016 in Kraft getreten und regelt die Sektoren Energie, Wasser, Ernährung sowie Informationstechnik und Telekommunikation. Der zweite Korb trat in Form einer Änderungsverordnung der bestehenden BSI-KritisV am 30. Juni 2017 in Kraft. Er regelt die noch verbleibenden KRITIS-Sektoren Gesundheit, Transport und Verkehr sowie Finanz- und Versicherungswesen und nimmt einige Konkretisierungen oder Änderungen an den bereits bestehenden Regelungen vor. Der Sektor Medien, der ebenfalls zu den Kritischen Infrastrukturen zählt, ist von dem Gesetz nicht betroffen, da der Bund hier keine Gesetzgebungskompetenz hat (siehe Abbildung der Sektoren).

KOOPERATIVE UMSETZUNG

Die Umsetzung des Gesetzes erfolgt kooperativ im Rahmen der Plattform UP KRITIS, in der KRITIS-Betreiber, Verbände und die zuständigen Behörden bereits seit zehn Jahren freiwillig am Schutz der Kritischen Infrastrukturen zusammenarbeiten. In verschiedenen Gremien des UP KRITIS werden die Meldeschwellen spezifiziert und sogenannte „Branchenspezifische Sicherheitsstandards“ (B3S) erarbeitet, mit denen der „Stand der Technik“ in Sachen IT-Sicherheit in den verschiedenen Branchen konkretisiert wird. Die B3S sind für die betroffenen Betreiber eine Chance, ausgehend von der eigenen Expertise selbst Vorgaben zum „Stand der Technik“ zu formulieren. Das BSI prüft auf Antrag – in Abstimmung mit dem Bundesamt

JUNI 2016

EUROPÄISCHE RICHTLINIE ÜBER „MASSNAHMEN ZUR GEWÄHRLEISTUNG EINES HOHEN GEMEINSAMEN SICHERHEITSNIVEAUS VON NETZ- UND INFORMATIONSSYSTEMEN“ WIRD VERABSCHIEDET

JUNI 2017

NIS-RICHTLINIEN-UMSETZUNGSGESETZ TRITT IN KRAFT

JUNI 2017

ZWEITER TEIL BSI-KRITISVERORDNUNG TRITT IN KRAFT

für Bevölkerungsschutz und Katastrophenhilfe (BBK) und den zuständigen Aufsichtsbehörden – die Eignung dieser B3S. Betreiber, die sich nach einem solchen als geeignet anerkannten B3S prüfen lassen, erlangen Rechtssicherheit im Hinblick auf den bei einem Audit verlangten und überprüften „Stand der Technik“. Eine gesetzliche Pflicht zur Erarbeitung oder Anwendung eines B3S besteht jedoch nicht.

Die Chance, einen B3S zu erarbeiten und damit mitbestimmen zu können, was in einzelnen KRITIS-Branchen als „Stand der Technik“ in Bezug auf IT-Sicherheit angesehen wird, wird von den Branchen im UP KRITIS rege genutzt. Der B3S „Wasser/Abwasser“ für die Branchen „Öffentliche Wasserversorgung“ und „Öffentliche Abwasserbeseitigung“ wurde als erster vom BSI als geeignet eingestuft. Weitere B3S werden gerade erarbeitet und sollen noch 2017 fertiggestellt werden.

Das IT-Sicherheitsgesetz sieht jedoch nicht nur Pflichten für KRITIS-Betreiber, sondern auch Rechte vor. Das BSI ist verpflichtet, die KRITIS-Betreiber mit Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen und der dabei beobachteten Vorgehensweise sowie einem kontinuierlichen Lagebild zu versorgen.

NIS-RICHTLINIEN-UMSETZUNGSGESETZ VERABSCHIEDET

Durch das „Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 06. Juli 2016 über Maßnahmen zur Gewährleistung eine hohen gemeinsamen Sicherheitsniveaus von Netz und Informationssystemen in der Union“ (NIS-RL-Umsetzungsgesetz) werden die Aufgaben und Kompetenzen des BSI erneut erweitert. So kann das BSI in Zukunft beispielsweise bei den Betreibern vor Ort die Einhaltung der Anforderungen nach § 8a Absatz 1 BSIG überprüfen.

Auch der Kreis der vom Gesetz betroffenen Betreiber erweitert sich durch das NIS-RL-Umsetzungsgesetz. Ab sofort gelten die Meldepflicht und die Umsetzung des Stands der Technik in der IT-Sicherheit (§ 8c BSIG) auch für die Anbieter digitaler Dienste wie Suchmaschinen, Cloud-Dienste und Online-Marktplätze. Daneben wurden in das Telekommunikationsgesetz (TKG) Regelungen aufgenommen, die es Betreibern von Telekommunikationsnetzen ermöglichen, auf Angriffe zu reagieren.

Gleichzeitig bekommen auch durch dieses Gesetz die KRITIS-Betreiber wieder neue Unterstützung. So kann das BSI die Betreiber zum Beispiel bei herausgehobenen IT-Sicherheitsvorfällen vor Ort unterstützen, um die Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems wiederherzustellen.

Sowohl das IT-Sicherheitsgesetz von 2015 als auch das NIS-RL-Umsetzungsgesetz vom April 2017 stellen die Zusammenarbeit zwischen dem BSI und den Betreibern Kritischer Infrastrukturen auf eine neue Grundlage. Mit den Gesetzen wird der seit vielen Jahren verfolgte kooperative Ansatz beim Schutz Kritischer Infrastrukturen weitergeführt und eine Win-win-Situation für Betreiber und Staat erreicht. ■

Weitere Informationen: https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS-Richtlinie.html

IT-GRUNDSCHUTZ RUNDERNEUERT

von Katrin Alberts, Referat IT-Grundschutz

Informationssicherheit für Wirtschaft und Verwaltung

Tausende Stunden fachlicher Bearbeitung der einzelnen Veröffentlichungen, Dutzende von Workshops mit IT-Grundschutz-Anwendern aus Verwaltung und Unternehmen sowie zahlreiche BSI-interne Diskussionen und Abstimmungen: Die Modernisierung des IT-Grundschutzes ist ein umfangreiches Großprojekt. Zur it-sa 2017 findet sie mit der Vorstellung der neuen BSI-Standards sowie des neuen IT-Grundschutz-Kompendiums einen ersten Abschluss. Die Inhalte stehen nun in kompakter und übersichtlicher Form für die unterschiedlichen Zielgruppen zur Verfügung. Anwender können auf dieser Basis selbst ein Managementsystem zur Informationssicherheit in ihrer Institution aufbauen.

DER IT-GRUNDSCHUTZ – DAS ORIGINAL IN DER INFORMATIONSSICHERHEIT

Neue BSI-Standards und Bausteine, ein neues IT-Grundschutz-Kompendium: Nach einer intensiven Phase der fachlichen Überarbeitung steht die bewährte IT-Grundschutz-Methode nun aktualisiert und modernisiert den IT-Grundschutz-Anwendern und neuen Interessenten zur Verfügung. Ob der Informationssicherheitsbeauftragte einer Behörde, der Chief Information Security Officer (CISO) eines großen Unternehmens oder der Geschäftsführer eines klein- oder mittelständischen Unternehmens (KMU): Sie alle können im neuen Angebot des IT-Grundschutzes passend zu den Anforderungen ihrer Institution geeignete Sicherheitsinformationen in den unterschiedlichen Publikationen finden: Wie ist der aktuelle Status der Informationssicherheit in der Institution? In welchen Bereichen gibt es Handlungsbedarf? Mit welchen Maßnahmen lässt sich das Sicherheitsniveau zeitnah erhöhen, welche Maßnahmen erfordern einen längeren Planungsvorlauf und mehr Ressourcen?

Der IT-Grundschutz bietet eine modulare und flexible Methode für Einsteiger und Fortgeschrittene, die sich mit Informationssicherheit befassen. Die Anwender können entsprechend ihrer Vorkenntnis unterschiedliche Angebote auswählen, mit denen sie in ihrer Institution arbeiten können. Im neuen IT-Grundschutz-Kompendium ist dafür ein großer Teil der erforderlichen neuen Bausteine veröffentlicht, die zur Erhöhung der Informationssicherheit einer Institution herangezogen werden können. Damit ist eines der wichtigsten Ziele im Rahmen des gesamten Modernisierungsprozesses erreicht. Für IT-Grundschutz-Anwender gibt es moderate Fristen, um vom „alten" IT-Grundschutz auf die modernisierten Inhalte zu migrieren. Dies gilt auch für alle Fragen rund um das Thema Zertifizierung.

NEUE INHALTE – VIELE ZIELGRUPPEN

Neben dem IT-Grundschutz-Kompendium wurden auch neue BSI-Standards zu einzelnen Schwerpunkten veröffentlicht. Der BSI-Standard 200-1 definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS). Mit dem BSI-Standard 200-2 zur IT-Grundschutz-Methodik kann die Basis gelegt werden, um ein solides ISMS aufzubauen. Der BSI-Standard 200-3 zum Risikomanagement enthält alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes. Neu im Angebotsportfolio ist ein „Leitfaden zur Basis-Absicherung". Die neue Veröffentlichung basiert auf dem BSI-Standard 200-2 und beschreibt, wie kleinere Unternehmen und Behörden zielgerichtet in die Basis-Absicherung einsteigen können.

Die Modernisierung der IT-Grundschutz-Inhalte hat in engem Austausch mit der IT-Grundschutz-Community stattgefunden. Die aktuellen Inhalte konnten durch die Anwender aus der Praxis überprüft und durch ihre Rückmeldungen noch praxistauglicher aufbereitet werden. Dieser Austausch hat sich als sehr wertvoll erwiesen, sowohl für die einzelnen Veröffentlichungen als auch zur Stärkung des Community-Gedankens im IT-Grundschutz selbst.

INFORMATIONSSICHERHEIT IST EIN PROZESS

Wenn der IT-Grundschutz auch durch die Modernisierung grundlegend überarbeitet und die Inhalte gemäß dem Stand der Technik aktualisiert wurden: Die Prozesshaftigkeit und das Entwicklungstempo in der Informationssicherheit bedingen, dass auch der IT-Grundschutz kontinuierlich weiter aktualisiert werden muss. Bestehende Veröffentlichungen müssen überprüft, zu neuen Entwicklungen zum Beispiel neue Bausteine verfasst werden. Zukünftig ist geplant, den bestehenden BSI-Standard 100-4 zum Notfallmanagement ebenfalls zu überarbeiten, auch ein ganz neuer Standard zum Thema Messbarkeit befindet sich in der Diskussion. Der IT-Grundschutz wird auch künftig dynamischen Herausforderungen gegenüberstehen, die das BSI gemeinsam mit den IT-Grundschutz-Anwendern engagiert annehmen wird. ■

LEITFADEN ZUR BASIS-ABSICHERUNG

Die drei Phasen des Sicherheitsprozesses

Weitere Informationen zu den neuen IT-Grundschutz-Angeboten finden Sie hier: https://www.bsi.bund.de/grundschutz

Neue Mindeststandards

von Dominique Hader und Philipp Deuster, Referat Mindeststandards Bund

Cyber-Sicherheit weiter stärken

Das BSI als die nationale Cyber-Sicherheitsbehörde erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes. Grundlage dafür ist der § 8 Abs. 1 BSI-Gesetz. Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Aktuelle Entwicklungen in der Informationstechnologie erfordern dabei, die Standards immer wieder zu aktualisieren oder neue zu entwickeln.

Im Jahr 2014 veröffentlichte das BSI den Mindeststandard für den Einsatz des SSL/TLS-Protokolls als erstes Dokument seiner Art. Seitdem hat sich viel getan. Unter anderem wurde die Aufgabe, Mindeststandards zu erstellen, durch das IT-Sicherheitsgesetz von 2015 weiter gestärkt. Das zentrale Ziel dieser gesetzlich verankerten Vorgaben besteht darin, ein konkretes Mindestniveau an Informationssicherheit für die Stellen des Bundes zu definieren. Natürlich können auch weitere Anwender aus Staat, Wirtschaft und Gesellschaft die Vorgaben als Maßstab für die Sicherheit ihrer eigenen Systeme heranziehen. Zum heutigen Zeitpunkt existieren Mindeststandards zu den folgenden sechs Themen:

- Einsatz des SSL/TLS-Protokolls
- Schnittstellenkontrollen
- Sichere Webbrowser
- Nutzung externer Cloud-Dienste
- Mobile Device Management
- Anwendung des HV-Benchmarks kompakt 3.0

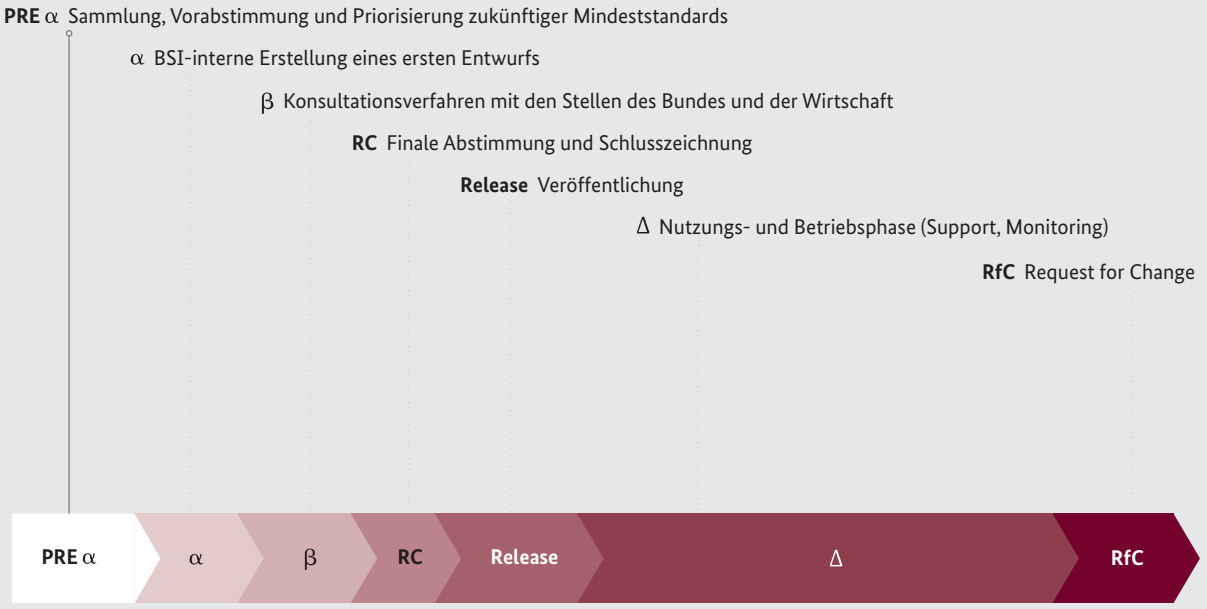
STANDARDISIERTE VORGEHENSWEISE

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten Rahmenbedingungen und Anforderungen gekennzeichnet. Dadurch entstehen nicht nur Herausforderungen bei den Anwendern, ihre IT zu sichern. Auch das BSI muss sich der Aufgabe stellen, für diese umfangreiche Thematik angemessene Vorgaben zu erarbeiten. Der Entwicklungspfad der bisher erarbeiteten Mindeststandards zeigt bereits die fachliche Vielfalt der Themenbereiche auf. Jedem Mindeststandard sind daher unterschiedliche Fachreferate und Expertenkreise im BSI zugeordnet. Aus diesem Grund erfordert der Erstellungsprozess ein hohes Maß an Kooperation zwischen allen beteiligten Experten, einschließlich der Anwenderseite in der Bundesverwaltung.

Um die Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards sicherzustellen, wird dieser Prozess in einer standardisierten Vorgehensweise genau beschrieben (siehe Abbildung S. 24). Im Rahmen der Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfungszyklen.

- Die Ideensammlung (PRE-α): Nicht nur das BSI entwickelt Themenvorschläge, sondern auch die Anwender können ihre Wünsche und Ideen einbringen. Dies bietet die Möglichkeit, die Zielgruppe bereits von Anfang an mit ihrer fachlichen Kompetenz einzubinden.
- Die BSI-interne Abstimmung (α): Wurde aus der Ideensammlung ein Thema für einen neuen Mindeststandard ausgewählt, wird der erste Entwurf zunächst im BSI abgestimmt. Dabei bringt sich nicht nur das entsprechende Fachreferat ein, sondern alle Abteilungen haben die Möglichkeit, an diesem Entwurf mitzuwirken.
- Das Konsultationsverfahren (β): Angelehnt an die Beta-Phase in der Softwareentwicklung, werden die Anwender eingeladen, die β-Version des Mindeststandards zu „testen“. Dazu wird ihnen der Entwurf zur Kommentierung übermittelt und sie können ihre eigenen Erfahrungen erneut mit einbringen.
- Die finale Abstimmung (Release Candidate): Nachdem auch die externen Kommentierungen zur Qualitätssicherung einbezogen wurden, wird der Mindeststandard zur Veröffentlichung (Release) freigegeben.
- Nutzungs- und Betriebsphase (Δ): In dieser Phase werden die Anwender unterstützt (Support) und die Effektivität und Effizienz des Mindeststandards wird beobachtet (Monitoring).
- Eventuelle Änderungen (Request for Change) werden aufgenommen und gegebenfalls eingearbeitet.

LEBENSZYKLUS DER MINDESTSTANDARDS



Ein solch umfangreicher, qualitätsorientierter Prozess benötigt natürlich seine Zeit. Je nach Umfang des Themas, Verfügbarkeit von Experten und diversen anderen Faktoren vergeht vom Beginn der Entwicklung bis zur Fertigstellung eines neuen Mindeststandards in etwa ein halbes Jahr. So wichtig die Mindeststandards auch sind: Sie sind immer nur eine Absicherung nach unten. In der Praxis ergeben sich regelmäßig höhere Anforderungen an die Informationssicherheit, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards müssen die Anwender diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

TEIL DER CYBER-SICHERHEITSSTRATEGIE

Mindeststandards sind ein wesentlicher Bestandteil der Cyber-Sicherheitsstrategie für Deutschland. In den strategischen Handlungsfeldern „Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung", „Gemeinsamer Auftrag von Staat und Wirtschaft" sowie „Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur" ermöglichen sie durch klar definierte Vorgaben, ein Mindestsicherheitsniveau für die Informationstechnik des Bundes zu erreichen. Außerdem stellen sie in zweierlei Hinsicht ein verbindendes Element dar: Zum einen werden sie nicht als isolierte Veröffentlichungen erarbeitet, sondern es wird Wert darauf gelegt, sie zu anderen Veröffentlichungen des BSI in Bezug zu setzen (zum Beispiel zum Anforderungskatalog C5). Zum anderen wird durch die Beteiligung der verschiedenen Stellen im Erstellungsprozess ein zielgerichteter Abgleich gefördert.

Aktuell erarbeitet das BSI Mindeststandards zur Mitnutzung von Cloud-Dienstleistungen, zur Protokollierung und Detektion von Cyber-Angriffen, zu Nutzerpflichten im Rahmen der Sicherung der ressortübergreifenden Kommunikationsinfrastruktur, sowie zur Anwendung des modernisierten IT-Grundschutzes. ■

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

VERTRAUENSVOLLE ZUSAMMENARBEIT

von Joachim Gutmann, Glücksburg Consulting AG

Erste IT-Sicherheitsplattform für industrielle KMU

Klein- und Mittelunternehmen (KMU) fehlen zumeist die Ressourcen, um Cyber-Angriffen mit spezialisierten Teams zu begegnen (Computer Emergency Response Teams – CERT). Sie müssen sich verstärkt für betriebsübergreifende Kooperationen öffnen. Da ist Vertrauen unbedingte Voraussetzung. Der Verband der Elektrotechnik Elektronik Informationstechnik e.V. (VDE) hat jetzt eine Lösung gefunden: eine CERT-Plattform.

Die digitale Transformation in Richtung Industrie 4.0 eröffnet große Chancen und Wertschöpfungspotenziale – gerade für den Wachstumsmotor Mittelstand. Zugleich steigt aber mit der fortschreitenden Vernetzung der Produktionsanlagen mit modernen Informations- und Kommunikationssystemen (IKT) das Risiko von Cyber-Angriffen. Die Bedrohungen reichen von System- und Produktionsausfällen über Fehlfunktionen mit Unfallfolgen bis hin zu Industriespionage und Sabotage. Entsprechend schwerwiegend sind die möglichen Folgen.

Kurzprofil Joachim Gutmann

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

Umso wichtiger ist es, IT-Sicherheit als kritischen Erfolgsfaktor für Industrie 4.0 und Digitalisierung zu stärken: erstens durch eine verbesserte Prävention bei der Systementwicklung, zweitens durch eine möglichst schnelle Detektion neuer Sicherheitslücken, drittens durch eine systematische und koordinierte Reaktion auf die Angriffe. Hier setzt CERT@VDE an: die erste Plattform zur Koordination von IT-Security-Problemen speziell für KMU im Bereich Industrieautomation. „Unsere Plattform bietet Herstellern, Integratoren, Anlagenbauern und Betreibern aus dem Bereich Industrieautomation die Möglichkeit, intensiv und vertrauensvoll Informationen auszutauschen“, wirbt Andreas Harner, Leiter des CERT@VDE. Auf der Hannover Messe Industrie wurde die in den VDE-Gremien angeschobene und von Industriemitgliedern des Verbandes entwickelte Plattform erstmals präsentiert.

SENSIBILISIERUNG IST DER ERSTE SCHRITT

Wie wichtig dieses Thema auch für die KMU ist, zeigen die Ergebnisse des VDE Tec Reports 2017, einer Umfrage unter den 1.300 VDE-Mitgliedsunternehmen und Hochschulen. Demnach sind 88 Prozent der Befragten davon überzeugt, dass IT-Sicherheit eine wesentliche Säule der erfolgreichen Digitalisierung darstellt. Und nahezu alle (93 Prozent) vertreten die Ansicht, dass Kritische Infrastrukturen – zum Beispiel im Energiesektor – besonders zu schützen sind. Mehr als die Hälfte der Befragten (53 Prozent) war bereits von Cyber-Attacken betroffen; dabei wurden große Unternehmen (71 Prozent) und bedeutende Hochschulen (68 Prozent) deutlich überdurchschnittlich übers Netz angegriffen. Besonders gefährdet sind dabei die Bereiche Forschung und Entwicklung (78 Prozent), IT/Software (70 Prozent), Produktion (57 Prozent) sowie Planung/Projektierung/Engineering (40 Prozent).

IT-SICHERHEIT AUF DER TECHNOLOGIEPOLITISCHEN AGENDA

Die Sensibilisierung ist also durchaus vorhanden, aber an der Umsetzung der Erkenntnisse hapert es noch bei vielen KMU der Industrieautomation. Während große nationale und internationale Unternehmen und Institutionen meist über ein eigenes CERT verfügen, um den Umgang mit Schwachstellen in den eigenen Systemen zu koordinieren und IT-Sicherheitsinformationen strukturiert bereitzustellen, fehlen KMU dazu in der Regel die Ressourcen. Viele KMU haben noch nicht einmal eine ausgebaute IT-Abteilung, geschweige denn die Kapazität für spezialisierte Notfallteams. Und selbst dort, wo diese bereits eingerichtet wurden, fehlt es noch an Strukturen zur vertrauensvollen Zusammenarbeit mit anderen Herstellern.

„Um dieses notwendige Vertrauen zu fördern“, erläutert VDE-Sicherheitsexperte Harner, „haben wir für die Plattform feste Leitlinien verabredet, die für alle Teilnehmer gelten.“ Basis der Zusammenarbeit auf der IT-Sicherheitsplattform ist eine Vertraulichkeitsvereinbarung. Die Leitlinien konkretisieren diese Vereinbarung und bestimmen die Kooperation mit dem CERT@VDE:

- Die Vertraulichkeit der Kundendaten hat höchste Priorität.
- Die Kooperation ist freiwillig und kann jederzeit beendet werden.
- Businessmodelle Einzelner dürfen unter den Aktivitäten des CERT@VDE nicht leiden.
- Durch wechselseitige Beiträge und Informationen sollen die Arbeitsabläufe aller Mitglieder optimiert werden.
- Informationen und Interessen anderer Mitglieder werden geschützt.

Bei regelmäßigen Arbeitstreffen der Plattformteilnehmer werden diese Leitlinien mit Leben gefüllt und um persönliches Vertrauen bereichert.

AUFBAU EINER WISSENSPLATTFORM

Anders als die bereits bestehenden CERTs in Deutschland (beispielsweise der CERT-Bund des BSI, das als zentrale Anlaufstelle für sämtliche Probleme in Computersystemen fungiert) ist die VDE-Sicherheitsinitiative auf den Bereich der Industrieautomation spezialisiert. „Aber natürlich

DIE SICHERHEITSPLATTFORM ERMÖGLICHT EINEN HERSTELLERÜBERGREIFENDEN AUSTAUSCH AUF EINER NEUTRALEN, VERTRAUENSWÜRDIGEN UND SICHEREN PLATTFORM.

suchen wir die Zusammenarbeit mit anderen CERT und dem CERT-Bund", sagt Harner. „Voneinander lernen ist nicht nur für die Teilnehmer des CERT@VDE, sondern ganz generell die oberste Maxime."

Die Sicherheitsplattform ermöglicht einen herstellerübergreifenden Austausch auf einer neutralen, vertrauenswürdigen und sicheren Plattform – natürlich unter Wahrung der Anonymität. Ehemals isolierte Informationen werden im CERT@VDE zentral gebündelt, strukturiert und verteilt, sodass verschiedenste Industrieteilnehmer stets über den gleichen und aktuellen Wissensstand im Hinblick auf Sicherheitsstandards und -gefahren verfügen. Der Zugang zur Plattform, die auch als Wissensdatenbank genutzt werden kann, erfolgt über einen kundenspezifischen Zugang. Eine Cockpit-Benutzeroberfläche erlaubt in Zukunft die Zusammenstellung und Anordnung der für den Benutzer relevanten Sicherheitsthemen. Von einem Angriff betroffene Unternehmen können zudem von IT-Sachverständigen kurzfristig eine Lageeinschätzung einholen und Hilfestellung in Anspruch nehmen.

„Wir schaffen damit effiziente und effektive Kooperationsstrukturen für IT-Sicherheits- und Produktionsverantwortliche und ermöglichen, gemeinsam an der Bewältigung des hohen Sicherheitsrisikos zu arbeiten, welches mit Industrie 4.0 zur zentralen Herausforderung geworden ist", ist sich Andreas Harner sicher.

CYBER-SECURITY FÜR EINE ERFOLGREICHE DIGITALISIERUNG

Die Plattform ist aber nicht nur die zentrale Know-how-Stelle zum Umgang mit Schwachstellen und ermöglicht deren zeitgerechte Bearbeitung. Für die Teilnehmer werden auch zielgruppenorientierte Schwachstelleninformationen aus diversen Quellen aufbereitet und verfügbar gemacht. Zudem wird über die Plattform die Unterstützung beim Schließen von Sicherheitslücken koordiniert.

Ohnehin sind Koordination und Kommunikation die beiden Leitbegriffe, unter die sich das Selbstverständnis der Plattformbetreiber fassen lässt. So wird über die Plattform ein firmenübergreifender Austausch zu Sicherheitsproblemen in geschützten Interaktionsräumen organisiert und der Austausch über geeignete Vorgehensweisen angeregt. Für die Teilnehmer aus der Automatisierungsindustrie werden Workshops angeboten und gemeinsam mit Partnern Best Practices erarbeitet.

„Wenn die KMU im Wettbewerb mit den Großen der Branche sicherheitstechnisch mithalten wollen", weiß Harner, „müssen sie in einer geschützten Atmosphäre die aus Konkurrenzfurcht errichteten Mauern niederreißen und firmenübergreifend voneinander lernen." Nur aus dem gemeinsamen Lernen erwachsen schnellere Einschätzungen bei Vorfällen und kann eine effektive Schadensbegrenzung angegangen werden. ■

Der VDE-Verband der Elektrotechnik Elektronik und Informationstechnik ist mit 36.000 Mitgliedern (davon 1.300 Unternehmen) einer der großen technisch-wissenschaftlichen Verbände Europas. Neben der CERT-Plattform betreibt der VDE die VDE/DKE-Kontaktstelle Informationssicherheit (KSI) und führt die Begleitforschung für BMBF-Projekte „Vernetzte IT-Sicherheit Kritischer Infrastrukturen (VeSiKi)" sowie „Zuverlässige drahtlose Kommunikation in der Industrie (BZKI)" durch. Mit der Normenreihe IEC 62443 „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme" und den Normungs-Roadmaps „IT-Sicherheit" und „Industrie 4.0" bringt VDE/DKE, bei dem auch das Standardization Council Industrie 4.0 organisatorisch angesiedelt ist, die Standardisierung der IT-Sicherheit und Industrie 4.0 voran. Im Bereich Prüfung und Zertifizierung bietet das VDE-Prüfinstitut das VDE-Zertifikat „Informationssicherheit geprüft" an.

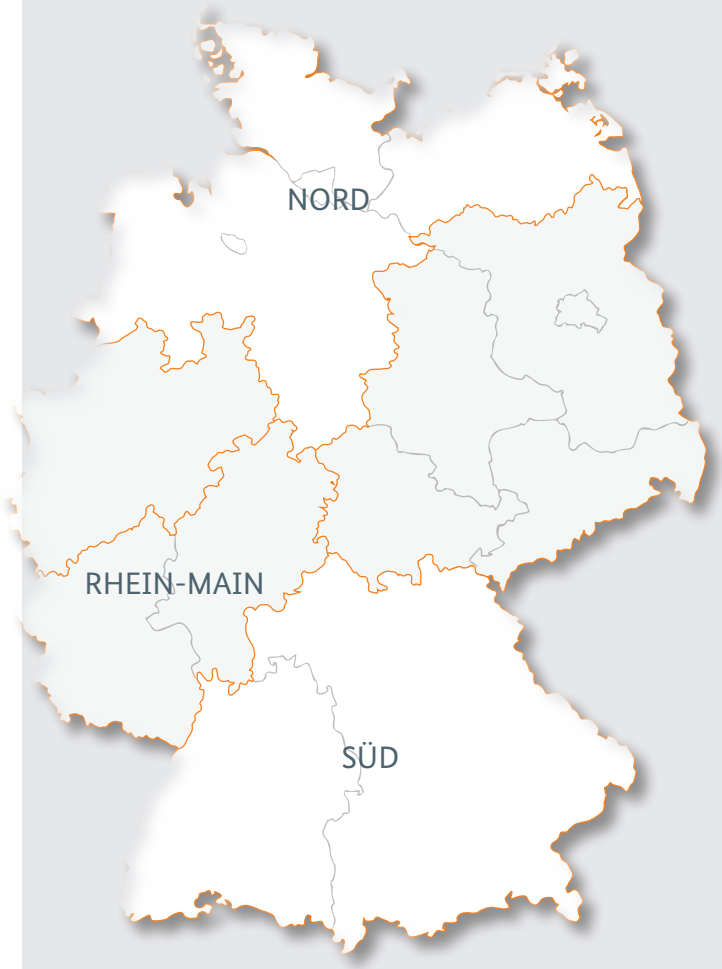
DAS BSI

Auf in die Fläche

von Fabienne Middeke, Nationales Verbindungswesen

BSI baut regionale Verbindungsbüros auf

Als nationale Kompetenzstelle für Cyber-Sicherheit bündelt das BSI fachliche und operative Expertise. Die Zahl seiner Kunden und Partner wächst. Doch wie kann diese Expertise flächendeckend für die Zielgruppen Staat, Wirtschaft und Gesellschaft in einheitlicher Form zugänglich gemacht werden? Damit beschäftigt sich seit Anfang 2017 ein neuer Bereich im BSI – das Nationale Verbindungswesen.



Die Abdeckung und Betreuung der Bundesländer durch die geplanten Verbindungsbüros des BSI

Das BSI wächst, nicht nur personell; dem Amt werden als nationale Cyber-Sicherheitsbehörde auch immer mehr Aufgaben übertragen. Das Nationale Verbindungswesen hat dabei neben der Pflege klassischer BSI-Kontakte zu Bundesbehörden, Unternehmen, Verbänden und Thinktanks auch den Auftrag, über Verbindungsbüros die Kompetenz des BSI in die Regionen zu tragen. Daneben betreut es im Bereich der Wirtschaft die „hidden champions“ und im Bereich des Staates die Bundesländer sowie internationale Organisationen mit Sitz in Deutschland.

BSI-BOTSCHAFTER VOR ORT

Um seine vielfältigen Aufgaben auch vor Ort erfüllen zu können, hat das BSI begonnen, sukzessive regionale Verbindungsbüros aufzubauen. Die Büros decken zunächst länderübergreifende Regionen beziehungsweise Ballungsräume ab, perspektivisch baut das BSI insgesamt fünf Verbindungsbüros auf – vier davon in Deutschland und eins in Belgien.

Der Aufbau hat 2017 mit Standorten im Rhein-Main-Gebiet und in Berlin begonnen. Der Pilotbetrieb ist bereits erfolgreich angelaufen, die Angebote des BSI und der Regionalbüros werden durch die verschiedenen Zielgruppen in großem Umfang nachgefragt.

2018 wird ein internationales Verbindungsbüro in Brüssel und Mitte des Jahres ein Büro in Süddeutschland eingerichtet. Anfang 2019 folgt dann noch ein Verbindungsbüro

in Norddeutschland. So erweitert das BSI mit dem Ausbau des Verbindungswesens sein Kooperationsmodell mit Staat, Wirtschaft und Gesellschaft um eine weitere Dimension.

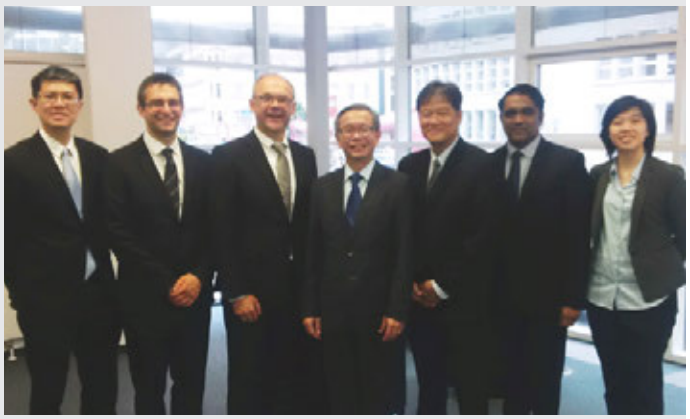
Die Verbindungspersonen werden in der Regel bei Partnerbehörden und -einrichtungen in der jeweiligen Region angesiedelt. Aktuell tragen das Bundeskriminalamt (BKA) in Wiesbaden und das Statistische Bundesamt (Destatis) in Berlin durch ihre logistische Unterstützung maßgeblich zum Erfolg des neuen BSI-Verbindungswesens bei.

BSI-Mitarbeiterinnen und -Mitarbeiter sind als Verbindungspersonen mehrere Tage in der Woche vor Ort erreichbar und stehen als Ansprechpartner für Fragen rund um das BSI und das Thema Cyber-Sicherheit zur Verfügung. Sie können außerdem eine erste Unterstützung und Anlaufstelle zu technischen Fragen sein. Und bei fachspezifischen Fragen haben sie einen kurzen Draht zu den relevanten Ansprechpartnern im BSI und erleichtern so den Zugang zum BSI als nationale Kompetenzstelle für Cyber-Sicherheit. Darüber hinaus beraten sie die Zielgruppen auch hinsichtlich der Produkte und Dienstleistungen des BSI.

START IM RHEIN-MAIN-GEBIET

Das Rhein-Main-Gebiet ist als Ballungsraum mit einer Vielzahl von dort ansässigen – zum Teil internationalen – Behörden und Unternehmen, ein idealer Startpunkt für den Aufbau des Verbindungswesens. Hier bildet die Kooperation mit dem BKA als herausgehobenem Partner einen wichtigen Schwerpunkt. Mit dem BKA arbeitet das BSI unter anderem im Nationalen Cyber-Abwehrzentrum und als Partner im German Competence Centre against Cyber Crime e.V. (G4C) zusammen.

Von Wiesbaden aus werden die Bundesländer Hessen, Rheinland-Pfalz und Saarland unterstützt. Aber auch für Unternehmen steht das Verbindungsbüro bei Fragen zum Thema Cyber-Sicherheit zur Verfügung. Im Rhein-Main-Gebiet gibt es mit der Technischen Universität Darmstadt zusätzlich ein bedeutendes Wissenschaftszentrum mit dem Forschungsschwerpunkt IT-Sicherheit. Auch hier soll das Verbindungswesen die Vernetzung mit dem BSI unterstützen. Für internationale Organisationen mit Sitz in Deutschland erbringt das BSI sogenannten „Host Nation Support“. Dies gilt auch für internationale Behörden im Raum Frankfurt.



Roland Hartmann, Referatsleiter Nationales Verbindungswesen (3.v.l.) und Fabian Weber, Verbindungsbeamter in Berlin (2.v.l.) eröffnen das Verbindungsbüro Berlin, verbunden mit dem Besuch einer Delegation der Cyber Security Agency (CSA) aus Singapur

FOKUS AUF DIE BUNDESLÄNDER

Als die nationale Cyber-Sicherheitsbehörde stellt das BSI seine Expertise künftig auch stärker den Ländern zur Verfügung. Grundlage für eine engere Betreuung der Bundesländer bildet die Cyber-Sicherheitsstrategie für Deutschland 2016, die auf eine Stärkung der Bund-Länder-Zusammenarbeit setzt und dem BSI die Aufgabe zuschreibt, Landesbehörden bei der Bewältigung von Cyber-Vorfällen zu unterstützen. Rechtlich festgelegt wird sie im Rahmen der Umsetzung der europäischen NIS-Richtlinie im jüngst geänderten BSI-Gesetz.

Die Unterstützung der Bundesländer findet im Wesentlichen auf drei Ebenen statt: Operativ im sogenannten Verwaltungs-CERT-Verbund der Computer Emergency Response Teams (CERTs), beratend durch Leistungen der Informationssicherheitsberatung und regional durch die unterstützenden Leistungen des Verbindungswesens. Das BSI stellt den Ländern Expertise, bewährte Verfahren und Produkte zur Verfügung; dies ersetzt jedoch nicht Investitionen in notwendige eigene Kompetenzen und Ressourcen auf Landesebene im Bereich Cyber-Sicherheit.

KONTAKT

Schon in der erfolgreichen Pilotierung zeigt sich, dass das BSI mit den neuen regionalen Schwerpunkten den richtigen Weg geht, um den aktuellen Herausforderungen des Cyber-Raums zu begegnen und als nationale Cyber-Sicherheitsbehörde die BSI-Expertise auch dezentral zur Verfügung zu stellen. Auch bei den weiteren Standorten in den ausgewählten Regionen wird es auf individuelle Schwerpunkte eingehen. Eine Kontaktaufnahme zum Nationalen Verbindungswesen und den Verbindungspersonen im Rhein-Main-Gebiet und in Berlin ist per E-Mail über die Adresse **BSIregional@bsi.bund.de** möglich. ■

Cyber-Sicherheit in der Digitalisierung

von Arne Schönbohm, Präsident des BSI

Das BSI als unabhängiger Gestalter

Die Digitalisierung ist zu einer wichtigen Grundlage für den technologischen Fortschritt sowie für den wirtschaftlichen und gesellschaftlichen Wohlstand geworden. Dazu zählen beispielsweise Verwaltungsverfahren wie die elektronische Beantragung von Ausbildungsförderung (BAföG), vollständig automatisierte Prozesse in der industriellen Fertigung oder die per Mobiltelefon getätigte Online-Überweisung. Doch mit den Chancen der immer weiter voranschreitenden Vernetzung wachsen auch die Herausforderungen: Die Komplexität der IT nimmt immer weiter zu und bietet Cyber-Angreifern weitreichende Möglichkeiten, Informationen auszuspähen, Geschäfts- und Verwaltungsprozesse zu sabotieren oder sich mit verschiedenen Methoden auf Kosten Dritter kriminell zu bereichern.

Es ist Aufgabe des Staats, Sicherheit auch im Cyber-Raum für seine eigenen demokratischen Verwaltungseinrichtungen, seine Wirtschaft und seine Bürgerinnen und Bürger zu schaffen und zu wahren. Mit diesem Ziel wurde vor mehr als 25 Jahren das Bundesamt für Sicherheit in der Informationstechnik durch die Bundesregierung gegründet. Es hat sich seitdem analog zur Fortentwicklung der Technologien zu einer zentralen Kompetenzstelle entwickelt. Der enorme Zuwachs an Personal in diesem Jahr um 30 Prozent auf 850 Mitarbeiter über alle Abteilungen hinweg ist ein Beleg, dass das BSI in seiner Rolle als die nationale Cyber-Sicherheitsbehörde anerkannt und gestärkt wird.

Durch diese personelle Verstärkung wird das BSI in die Lage versetzt, sich in vielen Bereichen besser aufzustellen – auch unterstützt durch eine organisatorische Neuordnung. So widmet sich beispielsweise seit Beginn des Jahres ein eigener Fachbereich dem Thema „Cyber-Sicherheit in der Digitalisierung“. IT-Sicherheitsspezialisten beschäftigen sich dort mit Themen wie der Energiewende, dem Internet der Dinge (IoT) und der Industrie 4.0 auf nationaler und internationaler Ebene und gestalten deren Entwicklung mit.

Mit der Neuordnung und dem starken Personalaufwuchs trägt das BSI den sich ändernden Anforderungen an eine nationale Cyber-Sicherheitsbehörde Rechnung. Wir verstehen, dass die Informationssicherheit Voraussetzung für die Digitalisierung ist. Und wir gestalten die Informationssicherheit. Dies gelingt nur mit einem breiten kooperativen Ansatz, der im BSI bereits seit vielen Jahren gelebt wird. Er umschließt nicht nur eine enge Zusammenarbeit mit externen Partnern aus Wirtschaft, Wissenschaft und Verwaltung, sondern insbesondere die abteilungsübergreifende Vernetzung der Mitarbeiterinnen und Mitarbeiter aus den verschiedensten Fachbereichen. Von der Kryptografie als Grundlagenforschung bis zu konkreten praktischen Angeboten wie dem IT-Grundschutz oder dem CERT-Bund sind alle notwendigen Kompetenzen zur Bewältigung hochkomplexer Fragestellungen im BSI vereint. Darin liegt das Alleinstellungsmerkmal des BSI.

Das Spektrum reicht noch viel weiter. So wird im Nationalen Lagezentrum ein tägliches Lagebild erstellt und gemeinsam in einer täglichen Lagebesprechung durch die unterschiedlichen Fachbereiche bewertet. Werden bei der Bewertung oder im täglichen Betrieb Auffälligkeiten detektiert, greifen etablierte interne und externe Reaktionswege. Meldungen für die betroffenen Zielgruppen werden erstellt, passgenaue Cyber-Abwehrmaßen werden eingeleitet und im direkten Kontakt oder durch Mobile Einsatzteams (Mobile Incident Response Team – MIRT) umgesetzt.

Dies war auch Mitte Mai der Fall, als erste Infektionen mit der Ransomware „Wannacry“ beobachtet werden konnten. Nach einer internen Bewertung und dem Austausch mit

„Wir verstehen, dass die Informationssicherheit Voraussetzung für die Digitalisierung ist.“

nationalen und internationalen Partnern hat das BSI die Betroffenen kontaktiert. Aus den von ihnen erhaltenen Informationen und der Fachexpertise konnten wir Warnungen verfassen und an unsere Kunden in Staat, Wirtschaft und Gesellschaft versenden. Aus den Erkenntnissen, die im Nachgang eines Vorfalls gezogen werden, leiten sich wiederum kurzfristige präventive Aufgaben ab, wie beispielsweise Beratungsleistungen, Produkte oder Formulierungen von Standards, um den Stand der Technik einzuhalten. So stellte das BSI im aktuellen Fall Antivirensignaturen für AV-Scanner und ein Dossier zum Schutz vor Ransomware zur Verfügung und passte seine Sensibilisierungsangebote für die Zielgruppen aus Staat, Wirtschaft und Gesellschaft an die aktuelle Lage an.

Darüber hinaus sind diese Vorfälle immer wieder Anlass, auf die strategischen Forderungen des BSI aufmerksam zu machen, so wie in diesem Fall auf Mindeststandards und die Verpflichtungen der Unternehmen für ihre IT-Produkte. Hier wird die für das kommende Jahr geplante Etablierung eines ersten Gütesiegels, wie in der Cyber-Sicherheitsstrategie gefordert, einen Meilenstein setzen.

Dieses schnelle, bewährte und zielführende Vorgehen wäre ohne das Zusammenwirken aller beteiligten Kolleginnen und Kollegen im BSI gemeinsam mit den nationalen und internationalen Partnern nicht möglich.

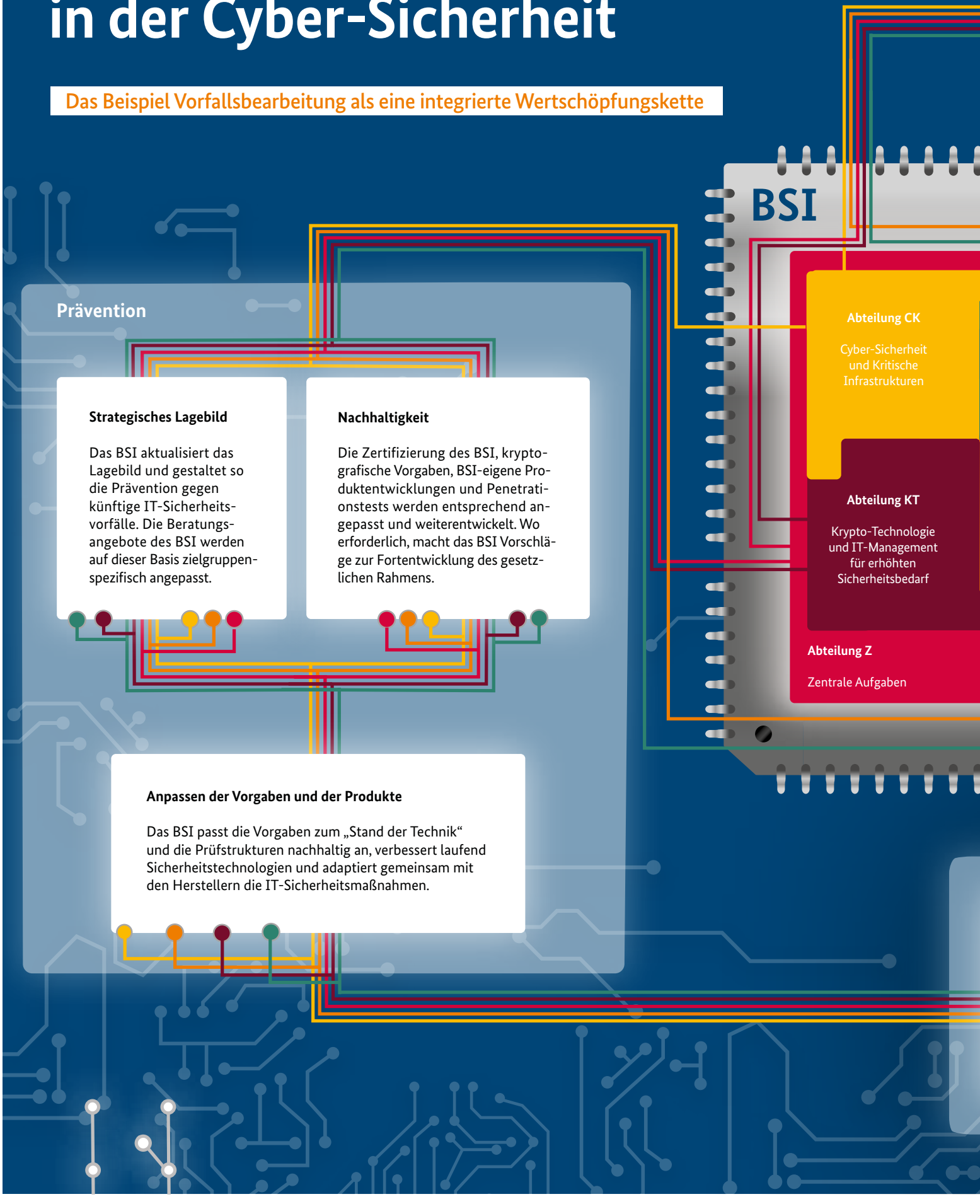
Nach unseren Erkenntnissen ist auch zukünftig mit einer Vielzahl solcher Vorfälle zu rechnen, die auch vor lebenswichtigen Einrichtungen oder Ländergrenzen keinen Halt machen – die zunehmende Digitalisierung aller Lebensbereiche lässt keinen anderen Schluss zu. Umso größer wird der Stellenwert einer engen internationalen Zusammenarbeit, eines unabhängigen Expertenwissens in der Digitalisierung sowie eines vernünftigen Risikomanagements, das das Thema Cyber-Sicherheit beinhaltet. Nur ein ganzheitlicher Ansatz der Informationssicherheit führt dazu, dass die Digitalisierung in allen Lebensbereichen gelingt.

Aufgrund der Synergien und der Abläufe sind diese Kompetenzen und Kooperationen im BSI gut aufgehoben. Erfolgsmodelle wie der BSI IT-Grundschutz als der nationale Standard für die Informationssicherheit beweisen dies eindeutig. Aber auch die Weiterentwicklung der Krisenreaktionsfähigkeit des BSI, mit einer neuen Aufstellung des Cyber-Abwehrzentrums, zählt dazu. Durch diese zentrale Stellung verfolgen wir das Ziel, als „Thought Leader“ für Cyber-Sicherheit wesentliche Impulse in der Gestaltung der Digitalisierung zu setzen.

Wir gehen davon aus, dass analog zum Wachstum der Bedeutung des Themas auch die Ressourcen für das BSI zunehmen werden. Dass die Ressourcen beim BSI in guten Händen sind, konnten wir bereits im ersten Halbjahr, mit der Besetzung von über der Hälfte der zugewiesenen Stellen, beweisen. ■

Das BSI – vernetzte Kompetenz in der Cyber-Sicherheit

Das Beispiel Vorfallsbearbeitung als eine integrierte Wertschöpfungskette



Detektion

Erkennen der Schwachstelle

Das BSI führt Tests der Hard- und Software durch und deckt dabei Sicherheitslücken und Schwachstellen auf. Diese Schwachstellen werden evaluiert sowie einer Sicherheitsanalyse unterzogen.

Erkennen des Angriffs

Das BSI detektiert Anomalien in IT-Netzen und Systemen und identifiziert so konkrete Cyber-Angriffe.

Abteilung B

Beratung für Staat, Wirtschaft und Gesellschaft

Abteilung D

Cyber-Sicherheit in der Digitalisierung, Zertifizierung und Standardisierung

Reaktion

Koordination der Cyber-Abwehr

Das BSI als nationales IT-Krisenreaktionszentrum koordiniert das Vorgehen mit Herstellern, Providern, Betroffenen, IT-Sicherheitswirtschaft, Kritischen Infrastrukturen und anderen Behörden.

Bewältigen des Cyber-Angriffs

Das BSI unterstützt die betroffenen Einrichtungen bei der Abwehr des konkreten Angriffs und hilft bei der Wiederherstellung des Regelbetriebes. Staat, Wirtschaft und Gesellschaft und internationale Partner werden über alle notwendigen Maßnahmen informiert.

Bewerten des Cyber-Angriffs

Das BSI erstellt in Zusammenarbeit mit allen Fachbereichen eine Lagedarstellung und gibt eine Bewertung zum Vorfall, der Schwachstelle und deren Ausnutzbarkeit. Diese Ausnutzbarkeit wird nochmal anhand von Einsatzszenarien für Staat, Wirtschaft und Gesellschaft aufgeschlüsselt dargestellt.

Das BSI wächst mit seinen Aufgaben

von Dr. Ildiko Knaack, Referat Organisation, Yanick Detzel, Referat Innerer Dienst, Arno Köster, Projektgurppe Neue Dienstliegenschaft

Neue Stellen, neue Organisation, neue Gebäude

Das BSI als nationale Informations- und Cyber-Sicherheitsbehörde wurde in diesem Jahr personell mit der Zuweisung von 180 Stellen weiter gestärkt. Das Amt wuchs damit um fast 30 Prozent auf nunmehr circa 850 Stellen an. Diesen Zuwachs zu managen, heißt zum einen, entsprechend qualifizierte Mitarbeiterinnen und Mitarbeiter zu gewinnen, sie unterzubringen und ihre Integration ins Haus sicherzustellen. Zum anderen wurde auch die Organisation an die neuen Aufgaben angepasst.

STELLENZUWEISUNG 2017

+30%

Links oben: Die im Mai bezogene neue Mietliegenschaft Heinemannstraße 11 in Bonn-Hochkreuz

Rechts oben: Feierliche Eröffnung der neuen Liegenschaft

Links: Oberbürgermeister der Stadt Bonn Ashok Sridharan, BSI-Präsident Arne Schönbohm und seine Amtskollegen von der österreichischen A-SIT, Wolfgang Ebner, der schweizerischen ISB, Peter Fischer, und der luxemburgerischen ANSSI, Gerard Caye

Um dem Stellenzuwachs der vergangenen Jahre auch räumlich gerecht werden zu können, hat das BSI im Mai dieses Jahres eine weitere Mietliegenschaft bezogen. Die vom Hauptgebäude des BSI gut zu Fuß zu erreichende Liegenschaft beherbergt auf zwei Etagen nun die Abteilung D sowie drei Referate der Abteilung B. Gegenwärtig wird der Bonner Immobilienmarkt auf Basis des genehmigten Raumbedarfs für das Jahr 2017 erneut sondiert, um eine weitere Liegenschaft anzumieten. Ziel ist es, mithilfe der Bundesanstalt für Immobilienaufgaben ein weiteres, den Ansprüchen des BSI gerecht werdendes Objekt zu finden, das sich am besten wieder in räumlicher Nähe zu den bereits angemieteten Flächen befindet.

NEUE DIENSTLIEGENSCHAFT

Durch die derzeitige getrennte Unterbringung in drei verschiedenen Liegenschaften werden die Geschäftsprozesse des BSI erheblich erschwert. Zudem entstehen unnötige Wegezeiten, da die Beschäftigten zwischen den Standorten pendeln müssen. Dieser unbefriedigende Zustand soll durch eine neue Dienstliegenschaft beendet werden.

Die neue Dienstliegenschaft sollte möglichst zentral liegen, nicht zuletzt, um eine enge Zusammenarbeit mit anderen Behörden und großen Firmen, insbesondere um das ehemalige Regierungsviertel herum, zu ermöglichen. Die direkte Nähe zu unseren Partnern und die damit verbundene unmittelbare Verfügbarkeit von Know-how sind maßgebliche Erfolgsfaktoren für die Aufgabenerfüllung des BSI. Ein weiteres Kriterium ist das stetig wachsende Aufgabenportfolio. Es wird absehbar für mehr Personal und einen größeren Flächenbedarf sorgen. Darum ist die neue Dienstliegenschaft so zu gestalten, dass eine variable Nutzung möglich ist. Und schließlich spielt auch die verkehrstechnische Lage eine wichtige Rolle. Aufgrund von Verfügbarkeitsanforderungen ist es wichtig, dass das BSI jederzeit problemlos mit Kraftfahrzeugen und dem ÖPNV erreichbar ist.

Planungsgebiet Neue Dienstliegenschaft BSI

Das BSI als die nationale Cyber-Sicherheitsbehörde wird daher am Standort Bonn einen adressbildenden Neubau realisieren, der den Sicherheits-, Geheimschutz- sowie technischen und funktionalen Anforderungen des BSI genügt, den Charakter des Amtes als fortschrittliche IT-Sicherheitsbehörde widerspiegelt, eine optimale Unterstützung der Geschäftsprozesse des Amtes sicherstellt, eine positive und zeitgemäße Arbeitsumgebung für die Beschäftigten bietet und Erweiterungsmöglichkeiten bereithält.

Das Planungsgebiet liegt – in rund einem Kilometer Entfernung vom heutigen Dienstsitz des BSI in der Godesberger Allee – im nördlichen Bereich des Stadtbezirks Bad Godesberg, Ortsteil Plittersdorf, direkt gegenüber dem Forschungszentrum Caesar. Das im Eigentum der Bundesanstalt für Immobilienaufgaben stehende Baugrundstück umfasst rund 37.500 m². Das Bebauungsareal wird begrenzt von der Ludwig-Erhard-Allee im Nordosten, der Johanna-Kinkel-Straße im Nordwesten und Westen und grenzt im Süden an die Bestandsbebauung entlang der Kennedyallee beziehungsweise der Frankenstraße an.

Für die Neubauplanung wird von einer Beschäftigtenzahl von rund 950 Mitarbeitern ausgegangen. Auf der Grundlage des definierten Raumprogramms und -bedarfs der Behörde ergibt sich ein Flächenbedarf von circa 60.000 m² Bruttogrundfläche. Um diesen zu realisieren, sind verschiedene städtebauliche Konzeptionen auf dem Grundstück denkbar. Für den Entwurf des Neubaus soll daher unter Beachtung der städtebaulichen Rahmenbedingungen der Stadt Bonn ein Architekturwettbewerb durchgeführt werden. Das Wettbewerbsergebnis wird dann auch Grundlage für das weitere Bebauungsplanverfahren werden.

REORGANISATION

Anfang 2017 wurde eine Reorganisation des BSI durchgeführt, um den wachsenden Aufgaben und dem damit verbundenem personellen Aufwuchs Rechnung zu tragen. Der neue Aufbau spiegelt die Zielgruppen Staat, Wirtschaft und Gesellschaft sowie die Handlungsfelder Prävention, Detektion und Reaktion wider, in denen das BSI die Informationssicherheit in der Digitalisierung gestaltet. Die vier Fachabteilungen werden dabei von der Zentralabteilung unterstützt. ■

DIE VIER FACHABTEILUNGEN UND DIE ZENTRALABTEILUNG

ABTEILUNG CK

In der **Fachabteilung CK „Cyber-Sicherheit und Kritische Infrastrukturen“** werden rund um die Uhr Cyber-Angriffe auf Regierungsnetze und auf Bundesbehörden detektiert sowie die Cyber-Sicherheit in Betriebssystemen, Anwendungen und im Internet gestaltet. Gleichfalls werden präventiv Penetrationstests und IS-Revisionen von Mitarbeitern des BSI durchgeführt. Weiterhin sind in dieser Abteilung das operativ arbeitende Nationale IT-Lagezentrum, die Meldestelle unter anderem für IT-Sicherheitsvorfälle, das Computer Emergency Response Team des Bundes (CERT-Bund), das Nationale Cyber-Abwehrzentrum und die Mobile Incident Response Teams (MIRT) angesiedelt. Auch das tägliche IT-Lagebild entsteht in dieser Abteilung. Ein weiterer präventiver Schwerpunkt, der mit der Umsetzung des IT-Sicherheitsgesetzes stark ausgebaut worden ist, ist die Betreuung der Kritischen Infrastrukturen. Und nicht zuletzt wird hier der bekannte IT-Grundschutz des BSI weiterentwickelt.

ABTEILUNG B

In der **Fachabteilung B „Beratung für Staat, Wirtschaft und Gesellschaft“** werden im Rahmen der Prävention alle Beratungsaufgaben gebündelt. Hierzu gehören die „klassische“ Informationssicherheitsberatung, die Lauschabwehr und Abhörsicherheit genauso wie die IT-Sicherheitsberatung für die IT-Konsolidierung, die Sicherheit der Regierungsnetze, Cloud Computing und Informationssicherheitsprodukte für Behörden. Neben dem Staat werden hier Cyber-Sicherheitsaufgaben für Wirtschaft und Gesellschaft wahrgenommen und die internationalen Beziehungen gepflegt. Daneben wird hier das Nationale Verbindungswesen zu anderen Bundesbehörden aufgebaut. Auch die Umsetzung und Entwicklung von IT-Sicherheitsvorgaben für die Politik und die fachliche Begleitung von Rechtssetzungen mit IT-Sicherheitsbezug finden in dieser Abteilung seinen Platz.

ABTEILUNG KT

Die **Fachabteilung KT „Krypto-Technologie und IT-Management für erhöhten Sicherheitsbedarf“** bündelt einerseits alle Aufgaben im Zusammenhang von Vorgaben und Zulassungen von Krypto-Systemen und ist andererseits für deren Evaluierung und Betrieb zuständig. Dazu gehören beispielsweise VS-IT-Systeme, kryptografische Verfahren und sichere mobile Lösungen. Auch die Abstrahlsicherheit von IT-Geräten und -Systemen wird hier auf den Prüfstand gestellt. Schließlich wird von dieser Abteilung das Krypto- und Schlüsselmanagement wahrgenommen. Im BSI werden vielfältige IT-Verfahren mit erhöhtem IT-Sicherheitsbedarf betrieben. Ihr Management, ihre Planung und ihr Betrieb gehören zu den Aufgaben der Abteilung KT, genauso wie das BSI-eigene IT-Sicherheitsmanagement.

ABTEILUNG D

Die Cyber-Sicherheit in der Digitalisierung von Staat, Wirtschaft und Gesellschaft ist ein Schwerpunkt der **Fachabteilung D „Cyber-Sicherheit in der Digitalisierung, Zertifizierung und Standardisierung“**. Ein weiterer ist die Cyber-Sicherheit für elektronische Identitäten (eID) in Anwendungen des E-Governments, in Chipkarten oder in Kontrollinfrastrukturen sowie die Sicherstellung der zugehörigen Chipsicherheit. Die Abteilung wirkt an nationalen, europäischen und internationalen Standards mit und erteilt weltweit die meisten Zertifikate für hardwarenahe Verfahren, Software, COTS-Produkte und IT-Sicherheitsdienstleister.

ABTEILUNG Z

Die **Zentralabteilung Z „Zentrale Aufgaben“** mit den klassischen Aufgabenfeldern Organisation, Personalmanagement, Haushalt und Innerer Dienst sowie der Vergabe und Projektbegleitung von mehr als 150 Projekten im Jahr und dem für eine IT-Sicherheitsbehörde besonders wichtigen Objekt- und Geheimschutz unterstützt durch interne Services die Fachabteilungen.

SICHERHEITSBEDÜRFNIS TRIFFT RISIKOBEREITSCHAFT

15. Deutscher IT-Sicherheitskongress

Vom 16. bis 18. Mai trafen sich die wichtigsten Vertreter der IT-Sicherheitsbranche auf dem 15. Deutschen IT-Sicherheitskongress in Bonn, der in diesem Jahr unter dem Motto „Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis“ stand. Rund 600 Teilnehmer tauschten sich in mehr als 50 Fachvorträgen und Podiumsdiskussionen unter anderem über die Herausforderungen der Digitalisierung, das Internet der Dinge und Quantenkryptografie aus. Eine kongressbegleitende Ausstellung ergänzte den Diskurs.

Bild oben: v.l. BSI-Präsident Arne Schönbohm, Andreas Könen (BMI), Wolfgang Ebner (A-SIT), Peter Fischer (ISB), Gerard Caye (ANSSI Luxemburg), Guillaume Poupard (ANSSI Frankreich)

Bild unten: Teilnehmer des 15. Deutschen IT-Sicherheitskongresses in der Stadthalle Bad Godesberg in Bonn

Nur wenige Tage nach dem Cyber-Angriff mit der Ransomware „WannaCry“, von der Computer in 150 Ländern betroffen waren, beherrschte das Thema Cyber-Bedrohungen den Auftakt des Sicherheitskongresses und verdeutlichte einmal mehr die Bedeutung von Cyber-Sicherheit. Bei seiner Eröffnungsrede betonte BSI-Präsident Arne Schönbohm, dass der Staat nicht wehrlos sei und stellte dessen Handlungsfähigkeit als wichtigen Bestandteil der IT-Sicherheit heraus. Denn nur wenn der Staat die Informationssicherheit gestalten könne, werde die Digitalisierung gelingen.

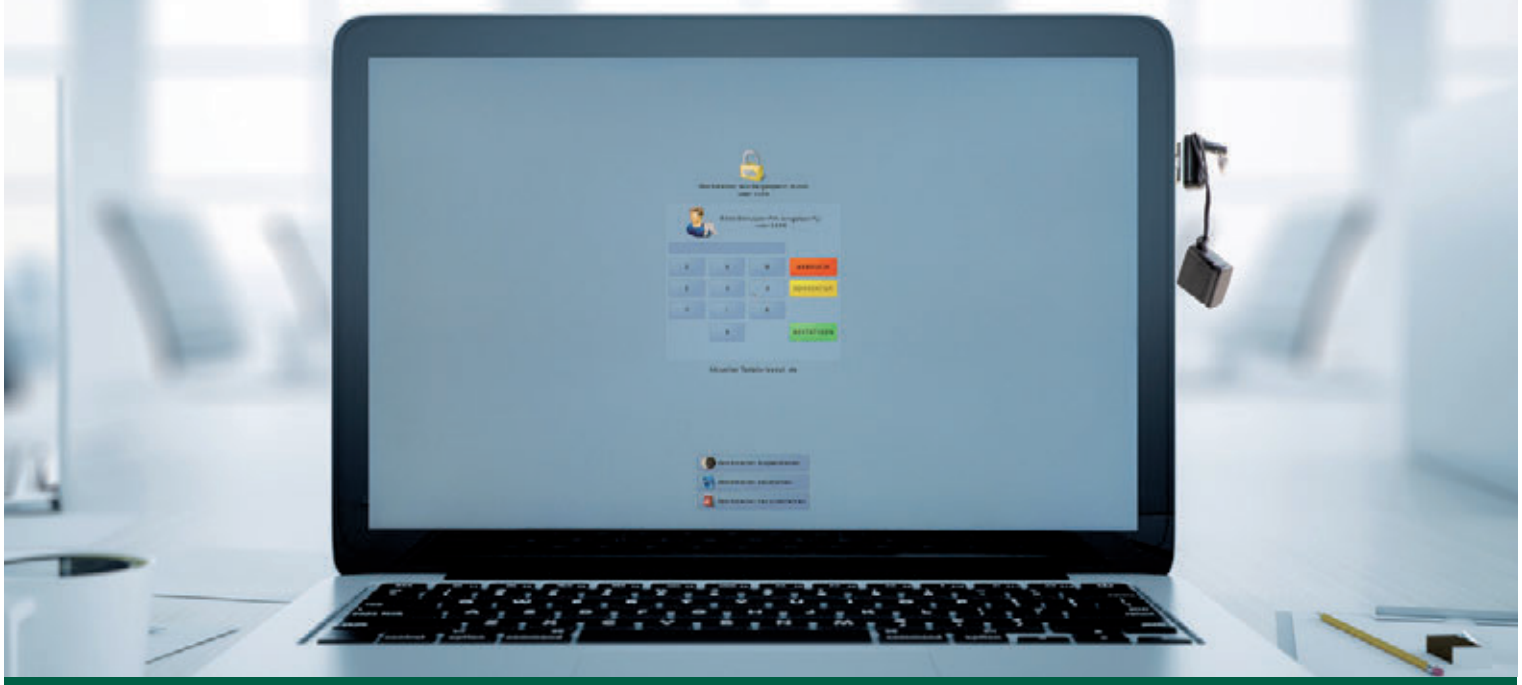
Der Deutsche IT-Sicherheitskongress, alle zwei Jahre eine feste Größe im Veranstaltungskalender der IT-Sicherheitsbranche, hat zum Ziel, Cyber- und IT-Sicherheit aus verschiedenen Perspektiven zu beleuchten, zukunftsorientierte Lösungsansätze vorzustellen und weiterzuentwickeln. ■

IT-SICHERHEIT
IN DER PRAXIS

Vertrauliches mobiles Arbeiten

von Oliver Zendel, Referatsleiter Kryptografie in Anwendungen

Kollaboratives Verarbeiten digitaler Verschlusssachen



Moderne IT-Systeme sind in der Regel nur dafür konzipiert, digitale Verschlusssachen bis zu einem gewissen Geheimhaltungsgrad zu verarbeiten, denn sie werden immer in einem Spannungsfeld von Funktionalität, Kosten, Sicherheit und Zeit entwickelt und realisiert. Das nach den Vorgaben des BSI konzipierte Produkt SINA Workflow hingegen setzt die Anforderungen an ein elektronisches Vorgangsbearbeitungssystem für digitale Verschlusssachen auch für höhere Geheimhaltungsstufen um.

Wer kennt nicht diese Situation? Kurz vor Feierabend müssen noch wichtige Informationen erstellt und an die richtigen Adressaten verteilt werden. Und dies alles so schnell, so effizient und so sicher wie möglich. Moderne IT-Systeme treten mit dem Versprechen an, solche Anwendungsszenarien abbilden zu können. Diese Systeme sind in der Regel jedoch nur dafür konzipiert, Verschlusssachen bis zum maximalen Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH zu verarbeiten. Doch wie sieht die Situation bei Verschlusssachen der Geheimhaltungsgrade VS-VERTRAULICH und GEHEIM aus? Die Realisierung geeigneter IT-Systeme zur Bearbeitung digitaler Verschlusssachen wird in einem Spannungsfeld von Funktionalität, Kosten, Sicherheit und Zeit durchgeführt. Dabei ist zu beachten, dass im Falle einer Kenntnisnahme durch Unbefugte der Bundesrepublik Deutschland oder einem ihrer Länder schwerer Schaden zugefügt werden kann – in Einzelfällen sogar mit Gefahr für Leib und Leben.

KENNTNIS NUR, WENN NÖTIG

Von einer Verschlusssache dürfen zur Risikominimierung nur die Personen Kenntnis erlangen, die diese Informationen benötigen, um ihre Aufgaben zu erledigen. Dieses Prinzip wird „Kenntnis nur, wenn nötig“ genannt. Um es nachvollziehbar und überprüfbar umzusetzen, bietet es sich an, ein Rechte- und Rollen-Konzept umzusetzen, das seine Grundsicherheit aus kryptografischen Verfahren ableitet. Dies bedeutet, dass alle schützenswerten Informationen verschlüsselt gespeichert werden. Nur die Benutzer, die nach dem oben genannten Grundsatz auf die Informationen zugreifen dürfen, sind in der Lage, sie zu entschlüsseln. Ergänzt man diese Verschlüsselung mit einer sicheren Umgebung, um die Informationen zu entschlüsseln, zu kapseln und zu betrachten, erhält man zusätzlich eine sichere Informationsflusssteuerung.

SICHERHEIT ÜBER DEN KOMPLETTEN LEBENSZYKLUS

Um diese Anwendungsszenarien umzusetzen, ist der komplette Lebenszyklus von digitalen Verschlusssachen abzubilden. Insbesondere die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität müssen bei der Verarbeitung digitaler Verschlusssachen über den kompletten Lebenszyklus zugesichert werden können. Dieser Lebenszyklus lässt sich grob folgendermaßen beschreiben:

- Erstellung: Umgebung zur kontrollierten Erstellung und Verarbeitung von Verschlusssachen mit einer Integrationsfähigkeit von handelsüblichen Produkten
- Speicherung: Software zur sicheren Speicherung von elektronischen Verschlusssachen
- Zugriff und Verwaltung: Registratur-, Dokumenten-, Metadaten- und Indexverwaltung für den geordneten Zugriff auf die sicher gespeicherte Information unter Wahrung des Prinzips „Kenntnis nur, wenn nötig“
- Prozessunterstützung: Workflow- und Business-Process-Management-Software zur Steuerung der VS-Prozesse, wie beispielsweise Weitergabe, Registrieren oder Drucken von Verschlusssachen
- Protokollierung: Software zur revisionssicheren Protokollierung der VS-Prozesse entsprechend rechtlichen und regulativen Anforderungen. Hierdurch werden die benötigten Nachweise erzeugt und sicher gespeichert.

Nachvollziehbares Verwaltungshandeln spielt auch bei der Bearbeitung von elektronischen Verschlusssachen eine wichtige Rolle. Dokumente zu Vorgängen und Akten zu gruppieren ist als Basisfunktionalität des nachvollziehbaren Verwaltungshandelns eine unverzichtbare funktionale Anforderung. Zur Verwaltung von digitalen Verschlusssachen zählt neben dem geordneten Ablegen in Vorgängen und Akten auch das gesicherte Identifizieren einzelner Dokumente, Vorgänge oder Akten. Durch dieses sichere Identifizieren ist es möglich, Metadaten wie insbesondere den Geheimhaltungsgrad sicher an eine elektronische Verschlusssache zu binden.

SICHERE UND VERTRAUENSWÜRDIGE NACHWEISE

Der Schutz von geheim zu haltenden Informationen bedeutet für jeden Beteiligten eine große Verantwortung. Deren Grundlage ist das Vertrauen, das jedem Benutzer entgegengebracht wird. Darauf aufbauend ist es technisch zwingend erforderlich, dass Entscheidungen der Benutzer gesichert nachgewiesen werden. Dies leistet eine Funktion, die Aktionen sicher an die Benutzer bindet. Vergleichbar mit einer Unterschrift unter einem Vertrag werden Aktionen somit nachweisbar den jeweils handelnden Benutzern zugeordnet. Diese elektronischen Nachweise sind die vertrauenswürdige Grundlage für die durch die Vorschriften geforderten Verzeichnisse, wie beispielsweise das Bestandsverzeichnis oder das Quittungsbuch.

KOLLABORATIVES ARBEITEN MIT WORKFLOWS

In der Regel sind an der Erstellung von Dokumenten mehrere Personen beteiligt. Die Gründe dafür sind vielfältig: Mal geht es um Qualitätssicherung, mal um das kollaborative Erstellen von Texten. Ein bewährter Prozess zur Qualitätssicherung in Behörden sind beispielsweise Mitzeichnungen. Ein modernes IT-System zur Realisierung einer Vorgangsbearbeitung für elektronische Verschlusssachen muss diese Prozesse auf eine sichere Art und Weise anbieten. Dabei ist zu berücksichtigen, dass nicht alle Anwender und alle Anwendungsszenarien gleich sind. Die Workflows müssen flexibel anpassbar sein, ohne dass diese notwendige Flexibilität die Sicherheitseigenschaften des Gesamtsystems negativ beeinflusst.

SINA WORKFLOW

Das nach den Vorgaben des BSI konzipierte Produkt SINA Workflow setzt die hier dargestellten Anforderungen beispielhaft für ein elektronisches Vorgangsbearbeitungssystem für digitale Verschlusssachen um. Das Bundeskriminalamt konnte während der Entwicklung des SINA Workflow als Pilotbehörde gewonnen werden und erprobt die Lösung auf Praxistauglichkeit in Abstimmung und mit Unterstützung durch das BSI. ■

Weitere Informationen: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/SINA.html

Verifikation von digitalen Zertifikaten

von Dr. Heike Hagemeier und Armin Cordel, Kryptographische Vorgaben und Entwicklungen

Entwicklung eines Testtools als Open Source Software

Digitale Zertifikate sind bei der authentisierten und verschlüsselten Kommunikation ein wichtiger Vertrauensanker. Fehler bei der Gültigkeitsprüfung dieser Zertifikate können sicherheitskritisch sein. Ein BSI-Projekt soll dazu beitragen, dass Routinen zur Verifikation von digitalen Zertifikaten korrekt implementiert werden.

Für die digitale Kommunikation werden Zertifikate benötigt, um die Identitäten der Kommunikationspartner zu bestätigen beziehungsweise öffentliche Schlüssel für Public-Key-Verfahren zu validieren. Diese digitalen Zertifikate dienen der Bindung der öffentlichen Schlüssel an die Identität der Teilnehmer. Ein Teilnehmer kann dabei beispielsweise der Server einer Bank oder eines anderen Onlinedienstes sein.

Die Verwaltung digitaler Zertifikate erfolgt in Public-Key-Infrastrukturen (PKI). Eine PKI ist eine Zertifizierungshierarchie, die wie ein Baum strukturiert ist. An der Wurzel dieses Baumes sitzt die Root Certification Authority (Root-CA). Diese stellt sich ein selbstsigniertes Zertifikat aus, mit dem sie dann weitere Zertifikate für untergeordnete Certification Authorities (Sub-CAs) signiert. Die Blätter des Baumes werden von den Zertifikaten der Teilnehmer gebildet. Einen Pfad von der Wurzel bis zu einem Blatt nennt man eine Zertifikatskette (siehe Abbildung rechts).

Um die Bindung der Identität eines Teilnehmers an seinen Schlüssel durch einen weiteren Teilnehmer (beziehungsweise dessen Applikation) prüfen zu können, ist eine zuverlässige Verifikation dieser Zertifikatsketten unerlässlich. Beispielsweise muss ein Browser die Identität des Servers einer Bank anhand des vom Server übermittelten Zertifikats überprüfen können. Werden von Anwendungen fehlerhafte, ungültige Zertifikatsketten (aufgrund von Programmierfehlern) akzeptiert, so stellt dies in gleicher Weise ein Sicherheitsrisiko dar wie Fehler in den Implementierungen der kryptografischen Algorithmen.

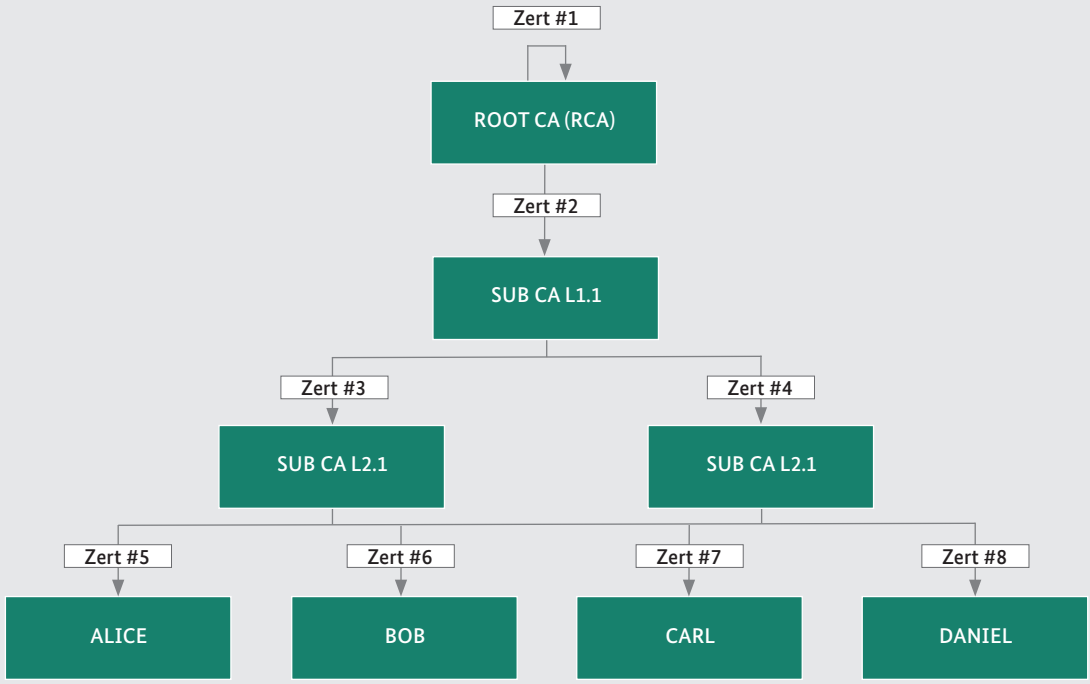
VERSCHIEDENE FORMATE, VIELE FEHLER

Es gibt verschiedene Formate für digitale Zertifikate, wobei X.509 (in der Version 3) der gängigste Standard ist. Dieser definiert ein Rahmenwerk für Public-Key-Infrastrukturen und digitale Zertifikate, das für die jeweiligen Anwendungsfelder weiter konkretisiert werden kann. Für die Nutzung von X.509-Zertifikaten im Internet hat die Internet Engineering Task Force (IETF) Konkretisierungen zum X.509-Standard im Request for Comments (RFC) 5280 festgelegt. Dort wird das Format von X.509-Zertifikaten mit allen Erweiterungsmöglichkeiten sowie ein Algorithmus zur Verifikation von Zertifikatsketten ausführlich beschrieben.

Dennoch sind in der Vergangenheit in vielen bekannten Kryptobibliotheken Fehler in den Routinen zur Verifikation von Zertifikatsketten gefunden worden. Forscher der

BEISPIEL EINER PKI-HIERARCHIE

Pfeile sind Zertifikate und Kästen sind Einheiten / PKI-Teilnehmer



Stanford University und der University of Texas haben im Herbst 2012 die Zertifikatsverifikation in TLS-Bibliotheken (zum Beispiel OpenSSL) und Bibliotheken für den Datentransport (zum Beispiel Apache HttpClient, cURL) untersucht und zogen folgendes Fazit: „Our main conclusion is that SSL certificate validation is completely broken in many critical software applications and libraries."

Ein weiteres Team von Forschern der University of Texas hat im Mai 2014 in den meistgenutzten TLS -Implementierungen nach Fehlern in der Zertifikatsverifikation gesucht. Ihr Ansatz dabei war, aus bestehenden, im Internet verfügbaren Zertifikaten neue Zertifikate („Frankencerts") zusammenzufügen. Dadurch entdeckten sie verschiedene Fehler bei der Zertifikatsverifikation in Kryptobibliotheken wie PolarSSL und GnuTLS.

INNOVATIVES BSI-PROJEKT

In einem Projekt des BSI entwickelt die media transfer AG mit dem Unterauftragnehmer cryptosource GmbH derzeit ein Testtool, mit dessen Hilfe Routinen zur Verifikation von digitalen Zertifikaten beziehungsweise Zertifikatsketten untersucht werden können. Dafür wurde auf Basis einer Analyse von RFC 5280 und weiteren relevanten Standards eine Testspezifikation ausgearbeitet. Für jeden der Fälle aus der Testspezifikation erstellt das Tool eine Reihe von Zertifikaten. Diese bilden abhängig vom Testfall eine gültige oder eine fehlerhafte Zertifikatskette. In einzelne Zertifikate werden dafür bewusst Fehler eingebaut. Beispielsweise kann der Gültigkeitszeitraum des Zertifikats in der Vergangenheit liegen. Mittels dieser (fehlerhaften) Zertifikatsketten können dann (Implementierungs-)Fehler in den Verifikationsroutinen detektiert werden.

Nach Abschluss des Projekts soll das Testtool als Open Source zur Verfügung gestellt werden. ■

Weitere Informationen zum Thema Zertifikate und Verwaltungs-PKI: https://www.bsi.bund.de/VPKI

SICHERHEITSRELEVANTE MODULE

Von Jawad Ahmad, eID-Anwendungen im E-Government und Dr. Astrid Schumacher, Fachbereichsleiterin Beratung und Unterstützung

TR-RESISCAN und TR-ESOR in der praktischen Umsetzung

Es ist eine der wesentlichen Aufgaben des BSI, sicherheitsrelevante Produkte und Prozesse der Informationstechnik zu analysieren und zu bewerten sowie Orientierungshilfen und Handlungsleitfäden zur Verfügung zu stellen. Angesichts der voranschreitenden Digitalisierung und dem damit einhergehenden Bedarf an zeitgemäßen und sicheren E-Government Lösungen rückt die eAkte als zentrales Element für die Modernisierung der Verwaltungsprozesse weiter in den Fokus.

TECHNISCHE RICHTLINIEN ALS BASIS

Als nationale Cyber-Sicherheitsbehörde stellt das BSI Technische Richtlinien zur Verfügung, die eine Umsetzung entsprechender E-Government-Lösungen nach dem Stand der Technik ermöglichen.

- Für die rechtskonforme elektronische Aktenführung definiert die BSI-TR 03138 Ersetzendes Scannen (kurz: TR-RESISCAN) Anforderungen für die ordnungsgemäße und risikominimierende Gestaltung des Scanprozesses. Die TR-RESISCAN hat zum Ziel, Anwendern in Verwaltung, Justiz, Wirtschaft und Gesundheitswesen als Handlungsleitfaden und Entscheidungshilfe zu dienen, wenn es darum geht, Papierdokumente nicht nur einzuscannen, sondern nach Erstellung des Scanproduktes auch zu vernichten.

- Darüber hinaus definiert das BSI mit der Technischen Richtlinie BSI-TR 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ (kurz: TR-ESOR) auf Basis der internationalen Standards RFC 4998 und RFC 6283 und der ETSI-AdES-Signaturformate sowie der eIDAS-Verordnung und des Vertrauensdienstegesetzes einen Leitfaden für die Beweiswerterhaltung archivierter Daten und Dokumente bis zum Ende der gesetzlich vorgeschriebenen Aufbewahrungspflicht.

Der Gesetzgeber fordert für die elektronische Aktenführung die Einhaltung des „Stands der Technik“ (unter anderem in den §§ 6 und 7 des Gesetzes zur Förderung der elektronischen Verwaltung (eGovG) sowie in den §§ 298a Zivilprozessordnung (ZPO) und 32e Strafprozessordnung (StPO)). Der „Stand der Technik“ kann bei Befolgen der Technischen Richtlinien des BSI regelmäßig als eingehalten gelten.

Sowohl hinsichtlich dem ArchiSig-Modell, das der TR-ESOR zugrunde liegt, als auch mit einem nach TR-RESISCAN erzeugten Digitalitsat wurden Simulationsstudien durchgeführt, die in rechtlicher Hinsicht nachgewiesen haben, dass mit der jeweilige Beweiswert optimiert und die Beweisführung vor Gericht entsprechend vereinfacht werden kann, wenn den TR-Empfehlungen gefolgt wird.

TR-RESISCAN

Die TR-RESISCAN bietet mit ihren strukturierten Anforderungen pragmatische Orientierungshilfen zur Einhaltung ordnungsgemäßer (Scan-)Prozesse. Durch den modularen Aufbau ist ein auf den eigenen Anwendungsbereich individuell zugeschnittenes Konzept möglich, welches neben der Wahrung des Beweiswerts des papiergebundenen Originals (beispielsweise vor Gericht) auch eine angemessene Kosten-Nutzen-Relation berücksichtigt. Bereits mit dem Basismodul

werden alle grundsätzlichen Sicherheitsanforderungen an Integrität, Vertraulichkeit und Verfügbarkeit sowie Datenschutz erfüllt.

Die praktische Umsetzung der TR-RESISCAN erfolgte bereits durch zahlreiche Anwender aus Verwaltung und Wirtschaft. Unter anderem wurde die Leitlinie zum ersetzenden Scannen von Dokumenten in Kommunen erarbeitet. Hubert Ludwig, Geschäftsführer der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH, erklärt den Nutzen der TR-RESISCAN:

> *„Bei der voranschreitenden Digitalisierung ist die technische Richtlinie TR 03138 Ersetzendes Scannen (RESISCAN) des BSI ein wichtiges unterstützendes Instrument. Je nach erforderlichen Schutzbedarf der Dokumente kann mehr Rechtssicherheit für den Scanprozess erlangt werden, wenn das Papier nach dem Scannen vernichtet und nur noch das digitale Dokument verwendet werden soll. Dementsprechend ist die Zertifizierung ein gewichtiger Nachweis dafür, dass die Prozesse und Systeme für das ersetzende Scannen die in der Richtlinie aufgestellten technischen und organisatorischen Anforderungen erfüllen."*

Für Torsten Wunderlich (Leiter des DATEV-Informationsbüro/Berlin) hat sich die TR RESISCAN in der Praxis längst bewährt:

> *„Die Kombination aus branchenspezifischer Verfahrensbeschreibung und BSI-RESISCAN-Zertifizierung sichert beim Ersetzenden Scannen ein Beweiswertmaximum, wie eine juristische Simulationsstudie nachgewiesen hat. Die Steuerberater haben mit ihrer Musterverfahrensbeschreibung einen Standard gesetzt, der anderen Branchen als Vorbild dient und die DATEV-Lösung motiviert hat."*

TR-ESOR

Die TR-ESOR beschreibt eine mögliche Referenzarchitektur eines Systems zur Beweis- und Informationserhaltung elektronischer Unterlagen mit daraus abgeleiteten Anforderungen auf Basis internationaler, europäischer und nationaler Standards.

Thematisch behandelt die Technische Richtlinie TR-ESOR dabei:

- Daten- und Dokumentenformate,
- Austauschformate für Archivdatenobjekte und Beweisdaten,
- Empfehlungen zu einer Referenzarchitektur, zu ihren Prozessen, Modulen und Schnittstellen als Konzept einer Middleware,
- zusätzliche Anforderungen für Bundesbehörden sowie
- Konformitätsregeln für die Konformitätsstufe 1 „funktionale Konformität", die Konformitätsstufe 2 „technische Konformität" und die Konformitätsstufe 3 „Konformität mit dem Deutschen Bundesbehörden-Profil".

Darüber hinaus können TR-ESOR-Produkte gemäß dem Common Criteria Protection Profile BSI-CC-PP-0049-2014 zertifiziert werden.

Aus den funktionalen Anforderungen für den Erhalt des Beweiswerts leitet die Technische Richtlinie TR-ESOR eine modulare Referenzarchitektur ab. Auf der Basis des vorliegenden Anforderungskatalogs können Anbieter und Produkthersteller zu dieser Richtlinie 03125 konforme Lösungsangebote entwickeln, die auf Basis der vorgenannten Konformitätsstufen zertifiziert werden können.

AUSBLICK

Insbesondere durch die für die öffentliche sowie für die gesetzlich verankerte Verpflichtung zur Einführung der eAkte rücken die Themen „ersetzendes Scannen" und „Langzeitspeicherung" noch stärker in den Fokus. Das Angebot zur Zertifizierung, das für beide Richtlinien besteht, wird nicht nur in der Wirtschaft, sondern zunehmend auch im öffentlichen Bereich wahrgenommen. Aktuell sind insgesamt neun BSI-Zertifizierungen nach TR-RESISCAN und vier nach TR-ESOR erfolgt, weitere Verfahren laufen.

Die sicherheitsrelevanten Module der eAkte werden fortlaufend aktualisiert, um auch den künftigen Herausforderungen der Digitalisierung Stand halten zu können. Derzeit wird die TR-RESISCAN mitsamt aller Anlagen überarbeitet. Die Aktualisierung berücksichtigt neben den gesetzlichen Änderungen auch die Resonanz aus der Praxis. Ab 2018 ist auch eine Überarbeitung der TR-ESOR geplant. ■

Weitere Informationen und Kontaktdaten:

TR-ESOR	TR-RESISCAN	ZERTIFIZIERUNG	
tresor@bsi.bund.de	resiscan@bsi.bund.de	zertifizierung-tr@bsi.bund.de	https://www.bsi.bund.de/TR

„Wir müssen handeln“

Interview mit Norbert Winkeljohann und Derk Fischer, PwC Deutschland

Die Angst vor Cyber-Attacken wächst. Wie verwundbar die digitale Gesellschaft ist und wie das IT-Sicherheitsgesetz (IT-SiG) den Wirtschaftsstandort Deutschland sicherer macht, darüber sprechen Norbert Winkeljohann, Sprecher der Geschäftsführung PwC Deutschland, und Derk Fischer, der den Bereich Cyber Security bei PwC Deutschland verantwortet.

Die Welt wird digitaler. Alles, was vernetzt werden kann, wird vernetzt. Wie verwundbar ist die digitale Gesellschaft?

Norbert Winkeljohann: Mit der fortschreitenden Digitalisierung und der zunehmenden Vernetzung steigen die Angriffsflächen für Hacker-Angriffe ebenso rasant wie die vielen technischen Möglichkeiten, von denen wir profitieren. Angreifer aus dem Netz verfügen über flexibel einsetzbare, hochleistungsfähige Mittel und sind untereinander gut vernetzt. So spähen sie Informationen aus, sabotieren Prozesse oder legen Produktionslinien lahm. Anlass zur Sorge geben dabei vor allem die Versuche, Einfluss auf demokratische Wahlen zu nehmen, wie in Frankreich und in den USA geschehen. Im Visier der Angreifer sind aber vor allem auch Industrieanlagen und IT-Systeme von Unternehmen. Durch erfolgreiche Attacken wird enormer Schaden verursacht. Das zeigt, wie verwundbar wir sind. Wir müssen also handeln.

Wie gut sind Unternehmen derzeit aufgestellt, um das Thema angemessen zu adressieren?

Norbert Winkeljohann: In großen Konzernen wird Cyber-Sicherheit von Aufsichtsgremien getrieben. Doch deutsche Familienunternehmen und Mittelständler sind oft schlechter gesichert. Dabei unterscheiden Angreifer nicht zwischen Großkonzernen und Mittelstand. Gleichzeitig setzen auch Mittelständler auf Digitalisierung: Sie transformieren ihre Prozesse, vernetzen sich mit Zulieferern, Geschäftspartnern und Kunden. Dadurch entstehen integrierte Prozessketten auf Basis hochkomplexer IT-Infrastrukturen, die völlig neue Herausforderungen an die Sicherheit stellen. Gleichzeitig werden die Methoden der Angreifer aggressiver, ausgefeilter und umfassender. Die Folge: Cyber-Angriffe nehmen zahlenmäßig zu mit stetig steigenden Erfolgsraten.

Hat der Mittelstand die Bedrohung denn nicht erkannt?

Derk Fischer: Im Mittelstand reagieren viele Firmen nur zögerlich mit konkreten Maßnahmen – trotz des massiven Anstiegs von Angriffen. Dennoch schätzen sich die Unternehmen in Bezug auf die eigene Sicherheit als gut oder sehr gut geschützt ein. Diese Selbsteinschätzung basiert aber oft auf einem tradierten Prozess- und IT-Verständnis der Entscheidungsträger, das aktuelle und drängende Themen der Digitalisierung nicht angemessen einbezieht. Damit klaffen Selbsteinschätzung und tatsächliche Bedrohungslage auseinander. Es besteht also kein grundsätzliches Erkenntnis-, sondern ein Umsetzungsproblem hinsichtlich der Transformationsherausforderungen.

Seit 2015 gilt das IT-Sicherheitsgesetz (IT-SiG). Zeigen sich erste Erfolge?

Norbert Winkeljohann: Es ist ein positiver Effekt eingetreten: Der Handlungsdrang für Betreiber sogenannter Kritischer Infrastrukturen (KRITIS) strahlt

Kurzprofil Norbert Winkeljohann und Derk Fischer

WP/StB Prof. Dr. Norbert Winkeljohann ist seit Juli 2010 Vorstandssprecher beziehungsweise Sprecher der Geschäftsführung von PwC Deutschland und Chairman von PwC Europe. Zudem ist er Mitglied im fünfköpfigen Executive Board des globalen PwC-Netzwerks.

Derk Fischer ist Partner im Bereich Risk Assurance Solutions. Er ist seit 26 Jahren in der IT-Sicherheitsberatung tätig, davon 17 Jahre bei PwC.

weit über die vom Gesetz erfassten Unternehmen hinaus. Denn auch Geschäftspartner müssen aufrüsten, wenn sie in Sachen Sicherheit auf dem gleichen Niveau sein wollen. Unternehmen erkennen mittlerweile selbst, dass ihnen dieser Druck guttut.

Derk Fischer: Das IT-SiG sorgt insgesamt dafür, dass Mindeststandards für Informationssicherheit eingehalten werden und trägt damit zu einer eklatanten Verbesserung der Informationssicherheit in Deutschland bei. Das darf uns aber nicht darüber hinwegtäuschen, dass es weiterhin Nachholbedarf gibt.

Wo genau sehen Sie Nachholbedarf?

Derk Fischer: Das Gesetz klammert explizit den öffentlichen Sektor aus. Die gesetzlichen Anforderungen an Vorkehrungen zur Vermeidung von Störungen sind im öffentlichen Sektor geringer als an Unternehmen. Infolgedessen hat die öffentliche Hand weniger in die Sicherheit investiert als beispielsweise Banken oder Versicherungen.

Und wie muss unsere IT-Sicherheitslandschaft erst aussehen, wenn Roboter den OP erobert haben?

Derk Fischer: Aktuell erleben wir einen Evolutionssprung, dessen Folgen wir noch nicht vollständig abschätzen können. Nicht nur in der Medizin werden neue selbstlernende Systeme eingesetzt. Ein weiteres Beispiel liefert die Automobilindustrie mit Modellreihen von TESLA, BMW, Mercedes oder Volkswagen. Autonomes Fahren ist dort weitgehend umgesetzt und wird nur noch durch fehlende rechtliche Rahmen ausgebremst. Für uns als Gesellschaft bedeutet das: Wir müssen uns damit auseinandersetzen, wie wir mit den dahinterstehenden überwiegend sehr persönlichen Daten umgehen. Wem gehören die Daten, wer darf sie unter welchen Voraussetzungen verwenden? Wie sind sie zu schützen? Das erfordert einen Balanceakt zwischen Nutzen und totaler Überwachung. Als Gesellschaft müssen wir uns über die Grundprinzipien eines Umgangs mit der neuen Datenwelt einig sein, da ist auch die Politik gefragt. Vor einem solchen Anspruch erscheinen Bedrohungen aus krimineller Motivation heraus fast zweitrangig, auch wenn wir davon ausgehen müssen, dass diese uns zukünftig noch viel mehr als bisher beschäftigen werden. ■

PricewaterhouseCoopers (PwC) ist eine Wirtschaftsprüfungs- und Beratungsgesellschaft mit Sitz in Frankfurt am Main. Im Auftrag des BSI hat PwC Mindestanforderungen für Cloud-Anbieter entwickelt, mit denen sich diese seit Januar 2016 prüfen lassen können.

Weitere Informationen: https://www.pwc.de/de/mittelstand/informationssicherheit-im-deutschen-mittelstand.html

„Ohne Kooperation geht es nicht.“

Interview mit Dr. Evi Haberberger, LKA Bayern

Im Bayerischen Landeskriminalamt wurde Anfang 2014 das Dezernat 54 – Cybercrime eingerichtet, um die Bayerische Polizei im Kampf gegen Internetkriminalität zu verstärken und ein Kompetenzzentrum aufzubauen. Das BSI-Magazin sprach mit Dr. Evi Haberberger, Sachgebietsleiterin der Zentralstelle Cybercrime im Dezernat 54.

Kurzprofil Dr. Evi Haberberger

Dr. Evi Haberberger wurde 1973 in Bayreuth geboren. Nach ihrem Studium der Diplom-Mathematik an der Universität Bayreuth promovierte sie dort 2002 im Bereich der Diskreten Mathematik. Von 2002 bis 2009 war sie Sachbearbeiterin für Kriminalanalyse auf der Dienststelle für Organisierte Kriminalität im Polizeipräsidium Oberfranken in Bayreuth und wechselte danach als Sachbearbeiterin Kriminalanalyse ins Bayerische Landeskriminalamt (BLKA). Seit 2014 ist sie Sachgebietsleiterin des SG 541 – Zentralstelle Cybercrime im BLKA.

Frau Dr. Haberberger, welche Ziele verfolgt das Landeskriminalamt Bayern mit dem Aufbau des Kompetenzcenters Cybercrime?

Hauptziel unserer Aktivitäten ist natürlich die direkte Bekämpfung von Cybercrime jeglicher Art. Aber auch die Vernetzung der Kollegen, die im Umfeld des sehr dynamischen Felds Cybercrime tätig sind, ist sehr wichtig, da ja die gesamte Polizei von dieser neuen Spielart der Kriminalität betroffen ist. Und wir wollen Expertise und Handlungssicherheit auf den verschiedensten Ebenen aufbauen: vom Beamten in der polizeilichen Ausbildung über Kolleginnen und Kollegen der Schutzpolizei bis hin zu Ermittlern im Phänomenbereich Cybercrime und zahlreichen anderen Deliktsfeldern wie beispielsweise Rauschgift, Waffen, Betrug, Staatsschutz. Daneben ist uns der Präventionsgedanke sehr wichtig und auch Führungskräfte müssen für die Thematik entsprechend sensibilisiert werden.

Wird die gesamte Cybercrime-Kompetenz der Bayerischen Polizei im Center konzentriert?

Nein. Neben dem Dezernat 54 im Bayerischen Landeskriminalamt existiert in jeder Kriminalpolizeiinspektion in Bayern ein Fachkommissariat zur Bekämpfung der Cyber-Kriminalität. Bayern geht darüber hinaus beim Personal der Bayerischen Polizei einen Sonderweg, indem zur Bekämpfung des Deliktsbereichs Cybercrime im Freistaat gezielt Informatiker eingestellt und im Rahmen einer einjährigen Ausbildung zu Vollzugsbeamten ausgebildet werden. Aktuell sind dies in Bayern etwa 50 Beamte. Im Lauf des Jahres 2017 werden rund 70 weitere Informatiker als IT-Kriminalisten eingestellt und in die Ausbildung gehen. Hierdurch wird die IT-Expertise in der Bayerischen Polizei flächendeckend maßgeblich erhöht, da die Zusammenarbeit von Informatikern und Kriminalpolizisten sehr gewinnbringend für beide Seiten ist.

Wie ist das Kompetenzcenter aufgebaut?

Es ist ein Dezernat mit derzeit etwa 50 Mitarbeitern und besteht aus drei Sachgebieten: der Zentralstelle Cybercrime, dem Sachgebiet Ermittlungen Cybercrime und dem Sachgebiet Netzwerkfahndung. Zu meinem Sachgebiet, Zentralstelle Cybercrime, zählt dabei auch die Zentrale Ansprechstelle Cybercrime (ZAC) für Behörden und Unternehmen.

Wurde das Kompetenzcenter komplett neu aufgebaut?

Nicht komplett. Den Nukleus bildete das Sachgebiet Netzwerkfahndung, ein Vorläufer-Sachgebiet, das sich sogar bereits seit 1995 mit Recherchen im Internet und der Ermittlungsunterstützung der bayerischen Polizeidienststellen beschäftigte. Ein Schwerpunkt lag dabei von Anfang an im Bereich der Recherche nach kinderpornografischem Material im Internet sowie der Unterstützung der Sachbearbeitung dieser Delikte. Die Aufgaben wurden jedoch sukzessive mehr und verbreiterten sich im Lauf der Jahre in verschiedene Deliktsfelder. Durch die allgegenwärtige Digitalisierung und zunehmende Nutzung digitaler Informations- und Kommunikationsmedien und -technologien wurde Cybercrime fast allgegenwärtig. Dadurch wurde auch in Bayern die personelle Aufstockung und Gründung des Dezernats notwendig.

„Gerade ein kontinuierlicher Austausch mit dem BSI ist entscheidend.“

Wie ist das Dezernat in das LKA eingebunden?

Das Dezernat ist in der Abteilung V – Zentrale Kriminalpolizeiliche Dienste verortet. Auf diese Weise wird der Schwerpunkt und hohe Stellenwert der Unterstützungsleistungen für die Dienststellen der Bayerischen Polizei als deren Zentralstelle zum Thema Cybercrime unterstrichen. Einen großen Raum nimmt dabei die Koordination von länderübergreifenden Großverfahren, die Beratung polizeilicher Sachbearbeiter, die Konzeptionierung und Durchführung von Aus- und Fortbildungsmaßnahmen für verschiedene Zielgruppen in der Bayerischen Polizei in Zusammenarbeit mit dem Fortbildungsinstitut der Bayerischen Polizei sowie der Austausch von Informationen mit Ermittlern und Dienststellen sowohl auf Landes- und Bundesebene als auch international ein. Und selbstverständlich werden im Kompetenzcenter auch herausragende Ermittlungsverfahren geführt, die uns durch das Bayerische Innenministerium oder durch die Staatsanwaltschaft zugewiesen werden. Dies kann der Fall sein, wenn beispielsweise eine kritische Infrastruktur oder eine Behörde von einer Cybercrime-Straftat betroffen ist.

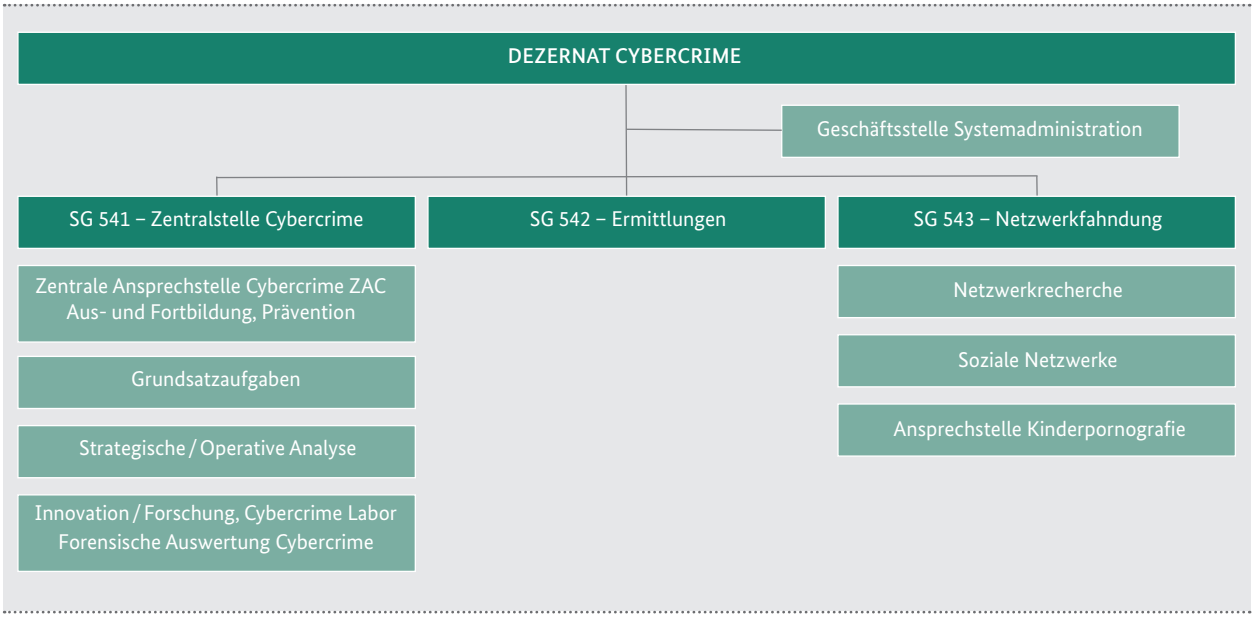
Wie findet denn dieser Informationsaustausch statt?

Nun, ein gutes Beispiel ist hier ein Informationsportal im Intranet der Bayerischen Polizei, auf welchem die wichtigsten Phänomene von Cybercrime ebenso wie aktuelle News, Ermittlungshilfen und Informationen zu Ansprechpartnern sowie Links zu geprüften externen Quellen enthalten sind.

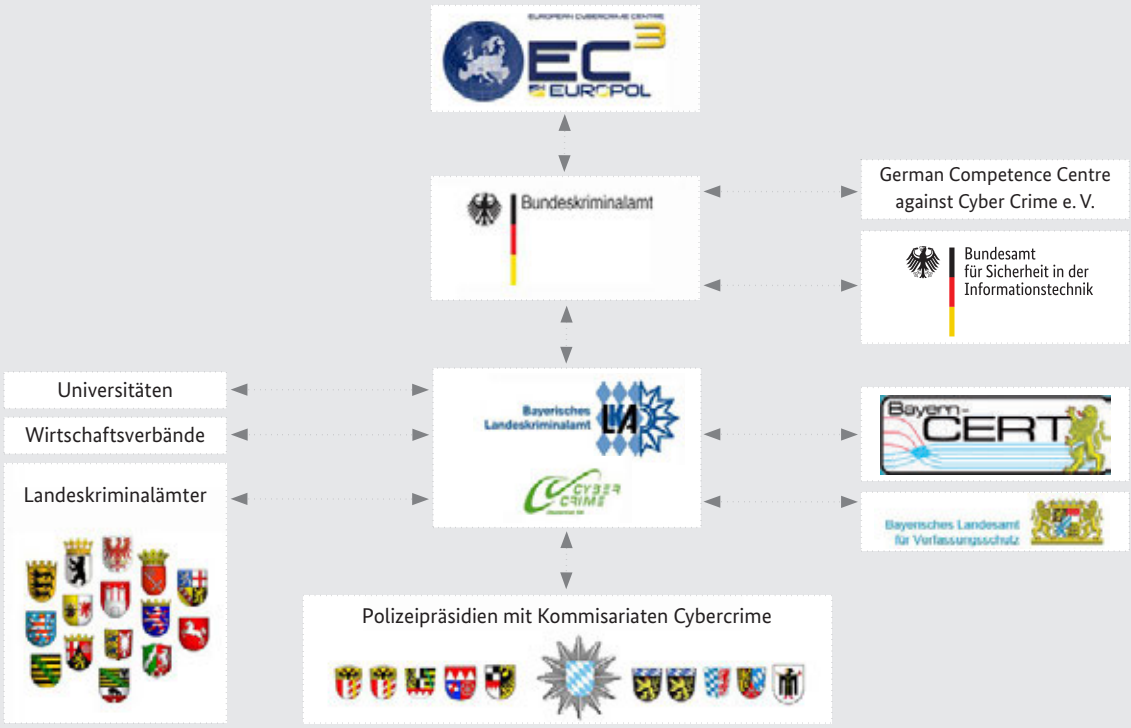
Sie haben die Kooperation auf Landes- und Bundesebene angesprochen. Können Sie dafür Beispiele nennen?

Ich möchte zunächst einmal generell betonen: Die Zusammenarbeit mit anderen Akteuren der Cyber-Sicherheit, allen voran mit dem BSI sowie dem gerade entstehenden Cyber-Cluster an der Universität der Bundeswehr in München, ist für uns ebenso wie für die deutsche Polizei insgesamt ausgesprochen wichtig.

Gerade ein kontinuierlicher Austausch mit dem BSI ist entscheidend. Einmal im Hinblick auf allgemeine technische Informationen, die als Quelle beispielsweise für Präventionstipps für die bayerischen Bürger und Unternehmen dienen



VERNETZUNG DES DEZERNATS 54



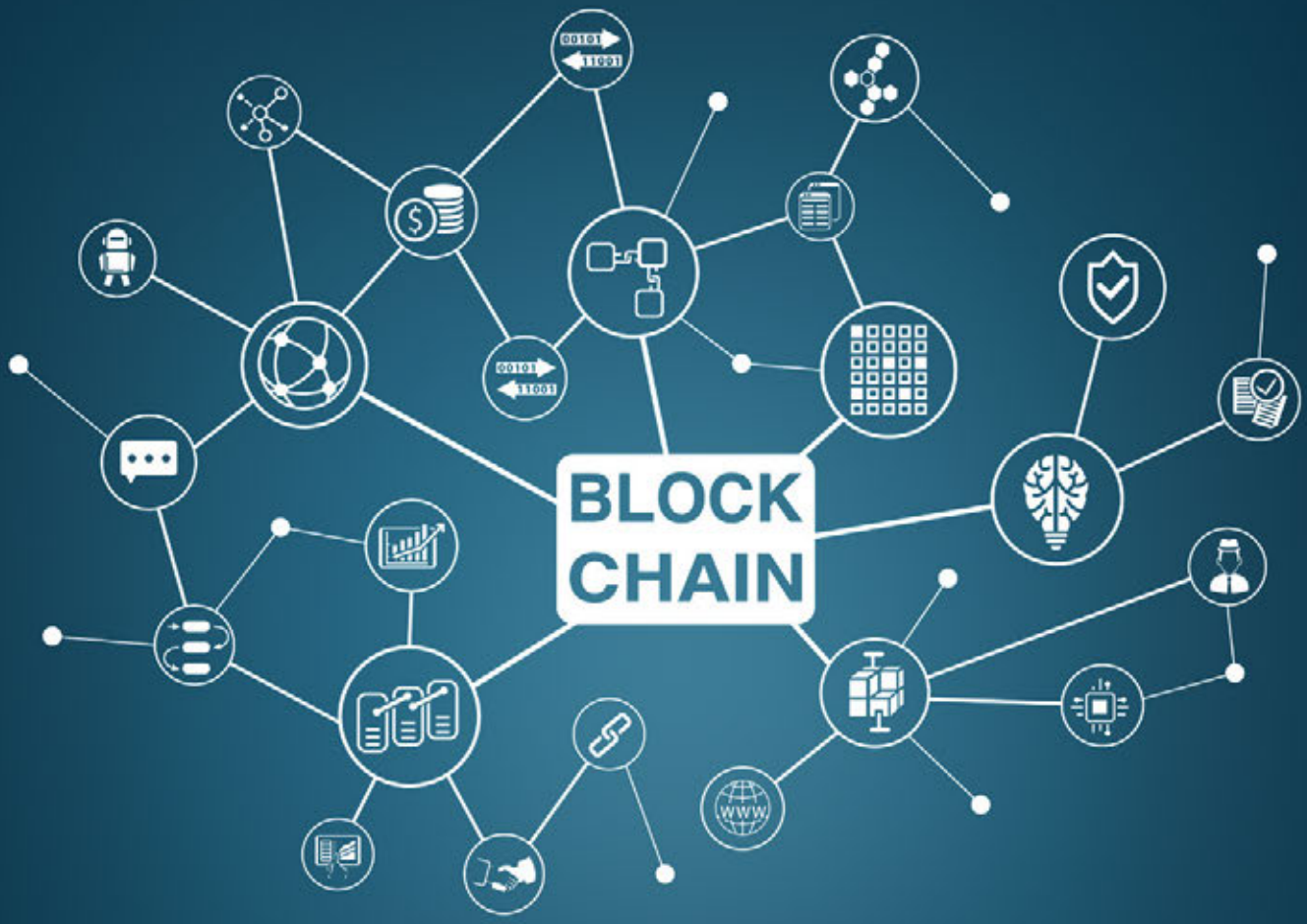
(Stichwort: BSI für Bürger). Aber auch im Hinblick auf den Schutz Kritischer Infrastrukturen als Kontaktstelle für unsere Zentrale Ansprechstelle Cybercrime, die bereits im Vorfeld möglicher Angriffe Kontakt mit Unternehmen aufnimmt, um im Schadensfall schnell agieren und Ermittlungen initiieren zu können.

Warum sind diese Kontakte und Routinen so wichtig?

Für den Gang von Ermittlungsverfahren ist es unerlässlich, möglichst schnell die Angriffsvektoren zu erkennen und Spuren zu sichern, damit Folgemaßnahmen zeitnah ergriffen werden können und die Recovery-Maßnahmen im betroffenen Unternehmen möglichst früh getroffen werden können, ohne zu viele Spuren der Straftäter zu vernichten. Hier ist die Reaktionsfähigkeit der Polizei gepaart mit fachlicher Kompetenz, ggf. ergänzt um Expertise des BSI, entscheidend für die Bekämpfung von Cyber-Angriffen. Zudem sind ressortübergreifende Kontakte notwendig, da häufig am Anfang eines Angriffs beispielsweise auf die Energieversorgung nicht erkennbar ist, ob es sich um „normale“ erpresserische Cybercrime-Straftaten, eine staatsgefährdende Straftat oder eventuell sogar um einen Angriff im staatlichen Auftrag handelt. Hier müssen Bekämpfungs- und Reaktionsstrategien und -mechanismen über die Zuständigkeitsgrenzen hinweg abgestimmt und gemeinsam entwickelt werden. Deshalb ist es für uns als ein Akteur in einem großen Netzwerk immens wichtig, dieses Netzwerk weiter auszubauen und zu pflegen, um einen bestmöglichen Schutz für unsere Bürger und die Unternehmen zu erreichen. Cyber-Sicherheit geht uns alle an und kann nur gemeinsam als gesamtstaatliche Aufgabe wahrgenommen werden. ■

Weitere Informationen: http://www.polizei.bayern.de/lka/kriminalitaet/internet/index.html

DIGITALE GESELLSCHAFT



POTENZIALE UND HERAUSFORDERUNGEN DER BLOCKCHAIN-TECHNOLOGIE

von Dr. Sarah Maßberg und Dr. Manfred Lochter, Kryptographische Vorgaben und Entwicklungen

Kryptografische Mechanismen schaffen Vertrauen

Bereits seit einigen Jahren stehen virtuelle Währungen wie Bitcoin im Fokus der Öffentlichkeit. Zunehmend gewinnt auch deren technologische Grundlage, die Distributed-Ledger-Technologie (DLT), an öffentlicher Aufmerksamkeit. Die im nachfolgenden Artikel behandelte Blockchain-Technologie ist eine spezielle Ausgestaltung der DLT, die der virtuellen Währung Bitcoin zugrunde liegt.

„Erpressung mit «Wanna Cry» - Bitcoin wird dem dubiosen Ruf gerecht", titelte im Mai 2017 die Neue Zürcher Zeitung, nachdem eine neue Ransomware-Welle weltweit Zehntausende von Computern erfasst hatte. Neben Jubelmeldungen über Kurshöchststände der Krypto-Währung Bitcoin mit 150 Prozent Zuwachs in der ersten Jahreshälfte 2017 sind es immer wieder Presseberichte über kriminelle Machenschaften im Bitcoin-System, die die öffentliche Wahrnehmung von Krypto-Währungen und der Blockchain-Technologie beeinflussen. Dabei liegen hier massive begriffliche Unschärfen vor, die mal zu einem undifferenzierten Lobgesang auf Blockchain und mal zu pauschaler Kritik an der neuen Technologie führen.

VERTRAUEN DURCH KRYPTOGRAFISCHE MECHANISMEN

Die Grundidee der Blockchain-Technologie basiert auf der Konstruktion der sogenannten Distributed-Ledger-Technologie (DLT).

WAS IST EIN DISTRIBUTED LEDGER?

Ein Distributed Ledger (englisch wörtlich für „verteiltes Kontobuch") ist ein öffentliches, dezentral geführtes Kontobuch. Es ist die technologische Grundlage virtueller Währungen und dient dazu, im digitalen Zahlungs- und Geschäftsverkehr Transaktionen von Nutzer zu Nutzer aufzuzeichnen, ohne dass es einer zentralen Administrationsstelle bedarf, die jede einzelne Transaktion legitimiert. Eine Blockchain ist ein spezielles Distributed Ledger, das zum Beispiel der virtuellen Währung Bitcoin zugrunde liegt.

Im Distributed Ledger werden die Daten nicht zentral, sondern verteilt, synchronisiert und konsensual vorgehalten. Ein Peer-to-Peer-Netzwerk und ein Konsensmechanismus garantieren eine valide Verteilung der Daten auf alle Netzwerkknoten. Bei der Blockchain-Technologie wird der verteilte Konsens durch eine sichere Verkettung von Datenblöcken realisiert.

Der konkrete Begriff „Blockchain" wurde erstmals als Bezeichnung für die Datenstruktur verwendet, die der Krypto-Währung Bitcoin zugrunde liegt. Er wird aber heute viel weiter gefasst. Allen Blockchain-Ansätzen gemeinsam ist dabei das neuartige Vertrauensmodell: Vertrauen in die Integrität und Sicherheit der Datenhaltung entsteht nicht aus dem Vertrauen auf eine zentrale Instanz, sondern basiert auf kryptografischen Mechanismen wie Hashfunktionen und Signaturen. Die Regeln des Systems sind intrinsisch durch sogenannten Chaincode (auch Smart Contracts genannt) codiert und werden automatisch ausgeführt.

VERSCHIEDENE ANWENDUNGEN

Aufbauend auf der Blockchain-Technologie können die verschiedensten Anwendungen realisiert werden. Blockchain ermöglicht beispielweise Automatisierungen in der Verwaltung von Versicherungsfällen durch Schadens- und Unfallversicherer, indem Schäden zeitnah auf der Basis historischer Fälle eingeschätzt werden. Im Finanzbereich gibt es Ansätze, den nachbörslichen Handel durch den Einsatz von Blockchains kostengünstiger und schneller zu gestalten. Außerdem bietet sich durch Blockchain die Möglichkeit, einem Großteil der Weltbevölkerung, der bisher keinen Zugang zu den klassischen Finanzsystemen hatte, eine Teilhabe an Handels- und Geschäftsprozessen zu ermöglichen (finanzielle Inklusion). Bei der Vergabe von Konsortialkrediten kann Blockchain die Bildung des Konsortiums und die Auszahlung des Geldes beschleunigen.

Auch die Energiewirtschaft zeigt ein gesteigertes Interesse an der neuen Technologie. So gibt es zum Beispiel im Bereich E-Mobilität viele denkbare Anwendungsmöglichkeiten wie die Abwicklung und Bezahlung von Ladevorgängen an Stromtankstellen über eine Blockchain. Im Energiehandel gibt es erste Ansätze für lokale Blockchain-Netzwerke, in denen auch kleine Energieerzeuger wie Privathaushalte mit einer Solaranlage auf dem Dach ihren Strom handeln können. Im Gesundheitssektor werden mögliche Anwendungen von der elektronischen Krankenakte über die digitale Krankenversicherung bis hin zur Arzneimittelsicherheit diskutiert.

Und auch staatliche Ansätze, die Blockchain-Technologie einzusetzen, gibt es bereits. So experimentieren verschiedene Länder (unter anderem Ghana und Schweden) mit Blockchain-basierten digitalen Grundbüchern. Die Verteilung von UN-Hilfsgeldern in Jordanien wird seit Kurzem testweise über eine Blockchain-Lösung realisiert. Und Estland als Vorreiter der Digitalisierung in Europa setzt die Blockchain-Technologie bereits in verschiedenen Bereichen wie dem e-Residency-

Programm, der transnationalen digitalen Staatsbürgerschaft oder bei der Verwaltung von Gesundheitsdaten ein.

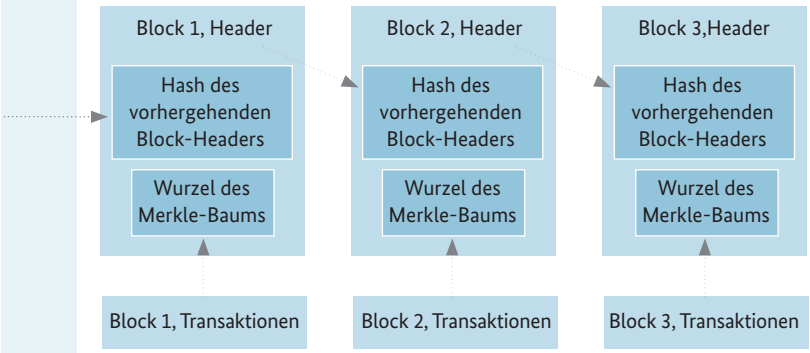
EIN PROMINENTES BEISPIEL: DIE KRYPTO-WÄHRUNG BITCOIN

Eine besonders prominente Anwendung der Blockchain-Technologie ist die Krypto-Währung, ein digitales Zahlungsmittel mit einem verteilten, dezentralen und kryptografisch abgesicherten Zahlungssystem. Und wiederum ein Spezialfall und das bislang in Bezug auf seine Verbreitung erfolgreichste Beispiel einer Krypto-Währung ist Bitcoin.

Transaktionen (Zahlungen mit Bitcoin) werden im Bitcoin-System mithilfe eines Public-Key-Verfahrens authentisiert. Dabei dienen kryptografische Schlüssel einerseits zur Adressierung von Zahlungsempfängern (öffentliche Schlüssel) und andererseits zur Signatur der Transaktionen durch die Absender (geheime Schlüssel).

Die Transaktionen werden im Bitcoin-Netzwerk verteilt und dann von sogenannten Minern zu neuen Blöcken zusammengefasst und an das Ende der Bitcoin-Blockchain angehängt. Dieses Anhängen (siehe Abbildung) ist mithilfe einer kryptografischen Hashfunktion gesichert. So wird die Integrität der gesamten Kette garantiert.

VEREINFACHTE BITCOIN-BLOCKCHAIN



Um einen Block hinzufügen zu können, muss eine rechenaufwendige Aufgabe (ein sogenanntes Krypto-Puzzle) gelöst werden. Wenn die Miner diese Aufgabe lösen und die Blockchain verlängern, werden sie in Form von Bitcoins belohnt und können zusätzlich Transaktionsgebühren erwarten. Dieses Verfahren – auch Proof-of-Work (PoW) oder Mining (also „Schürfen“) genannt – bildet den Konsensmechanismus im Bitcoin-System.

Ein gravierender Nachteil von Bitcoin ist der beschränkte Datendurchsatz im Bitcoin-Netzwerk und der aufgrund der erforderlichen Rechenleistung gleichzeitig enorm hohe Energieverbrauch des Minings. Er entspricht zurzeit ungefähr der gesamten Leistung eines konventionellen Kraftwerks.

Wenn auch die verwendeten kryptografischen Mechanismen heute als sicher gelten, stellt sich immer noch die Frage nach der Implementierungssicherheit. Dies betrifft die Bitcoin-Software und die Sicherheit von sogenannten Bitcoin Wallets („Geldbörsen“), in denen die kryptografischen Schlüssel verwaltet werden. Es sind Fälle bekannt geworden, in denen die Schlüsselerzeugung sehr schwach war und mithin Diebstähle erlaubte. Außerdem wirkt bei Bitcoin eine offene Entwicklercommunity mit, die schwer zu durchschauen und zu kontrollieren ist.

Oft wird behauptet, dass das Bitcoin-System Anonymität garantiert, da die Teilnehmer nur über einen kryptografischen Schlüssel (und damit eine zufällige Bitfolge) adressiert werden. Es ist aber schon gelungen, Inhaber von Bitcoins über die Sammlung und Analyse von Metadaten zu identifizieren. Andererseits zieht das Anonymitätsversprechen von Bitcoin Kriminalität geradezu magisch an. Bitcoin ist so – wie die letzten Erpressungsversuche mit Ransomware zeigen – zu einer beliebten Hackerwährung und zum Standardzahlungsmittel im Darknet geworden.

STANDARDISIERUNG BEGINNT

Um die neue Technologie in einen gewissen formellen Rahmen zu stellen, die Begrifflichkeiten festzulegen und die Grundlagen für regulatorische Maßnahmen zu schaffen, ist im April 2017 bei der internationalen Organisation für Normung (ISO) der TC 307 „Blockchain and Distributed Ledger Technologies“ unter der Leitung von Australien gegründet worden. Damit entsteht gerade der erste internationale Standard zum Thema Blockchain.

Daneben entwickeln sich durch Zusammenschlüsse der Industrie (wie beispielsweise R3-Konsortium, Hyperledger-Projekt) Quasi-Standards in den verschiedenen Wirtschaftszweigen, die die Entwicklung und den Einsatz von Blockchain maßgeblich beeinflussen. Außerdem haben sich viele Forschungsinstitute (zum Beispiel Fraunhofer-Gesellschaft) und Wirtschaftsverbände (zum Beispiel Bitkom und Teletrust) schon intensiv mit dem Thema befasst und entsprechende Papiere und Stellungnahmen veröffentlicht.

PROBLEME UND HERAUSFORDERUNGEN VON BLOCKCHAIN

Viele in der Praxis auftretende Probleme der Blockchain-Technologie sind noch nicht gelöst. Da die Sicherheit der Blockchain-Technologie zu großen Teilen kryptografisch fundiert ist, spielt die Auswahl und Umsetzung der eingesetzten kryptografischen Primitive und Protokolle eine große Rolle. Bereits beim Systemdesign muss die Langzeit-

WAS IST BITCOIN?

Bitcoin (englisch sinngemäß für „digitale Münze“) ist ein weltweit verwendbares dezentrales Zahlungssystem und der Name einer digitalen Geldeinheit. Das System wurde erstmals 2008 in einem unter dem Pseudonym Satoshi Nakamoto veröffentlichten White Paper beschrieben. Im Jahr darauf wurde eine Open-Source-Referenzsoftware dazu veröffentlicht. Nakamoto erzeugte auch den ersten Block (Genesisblock) der Bitcoin-Blockchain und damit die ersten 50 Bitcoins. Bis heute ist unklar, welche Person oder Personengruppe sich hinter diesem Namen verbirgt; die Bitcoins von Nakamoto sind bislang nicht benutzt worden.

sicherheit zum Beispiel in Form von Wechselmechanismen besonders berücksichtigt werden.

Auch die anderen bekannten Problemfelder der IT-Sicherheit wie Endpunktsicherheit, Netzwerksicherheit, Hardware- und Softwaresicherheit werden durch Blockchain keinesfalls gelöst, sondern sind gerade in verteilten, dezentralen Systemen eine große Herausforderung, die bisher noch nicht ausreichend Beachtung gefunden hat.

Große Unsicherheit besteht außerdem bei rechtlichen Fragen zum Einsatz von Blockchain. Die heute in Gesetzestexten verwendeten rechtlichen Begriffe passen oft nicht zu den technologischen Inhalten und müssen erst noch geeignet interpretiert werden. Gerade die fehlende zentrale Instanz kann hier zum Problem werden. Besonders beim Datenschutz gibt es noch Vorbehalte gegen die Blockchain-Technologie, da einige Grundprinzipien wie Datensparsamkeit oder das Recht auf Vergessenwerden der Konstruktion einer Blockchain zu widersprechen scheinen.

Auch die Möglichkeit, Teilnehmer transnational zu vernetzen, stellt eine Herausforderung dar. Für viele Blockchain-Anwendungen wird – auch oder gerade in einem dezentralen, verteilten System – ein gewisses Maß an international abgestimmter Steuerung und Regulierung notwendig sein. Wenn die Blockchain über Ländergrenzen hinweg betrieben wird, bleibt die Frage zunächst offen, wer für diese Regulierung und die entsprechende Durchsetzung verantwortlich sein soll.

GESTALTUNG ERFORDERLICH

Oft wird heute von einem Blockchain-Hype gesprochen, wenn über große wirtschaftliche und organisatorische Vorteile der Blockchain-Technologie gesprochen wird. Unabhängig davon, ob Blockchain überbewertet wird oder nicht, ist davon auszugehen, dass eine Reihe von Anwendungen weite Verbreitung erlangen wird.

Gerade in Einsatzbereichen, in denen eine intransparente zentrale Instanz vermieden werden soll oder digitale Infrastrukturen bisher unzureichend umgesetzt sind, bietet die Blockchain großes Potenzial. Auch in staatlichen Anwendungen könnte der Einsatz der Blockchain-Technologie die Transparenz und Zusammenarbeit staatlicher Stellen befördern.

Das BSI als Gestalter der IT-Sicherheit in Deutschland setzt sich vor dem Hintergrund möglicher Anwendungen in staatlichen oder Kritischen Infrastrukturen und angesichts der Bedrohungen durch kriminelle Machenschaften in Blockchain-Netzwerken intensiv mit den Sicherheitsaspekten von Blockchain auseinander.

Um die Chancen der Blockchain-Technologie gewinnbringend nutzen und die Risiken kontrollieren zu können, sind in jedem Fall weitere Anstrengungen im Bereich der Standardisierung und Regulierung notwendig, damit das Vertrauensmodell der Blockchain den Anforderungen rechtssicherer realer Anwendungen standhalten kann. Außerdem ist für alle Anwendungen die Verwendung starker Kryptografie und sicherer Protokolle sicherzustellen. Dies gilt vor allem für Anwendungen, die vertrauliche (etwa personenbezogene) Daten in einer Blockchain ablegen. Hier ist die Vertraulichkeit und Integrität der Daten langfristig kryptografisch sicherzustellen. Langzeitsicherheit ist ein durchaus anspruchsvolles Ziel, wenn man bedenkt, dass gleichzeitig potenzielle Quantencomputer diskutiert werden (siehe BSI-Magazin 2017/01), die Teile der heute verwendeten Kryptografie gefährden. ■

Weitere Informationen zu Bitcoin im IT-Grundschutz: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/Benutzerdefinierte_BS/BS_Bitcoin.html?nn=7712584

Kurzprofil Dr. Magnus Harlander

Dr. Magnus Harlander ist als technischer Geschäftsführer der genua gmbh verantwortlich für die Entwicklung der Sicherheitslösungen sowie die Zertifizierung der hochwertigen Produkte in Zusammenarbeit mit dem BSI. Die Firma genua mit Sitz in Kirchheim bei München gründete der Diplom-Physiker 1992 zusammen mit zwei weiteren IT-Security-Spezialisten.

„Einen entscheidenden Spin für unsere Produktentwicklung brachte die Beteiligung an einem Forschungsprojekt zu hochperformanten Firewalls, das vom BSI gefördert wurde."

25 Jahre genua

von Dr. Magnus Harlander, Geschäftsführer genua gmbh

Partnerschaftliche Zusammenarbeit mit dem BSI

Die Firma genua feiert in diesem Jahr ihr 25-jähriges Firmenjubiläum. Seit der Gründung 1992 ist in der IT-Sicherheit viel passiert: Kannte man anfangs die kursierenden Viren wie ‚Michelangelo' oder ‚I Love You' noch mit Namen, werden heute täglich über 390.000 neue Schadprogramme im Internet registriert. Waren Hacker früher großteils verspielte Nerds, sind es aktuell meistens Mitglieder professioneller Organisationen. Auch in der Branche gab es immer wieder Hochs und Hypes, aber auch Tiefs und platzende Blasen. In diesen 25 Jahren rasanter Entwicklung hat sich genua vom Spin-off dreier Physiker der TU München zu einem wichtigen Hersteller für hochwertige IT-Sicherheit in Deutschland entwickelt. Das BSI, gegründet 1991 und somit nahezu gleich alt, war in diesen Jahren ein ständiger Wegbegleiter. Da sowohl das BSI als auch genua das Ziel verfolgen, die IT-Sicherheit in Deutschland voranzutreiben, haben hier zwei Partner zu einer konstruktiven Zusammenarbeit zusammengefunden.

Ein ganz wichtiger Schritt war für genua die Zertifizierung der Firewall genugate durch das BSI im März 2002 nach dem Standard ITSEC. Die genugate war die erste Firewall, die ein BSI-Zertifikat erhalten hat. Der gesamte Prozess, der bereits 1998 begonnen hatte, mündete in einem Zertifikat, das unabhängig das hohe Sicherheitsniveau der Lösung bescheinigte.

BSI-ZERTIFIKAT ÖFFNET TÜREN

Für genua war die BSI-Zertifizierung der Türöffner zu Firewall-Projekten im Hochsicherheitsbereich. So konnten wir bereits 2002 die Ausschreibung zur Absicherung des großen Regierungsnetzes IVBB gewinnen, da genugate nachweislich sowohl die hohen Funktions- als auch Sicherheitsanforderungen erfüllte. In diesem zentralen Netzwerk ist die genugate immer noch im Einsatz – Stand heute ohne einen einzigen Ausfall. Die BSI-Zertifizierung hält also, was sie verspricht.

Zahlreiche weitere Firewall-Projekte im Behörden- und Industriebereich folgten. Neue Versionen der genugate haben wir regelmäßig beim BSI nach dem heute gängigen Common-Criteria-Verfahren rezertifizieren lassen.

Auch bei der Zulassung von IT-Sicherheitslösungen zur Bearbeitung von eingestuften Daten arbeiten wir regelmäßig mit dem BSI zusammen. Zuletzt haben wir im April 2017 für das Security Laptop vs-top die Zulassung für die Geheimhaltungsstufe VS-NfD erhalten. Mit dieser anwenderfreundlichen Lösung können mobile Mitarbeiter sicher an eingestufte Netzwerke angebunden werden.

Hier sei aber auch angemerkt: Das Zulassungsverfahren für das Security Laptop, das auf der Microkernel-Technologie basiert, hat rund zweieinhalb Jahre gedauert. Sowohl im Interesse der Hersteller als auch der Anwender sollten die Verfahren beschleunigt werden, um sicherzustellen, dass dieser Markt mit einer Auswahl an aktuellen Lösungen beliefert werden kann. An den Gesprächen zur Beschleunigung der Zulassungs- und auch Zertifizierungsverfahren beim BSI haben wir intensiv mitgewirkt, hier wurden aus unserer Sicht gute Ergebnisse erzielt.

IMPULSE FÜR DIE PRODUKTENTWICKLUNG

Vom BSI kamen immer wieder wichtige Impulse für die Produktentwicklung. So sind wir bei der Konzeption der zweistufigen Firewall genugate der BSI-Empfehlung gefolgt, dass an kritischen Schnittstellen dreistufige Sicherheitssysteme eingesetzt werden sollen. Die genugate besteht aus einer Kombination von Application Level Gateway und Paketfilter und bietet somit bereits zwei Stufen. Fügt man hier eine weitere Firewall hinzu, wird die empfohlene Lösung erreicht. Die Zweistufigkeit ist ein zentrales Sicherheitsmerkmal und damit für den Einsatz im Hochsicherheitsbereich prädestiniert.

Auch bei der Entwicklung des Personal Security Devices genucard zur sicheren Anbindung von mobilen Mitarbeitern und Home-Offices haben wir Vorgaben des BSI umgesetzt: Das kompakte Device ist im BOS-Bereich in großen Stückzahlen im Einsatz und ermöglicht unter anderem der Bundeswehr die Einrichtung von abgesicherten Heimarbeitsplätzen.

Einen entscheidenden Spin für unsere Produktentwicklung brachte die Beteiligung an einem Forschungsprojekt zu hochperformanten Firewalls, das vom BSI gefördert wurde. Hier haben wir uns mit der Microkernel-Technologie beschäftigt und deren Vorteile erkannt: Das minimalistische Betriebssystem ist eine flexible Plattform zur Entwicklung von Lösungen, die höchste Sicherheitsanforderungen erfüllen. Unsere ersten Produkte mit dieser Technologie sind Security Laptops für mobile Anwender im VS-Bereich und Datendioden zum Monitoring von Kritischen Infrastrukturen.

Zusammenfassend kann man sicherlich sagen, dass das BSI einen Anteil an der erfolgreichen Entwicklung von genua hat. Diese gute Zusammenarbeit möchten wir gerne fortsetzen und wünschen uns, dass das BSI weiterhin der Branche wichtige Impulse liefert, anspruchsvolle Sicherheitsstandards vorgibt und in allen kritischen Bereichen durchsetzt. Hersteller sollen die vorgegebenen Standards in Produkte umsetzen und die Möglichkeit haben, durch geeignete Zulassungs- und Zertifizierungsverfahren die Qualität ihrer Lösungen unter Beweis zu stellen. So können wir die IT-Sicherheit auch in den nächsten 25 Jahren weiter gemeinsam vorantreiben. ■

Weitere Informationen: https://www.genua.de

SMART UND SICHER

von Hanna Heuer, Cyber-Sicherheit für den Bürger und Öffentlichkeitsarbeit, und Florian Schumacher, Cyber-Sicherheit für die Gesellschaft

Projekt „Digitale Gesellschaft" auf der Zielgeraden

„Digitale Gesellschaft: smart & sicher" (SuSi). Unter diesem Motto erarbeiteten Vertreterinnen und Vertreter aus zivilgesellschaftlichen Organisationen, aber auch aus Wirtschaft und Verwaltung, Wissenschaft und Kultur gemeinsam mit dem BSI Impulse für eine sichere Informationsgesellschaft.

Während der Denkwerkstatt wurden Thesen zur sicheren Informationsgesellschaft formuliert

Die Vorbildfunktion des Staates im Bereich der IT-Sicherheit hervorheben, rechtlich verpflichtende Standards nach den Prinzipien security und privacy by design und by default für alle IT-Produkte etablieren, eine intensive Auseinandersetzung mit dem Thema Haftung im Bereich der IT-Sicherheit anregen und einen entsprechenden organisatorischen Rahmen hierzu schaffen: Unter anderem darum geht es im Projekt „Digitale Gesellschaft: smart & sicher". Sein Ziel ist es, das Thema Cyber-Sicherheit in der Gesellschaft mit einem breiten Spektrum an Akteuren gemeinsam zu diskutieren, Handlungsbedarfe zu identifizieren und Lösungsvorschläge zu erarbeiten.

DENKWERKSTATT SICHERE INFORMATIONSGESELLSCHAFT

Der inoffizielle Startschuss des Projektes war die vom BSI im April 2016 durchgeführte Denkwerkstatt „Sichere Informationsgesellschaft" (siehe BSI-Magazin 2016/02). Die dort im Konsens formulierten sieben Thesen für eine sichere Informationsgesellschaft, vor allem aber auch die vieldiskutierten Fragen, zu denen keine Einigung erzielt werden konnte – beispielsweise zur Sicherheitskultur oder der Rolle der Informationssicherheit bei der Digitalisierung –, stärkten das BSI in seiner Absicht, den Dialog mit unterschiedlichen Akteuren zu vertiefen.

Im Herbst 2016 wurde daher entschieden, mit dem Projekt „Digitale Gesellschaft: smart & sicher" (Susi) die Diskussionen im bewährten Format der Denkwerkstatt fortzusetzen und sie durch sozialwissenschaftliche Untersuchungen zu begleiten. Ein Konsortium aus dem nexus Institut und dem Digitale Gesellschaft e. V. zusammen mit der ipsos GmbH und Dr. Ben Wagner als Unterauftragnehmer führt im Auftrag des BSI das Projekt bis Februar 2018 durch.

GEMEINSAME DISKUSSIONEN UND ANALYSEN

Im Februar 2017 erarbeiteten 30 Teilnehmerinnen und Teilnehmer einer zweiten Denkwerkstatt Fragestellungen zu den Aspekten „Sicherheit und Technologie", „Vertrauen" und „Verantwortung" in der digitalen Gesellschaft. Diese flossen in unterschiedliche empirische Erhebungen ein: Mittels einer repräsentativen Onlinebefragung wurde erhoben, wie die Bevölkerung zu unterschiedlichen Aspekten der Digitalisierung steht und welchen Stellenwert IT-Sicherheit hierbei hat. Darüber hinaus beteiligten sich 20 Bürgerinnen und Bürger an einer Online-Community, über die qualitative Einschätzungen eingeholt wurden.

Eine weitere Perspektive auf die digitale Gesellschaft und die Rolle unterschiedlicher Akteure in dieser eröffneten Interviews des Projektteams mit Experten aus Zivilgesellschaft und Wissenschaft. Erste hieraus gewonnene Ergebnisse konnten den Teilnehmerinnen und Teilnehmern einer weiteren Denkwerkstatt im Juni 2017 präsentiert werden. Auch sie gingen mit in die weiteren Diskussionen ein. Am Ende dieser Denkwerkstatt stand das gemeinsam entwickelte und von den Akteuren mitgetragene „Impulspapier Sichere Informationsgesellschaft".

Im Beisein von BSI-Präsident Arne Schönbohm stellten die am Prozess Beteiligten diese Impulse am 7. September 2017 in Berlin der Öffentlichkeit vor. Die anschließende Podiumsdiskussion zwischen Vertretern des Bundesministeriums des Innern, der Verbraucherzentrale NRW, Amnesty International und des Bitkom unter dem Titel „Sicherheit in der digitalen Gesellschaft" ging insbesondere auf die Frage der Kennzeichnung sicherer Produkte und der Haftung ein. In einem Punkt waren sich alle am Projekt beteiligten Akteure einig: Der mit dem Projekt „Digitale Gesellschaft: smart & sicher" (SuSi) und der Veranstaltungsreihe Denkwerkstatt Sichere Informationsgesellschaft begonnene Dialog soll fortgesetzt und vertieft werden. Das erarbeitete Impulspapier soll hierfür als gemeinsame Grundlage dienen. ■

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

Drei Sekunden für mehr E-Mail-Sicherheit

BSI-Basistipp

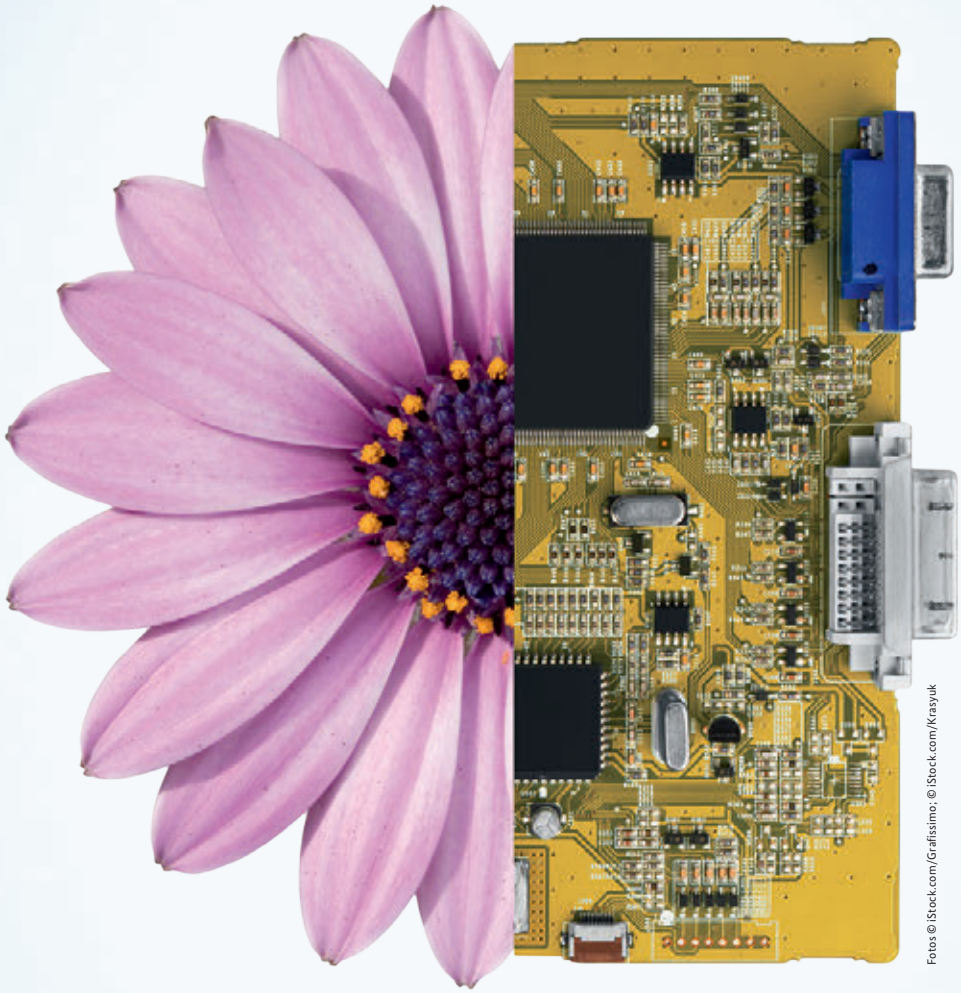
Nach wie vor einer der häufigsten Wege, Schadsoftware auf Computer einzuschleusen, sind verseuchte E-Mail-Anhänge oder Verlinkungen auf schadhafte Webseiten in der E-Mail: Öffnen Empfänger ihre elektronische Post zu unbedacht, ist der Rechner schnell infiziert. Die Auswirkungen reichen vom Befall einzelner Rechner über den Ausfall von Teilen der IT-Infrastruktur bis hin zum Verlust von wichtigen Daten.

ACHTEN SIE BEI E-MAILS ZUDEM AUF FOLGENDE PUNKTE:

- Betreff und E-Mail-Text sollten stimmig und plausibel sein
- Spam-Mails enthalten immer öfter eine korrekte Ansprache und weitere persönliche Daten
- E-Mails von bekannten Unternehmen werden oft täuschend echt nachgestellt
- Vage Formulierungen wie der Betreff „Rechnung“ oder „Mahnung“ sind ein Indiz für Spam-Mails
- Gehen Sie der Aufforderung, Links oder Dateien zu öffnen, nicht nach
- Persönliche Informationen sollten nicht auf in E-Mails verlinkten Webseiten eingegeben werden

Weitere Informationen:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Menschenverstand/E-Mail/E-Mail_node.html

Was wir wollen: Deine digitale Seite



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

Bundesamt
für Sicherheit in der
Informationstechnik

Informationstechnik ist die Grundlage des modernen Lebens. Umso wichtiger ist es, dass die Menschen der digitalen Welt vertrauen können. Darum kümmern wir uns. Als nationale Behörde für Cyber-Sicherheit gestalten wir IT-Sicherheit in Deutschland – aber auch in Europa und der Welt. Dazu arbeiten wir mit Wirtschaft und Wissenschaft zusammen. Wir beraten Politik und Verwaltung und stehen im Dialog mit den Bürgern sowie zahlreichen Verbänden. Im internationalen Austausch sind unsere Experten geschätzt und gefragt. Alles für ein gemeinsames Ziel: Informationssicherheit. Wir sorgen dafür, dass die Zukunft aus dem Netz erwachsen kann. Mit rund 720 Mitarbeitern sind wir ein vergleichsweise kleines Team für eine große Aufgabe. Und deshalb brauchen wir Verstärkung.

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

IMPRESSUM

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI) 53175 Bonn
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Referat B23 – Cyber-Sicherheit für den Bürger und Öffentlichkeitsarbeit Godesberger Allee 185–189 53175 Bonn Telefon: +49 (0) 228 999582-0 E-Mail: bsi-magazin@bsi.bund.de Internet: www.bsi.bund.de
Stand:	September 2017
Texte und Redaktion:	Stephan Kohzer und Nora Basting, Bundesamt für Sicherheit in der Informationstechnik (BSI); Joachim Gutmann, GLC Glücksburg Consulting AG; Fink & Fuchs AG
Konzept, Redaktion und Gestaltung:	Fink & Fuchs AG, Berliner Straße 164 65205 Wiesbaden Internet: www.finkfuchs.de
Druck:	Druck- und Verlagshaus Zarbock GmbH & Co KG Sontraer Str. 6 60386 Frankfurt a.M. Internet: www.zarbock.de
Artikelnummer:	BSI-Mag 17/706-2
Bildnachweise:	Titel: Smileus/fotolia (o.l.), Gorodenkoff/fotolia (o.r.), Kasto/fotolia (m.l.), BSI (m.m.), william87/fotolia (u.l.), Pressmaster/fotolia (u.m.), Kiri/fotolia (u.r.), zapp2photo/fotolia (Hintergrund); S. 2: Stephan Kohzer/BSI; S. 4: Henning Schacht (o.l.), Henning Schacht (u.l.), ECSM (u.r.); S. 5: NürnbergMesse it-sa (o.l.), NürnbergMesse (o.m.), NürnbergMesse (o.r.), Geza Aschoff (u.l.); S. 6: R. Winkler; S. 8: BSI; S. 9: Bundesregierung/Güngör (o.); BSI (m.l.); BSI (m.r.), BSI (u.l.), BSI (u.r.); S. 10: Wikipedia/BSI; S. 12: Bundespolizei; S. 13: Bundespolizeidirektion Flughafen Frankfurt/Main (o.l.), Bundespolizeidirektion Flughafen Frankfurt/Main (o.r.); S. 14: Fink & Fuchs AG (o.l.); S. 15: Fink & Fuchs AG (alle Bilder); S. 17: BSI (o.l.), BSI (o.r.); S.18: R. Winkler (o.), BSI (u.); S. 19: R. Winkler; S. 20 BSI; S. 21: BSI; S. 22: BSI; S. 24: BSI; S. 25: 1. Reihe von links nach rechts: Antonioguillem/fotolia, Bernardbodo/fotolia, Sepy/fotolia, miklyxa/fotolia, 2. Reihe von links nach rechts: industrieblick/fotolia, Kadmy/fotolia, Georgerudy/fotolia, Antonioguillem/fotolia; S. 26: Joachim Gutmann; S. 28: Fink & Fuchs AG; S. 29: BSI; S. 31: Henning Schacht; S. 32 – 33: Fink & Fuchs AG; S. 35: BSI (alle Bilder); S. 36: BSI; S. 38: Foto Klein; S. 39: Foto Klein (o.), Foto Klein (m.); S. 40: Peshkova/fotolia (Hintergrund), Geza Aschoff (Bildschirm); S. 43: BSI; S. 44: BillionPhotos.com/fotolia; S. 45: BSI; S. 47: PwC Deutschland (alle Bilder); S. 48: travelview/fotolia; S. 49: Bayerisches Landeskriminalamt; S. 50: BSI; S. 51: BLKA; S. 52: Iconimage/fotolia; S. 54: BSI; S. 55: Pickup/fotolia; S. 56: genua gmbh; S. 58: BSI; S. 59: BSI; S. 60: Fink & Fuchs AG, Foto Can Yesil/fotolia; S. 61: Fink & Fuchs AG, Fotos: iStock.com/Grafissimo, iStock.com/Krasyuk

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

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

www.bsi.bund.de