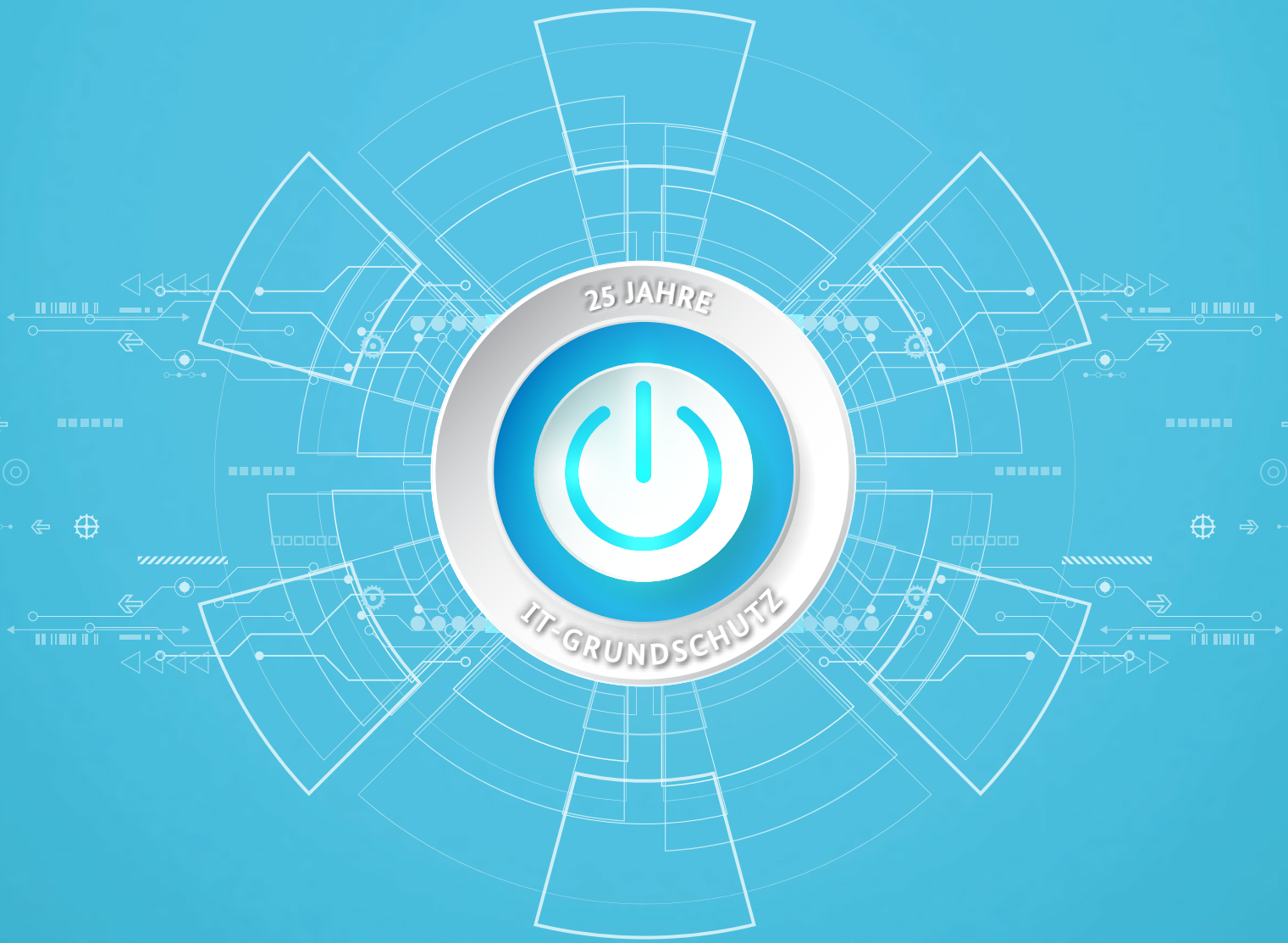
Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Magazin 2019/02

Mit Sicherheit

IT-Grundschutz als Fundament für Informationssicherheit



CYBER-SICHERHEIT

Die fünfte Generation – 5G und die Folgen

SONDERTHEMA

Konstante in der Informationssicherheit – 25 Jahre IT-Grundschutz

DIGITALE GESELLSCHAFT

Cyber-Sicherheit für die Digitalisierung der Energiewirtschaft

EDITORIAL

Valide, sicher, wertvoll

„IT-Sicherheitskonzepte und -maßnahmen sind nicht ‚nice-to-have', sie sind ein ‚must-have'."

Cyber-Angriffe mit den Schadprogrammen WannaCry und NotPetya haben 2017 weltweit Millionenschäden verursacht und einzelne Unternehmen in Existenznöte gebracht. Mitte 2019 wurde in der Funktion zur Fernverwaltung von Microsoft Windows die kritische Schwachstelle Bluekeep entdeckt. Das derzeit über Spam-Kampagnen verteilte Schadprogramm Emotet gilt als eine der größten Bedrohungen durch Schadsoftware weltweit und verursacht auch in Deutschland aktuell hohe Schäden.

Drei Beispiele, die zeigen, dass Informationssicherheit heute und in Zukunft zum entscheidenden Kriterium wird, damit in einer digitalisierten Gesellschaft Abläufe und Prozesse in Behörden und Verwaltungen, in großen wie kleinen Unternehmen, aber auch beim Privatanwender reibungslos und vor allem störungsfrei ablaufen können.

Um das Risiko eines Cyber-Angriffs zu minimieren, muss jede Institution daher ein individuelles und auf ihre Anforderungen abgestimmtes IT-Sicherheitskonzept erstellen, umsetzen und stetig überprüfen. Mit dem IT-Grundschutz bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) dafür ein seit 25 Jahren bewährtes Instrument: Eine modulare und flexible Methodik, um Informationen abzusichern und ein Managementsystem für Informationssicherheit (ISMS) aufzubauen.

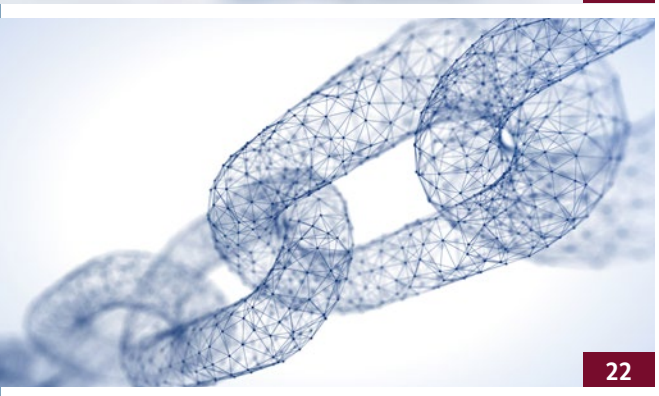
Beides dient natürlich dem Schutz. Aber schon heute ist ein IT-Sicherheitskonzept mehr. Neben Nachhaltigkeit, Diversität und Transparenz ist es ein weiteres wertvolles Qualitätsmerkmal, mit dem Behörden und Unternehmen sich auszeichnen und valide Nachweise gegenüber ihren Kunden, Dienstleistern, aber auch den eigenen Mitarbeitern erbringen können, dass der Schutz von Daten und Informationen auf ihrer Agenda ganz oben steht.

Denn da gehört er hin. Ohne Informationssicherheit kann die Digitalisierung in Verwaltung und Wirtschaft nicht erfolgreich vorangetrieben werden. IT-Sicherheitskonzepte und -maßnahmen sind nicht „nice-to-have", sie sind ein „must-have". Und damit dessen Aktualität, Validität und Vollständigkeit einfach nachprüfbar ist, müssen diese Konzepte zertifiziert sein. So wie das Umweltsiegel für Umweltfreundlichkeit und die TÜV-Plakette für verkehrssichere Fahrzeuge steht, belegt ein ISO 27001-Zertifikat auf der Basis des IT-Grundschutzes den Stellenwert der Informationssicherheit in dieser Institution.

Als Gesellschaft wie als Einzelner erfahren und lernen wir tagtäglich, welch immense Bedeutung Cyber-Sicherheit für das Zeitalter der Digitalisierung hat. Als es zu Beginn der Industrialisierung mit zunehmender Anzahl und Leistungsfähigkeit der Dampfmaschinen immer mehr Unfälle durch explodierende Dampfkessel gab, gründeten zwanzig badische Kesselbesitzer im Januar 1866 die „Gesellschaft zur Überwachung und Versicherung von Dampfkesseln" mit dem Ziel einer freiwilligen Qualitätskontrolle. Es war die Urzelle des heutigen TÜV. Und so sehe ich heute den IT-Grundschutz: Als Vorläufer und Vorreiter eines umfassenden und standardisierten, auf Freiwilligkeit basierenden Systems der IT-Sicherheit. Wir haben viel erreicht, aber wir haben noch mehr zu tun.

Ihr

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik



INHALT

AKTUELLES

KRITIS

Cyber-Angriff auf Krankenhäuser

Im Juli kam es zu einem Cyber-Angriff auf 16 Einrichtungen der DRK-Trägergesellschaft Süd-West, darunter Krankenhäuser und Pflegeeinrichtungen. Die Täter haben Schadsoftware aufgespielt und Daten verschlüsselt. Das Ziel: Geld gegen Daten. Zeitweise wurden die Notaufnahmen mit Stift und Zettel betrieben. Das sachkundige IT-Team vor Ort konnte zügig reagieren, brauchte aber Unterstützung. BSI und Klinikverbund standen sofort im engen Austausch. Kurz danach fuhr ein mobiles Einsatzteam des BSI nach Rheinland-Pfalz. Der Angriff wurde abgewehrt und weitere Attacken verhindert. Der Präsident des BSI, Arne Schönbohm, betont: „Krankenhäuser gehören schon lange zum KRITIS-Bereich. Unser Team aus Experten kann deutschlandweit bei Notfällen helfen. Mit einem auf Krankenhäuser zugeschnittenen IT-Grundschutzprofil werden wir sie stark machen gegen Netzangriffe."

Weitere Informationen: https://bsi.bund.de/kritis

Cloud-Security

Community-Draft des revisionierten C5

Der 2016 vom BSI veröffentlichte Cloud Computing Compliance Criteria Catalogue (kurz: C5) wird zur Zeit überarbeitet. Zur it-sa 2019 veröffentlichte das BSI ein Community-Draft des überarbeiteten C5 und stellte diese Version auf der Messe vor. In die Überarbeitung flossen die Erfahrungen von Cloud-Nutzern, -Anbietern und -Prüfern ein. Kernpunkte der Überarbeitung sind unter anderem die neue Domäne Produktsicherheit (womit die Regelungen des EU Cyber Security Acts adressiert werden) und die Berücksichtigung von DevOps. Konstruktive Kritik und Ergänzungen werden vom Cloud-Security-Team des BSI noch bis Ende November berücksichtigt (Kontakt: cloudsecurity@bsi.bund.de). Der endgültige neue C5 wird Ende Januar 2020 veröffentlicht.

Weitere Informationen: https://bsi.bund.de/Cloud

Allianz für Cybersicherheit

Initiativen erarbeiten Hilfestellungen für mehr Cyber-Sicherheit

Bei einem Cyber-Angriff stehen Organisationen häufig vor der Herausforderung, die Auswirkungen des Vorfalls zu minimieren und gleichzeitig möglichst schnell zum Tagesgeschäft zurückkehren zu müssen. Hilfestellungen für diese Aufgabe – insbesondere, aber nicht nur im Umfeld von KMU – haben Arbeitsgruppen innerhalb des Dialogs der Cyber-Sicherheits-Initiativen in den vergangenen Monaten erarbeitet. Die Ergebnisse werden unter anderem auf www.allianz-fuer-cybersicherheit.de zur Verfügung gestellt.

Zum Dialog der Cyber-Sicherheits-Initiativen treffen sich bereits seit 2017 regelmäßig Organisationen, die IT-Sicherheit fördern wollen. Mit Unterstützung der Allianz für Cyber-Sicherheit werden gemeinsame Projekte und Synergieeffekte identifiziert.

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

E-Mail-Sicherheit

BSI entwickelt sichere Mail-Verschlüsselung weiter

Mit der quelloffenen Browser-Erweiterung „Mailvelope“ können Anwender unter Verwendung des Verschlüsselungsstandards OpenPGP auch ohne spezielles E-Mail-Programm verschlüsselte E-Mails austauschen. Im Rahmen eines seit Januar 2018 laufenden Projekts hat das Bundesamt für Sicherheit in der Informationstechnik BSI „Mailvelope“ mit dem Ziel weiterentwickelt, die Installation, Konfiguration und Anwendung von Ende-zu-Ende-Verschlüsselung deutlich nutzerfreundlicher zu gestalten und damit eine größere Verbreitung von Verschlüsselung beim E-Mail- und Formular-Austausch zu erreichen. Zukünftig kann die Software auch genutzt werden, um vertrauliche Anfragen, zum Beispiel an Ärzte oder Banken, über Web-Formulare zu stellen.

Weitere Informationen:
https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Mailvelope-Extensions_200819.html

BSI INTERNATIONAL

„Europäische IT-Sicherheit sollte nicht in Silos gedacht werden“

Interview mit Prof. Dr. Reinhard Posch, CIO der österreichischen Bundesregierung

Durch seine bereits Jahrzehnte andauernde Arbeit im Bereich der Informationstechnik ist Prof. Dr. Reinhard Posch eine etablierte Persönlichkeit der österreichischen und europäischen Cyber-Sicherheit. Mit seinen wissenschaftlichen und praxisnahen Erfahrungen beleuchtet der Chief Information Officer (CIO) der österreichischen Bundesregierung die Entwicklungen auf EU-Ebene im Bereich Cyber-Sicherheit.

Seit 2001 haben Sie das Amt des CIO der österreichischen Bundesregierung inne. Auf welche Hauptaufgaben konzentrieren Sie sich als CIO heute und wie hat sich das Aufgabenspektrum verändert, seit Sie das Amt übernommen haben?

Mit der Einrichtung der Funktion eines CIO – Österreich war hier durchaus ein Vorreiter – wurde allen Beteiligten klar, dass dies nicht als parteipolitisch ausgerichtete Aktivität fokussiert sein kann, wenn langfristig Erfolge erwartet werden. Es gab und gibt in Österreich kaum IT-betriebliche Defizite. Stattdessen geht es darum, das Hauptziel in einem sich laufend ändernden Umfeld wie der IT, die unterschiedlich und autonom agierenden Player (Ministerien, Länder, Städte, Gemeinden und weitere Verwaltungsplayer), was die Werkzeuge, deren Zusammenspiel und die Sicht der Nutzer anlangt, zu koordinieren und einheitliche Zugänge zu fördern und zu ermöglichen. Hauptwerkzeug dazu ist das Vereinbaren von Umsetzungsstandards und Infrastrukturen (z. B. Register), auf Basis derer die unterschiedlichen Player in der Lage sind, ihre Dienstleistungen entsprechend auszurichten.

Sie sind nicht nur auf nationaler, sondern auch auf europäischer Ebene maßgeblich an Entwicklungsprozessen im Bereich der Informationssicherheit tätig. So waren Sie zum Beispiel von 2007 bis 2011 Vorsitzender des ENISA-Verwaltungsrats und haben als Mitglied im „IT-Rat der Weisen“ die EU-Kommission beraten. Was waren auf EU-Ebene Ihrer Meinung nach die wichtigsten Wegmarken für die europäische Cyber-Sicherheit?

Europäische IT-Sicherheit sollte nicht in Silos gedacht werden. Die Einrichtung des IT-Rates der Weisen hat in dieser Hinsicht ein wichtiges Signal gesetzt, IT-Sicherheit übergreifend innerhalb der Kommission, aber auch gemeinsam mit den Mitgliedsstaaten und den anderen Europäischen Institutionen zu diskutieren und umzusetzen.

Damit war dies auch mit ein Baustein, den Bereich „Network and Information Security“ (NIS) und die Zertifizierung im Sicherheitsbereich zu prägen und zu fördern. Die wichtigsten Elemente zur Stärkung der IT-Sicherheit in Europa sind Aspekte der Förderung EU-weiter und übergreifender versus siloorientierter Ansätze. Nur dadurch können wir den Herausforderungen von Ost und West auf technologischer und politischer Sicht wirksam begegnen.

Wie arbeiten Sie auf EU-Ebene als CIO mit den verschiedenen Akteuren und Institutionen, zum Beispiel der ENISA, zusammen und welche Veränderungen konnten Sie in der europäischen Institutionslandschaft wahrnehmen?

Ein wesentlicher Teil der strategischen Arbeiten und vor allem der richtungsbestimmenden Vorarbeiten findet auch auf informeller Ebene statt. Dazu ist ein hohes Maß an Vertrauen und freiwilliges Engagement unter den Beteiligten wichtig. Auf der Ebene der Institutionen sind personelle Rotationen ein gesetztes Faktum und durchaus wichtig. Allerdings wäre es dabei wichtig, Werkzeuge und Methoden der Kontinuität beim Übergang zu stärken.

Sicherheit wird von immer mehr Institutionen als horizontales Thema verstärkt betrachtet. Das ist wünschenswert, aber dabei entstehen aus Sicht

Kurzprofil Prof. Dr. Reinhard Posch

Prof. Dr. Reinhard Posch studierte Mathematik an der TU Graz. Dort ist er seit 1986 Leiter des Instituts für Angewandte Informationsverarbeitung und Kommunikationstechnologie und berät seit 2001 die österreichische Bundesregierung als Chief Information Officer.

Neben zahlreichen wissenschaftlichen Veröffentlichungen und Forschungsprojekten im Themenbereich der Informationstechnik ist er seit 1999 auch als Gesamtleiter des gemeinnützigen Vereins „A-SIT“ tätig, der sich für den Bereich E-Government mit dem aktuellen Stand der technischen Informationssicherheit befasst.

der einzelnen Institution sehr verständliche, aber dennoch unterschiedliche Ansätze. In der nächsten Stufe wäre eine verstärkte Koordination und Vereinheitlichung der Ansätze von Bedeutung – vor allem dann, wenn diese eine Auswirkung auf Mitgliedstaaten haben. Es ist zu hoffen, dass eine nunmehr auch personell gestärkte ENISA in diese Richtung innerhalb der EU-Institutionen einen positiven Beitrag leisten kann, von dem die Mitgliedstaaten indirekt profitieren würden.

Nach vorne blickend: Was sind Ihrer Meinung nach die wichtigsten Aufgaben im Bereich Cybersecurity, die im europäischen Raum in naher Zukunft vor uns liegen? Und wie können die neusten europäischen Legislativvorhaben, wie der dieses Jahr in Kraft getretene Cybersecurity Act, bei der Bewältigung dieser Aufgaben helfen?

„Cybersecurity und die Notwendigkeit, dieses Thema sehr ernst zu nehmen, ist in den Köpfen der Entscheidungsträger gelandet.“

Cybersecurity und die Notwendigkeit, dieses Thema sehr ernst zu nehmen, ist – nicht zuletzt gefördert durch Vorkommnisse – in den Köpfen der Entscheidungsträger gelandet. Der Cybersecurity Act legt dazu einen weiteren wichtigen Baustein, der sicher weit in die einzelnen Bereiche ausstrahlen wird müssen.

Dies kann dennoch nur der Anfang einer Entwicklung sein. Methoden und Anforderungen konzentrieren sich vor allem auf reaktive und beobachtende Maßnahmen und versuchen dabei, invasive Risiken abzustellen, zu erkennen, zu beseitigen und zu bekämpfen.

In letzter Zeit haben wir (z. B. unter den Schlagworten Spectre und Meltdown) aber erkennen müssen, dass auch nicht invasive und damit wesentlich schwerer zu erkennende Risiken auftreten, die auf ganze IT-Sparten wie Cloud Computing grundsätzliche Auswirkungen haben können. Ansätze des Umganges damit und die Intensivierung der Forschung in diese Richtungen sowie das Aufspüren von weiteren, bislang nicht in unserem Vorstellungsradar sich befindlichen Sicherheitsansätzen und Sicherheitsrisiken müssen deutlich stärker als bislang verfolgt werden. ■

CYBERSECURITY CAMPUS TU GRAZ

Im Februar 2019 wurde der Cybersecurity Campus der TU Graz eröffnet. Als Gemeinschaftsprojekt der TU Graz mit dem schweizerischen Warenprüfkonzern SGS sollen am Cybersecurity Campus im österreichischen Graz IT-Security-Forschung, -Ausbildung, -Produktprüfung und -zertifizierung angesiedelt werden. Als Kernstücke sind ein gemeinsames Forschungszentrum sowie ein Prüf- und Zertifizierungslabor für Cybersecurity geplant. Hierfür soll ein 7000 m² umfassender Neubau entstehen, damit bei voller Betriebsaufnahme dort rund 400 Personen forschen und arbeiten können.

CYBER-SICHERHEIT

Die fünfte Generation

5G und die Folgen

5G. Eine Zahl, ein Buchstabe. Sie bezeichnen das Netz der fünften Mobilfunkgeneration und sorgen derzeit für heftige Diskussionen. Dabei geht es weniger um die vielfältigen Anwendungsmöglichkeiten der neuen Technologie als um die befürchteten politischen Implikationen. Für das BSI ist prioritär, ein adäquates Sicherheitsniveau zu etablieren, damit Staat, Wirtschaft und Gesellschaft nachhaltig von dieser neuen Technologie profitieren können.

5G ist der direkte Nachfolger von LTE bzw. Advanced LTE (4G) und UMTS (3G). Der Standard bietet, verglichen mit der Vorgängertechnik, technologische und funktionale Neuerungen. So sind bei den für 5G reservierten, hohen Frequenzen hohe Übertragungsgeschwindigkeiten möglich und es werden Grundlagen für sinkende Kosten und niedrigeren Energieverbrauch gelegt. Durch potenziell niedrige Latenzzeiten, in bestimmten Situationen unter einer Millisekunde, ermöglicht die fünfte Generation bisher unerreichbare Reaktionsgeschwindigkeiten. Möglich werden diese Verbesserungen durch neuartige Übertragungstechniken auf der Luftschnittstelle sowie eine angepasste Netzarchitektur. Zudem ist 5G deutlich variabler als ein 4G-Netzwerk. Das Netz kann registrieren, ob wenige Geräte eine hohe Datenrate verlangen oder sich viele Geräte mit vergleichsweise geringem Bedarf an einem Ort aufhalten. Je nach Anforderungen kann das Netzwerk dann seine Leistung anpassen und präzise verteilen.

Jeder Technologiesprung, sei es von 2G zu 3G oder wie 2011 von 3G zu 4G, führte zu einem Paradigmenwechsel. 4G ermöglichte erstmals, Videos und Dutzende Bilder in kürzester Zeit abzurufen bzw. zu versenden. Der Sprung von 4G zu 5G ermöglicht gleichfalls völlig neue Anwendungen, Produkte und Dienste für Staat, Wirtschaft, Gesellschaft und den Einzelnen, die sich nur zum Teil heute schon konkret ableiten lassen (siehe Beispiele). Die Standardisierungsdokumente für 5G bietet den Betreibern der Funknetze ein Baukastensystem an, um die gewünschte Funktionalität zu erreichen. So können sowohl lokale Campus-Netze als auch nationale Funknetze aufgebaut werden.

- Für Unternehmen kann 5G beispielsweise die Vernetzung innerhalb und zwischen Firmen verbessern und die Anlagensteuerung mittels Maschine-zu-Maschine-Kommunikation (M2M) revolutionieren.
- Intelligente Autos können ihre Telemetriedaten miteinander austauschen, um z. B. Unfälle zu verhindern.
- Datenintensive und latenzsensitive Anwendungen, wie z. B. simultane virtuelle Realitäten, können zeitgleich erlebt werden.
- 5G kann einen wertvollen Beitrag bei der Digitalisierung von Städten und ländlichen Räumen auf deren Weg zu Smart Cities/Regions leisten.
- Die medizinische Fernbehandlung kann zur flächendeckenden Alternative werden.
- Verbraucher können mit 5G von einem schnelleren mobilen Netz profitieren, mit dem sich eine wachsende Anzahl von Gegenständen im Internet of Things (IoT) vernetzen lassen. Fernsehbilder können ohne Verzögerungen aus mehreren Perspektiven übertragen werden.

5G UND DIE SICHERHEIT IM MOBILFUNK

Das hohe Nutzenversprechen des neuen Mobilfunkstandards ist aber nur dann umsetzbar, wenn es mit dem dafür erforderlichen Sicherheitsniveau konnotiert. Denn mit der durchgängigen Vernetzung und zunehmender Komplexität der Netzwerke werden die digitalen Akteure in allen Bereichen angreifbarer.

5G-SICHERHEITSNIVEAU

Zu den Leistungsmerkmalen von 5G gehört auch ein höheres Sicherheitsniveau. Insgesamt setzen die neuen Sicherheitsvorkehrungen auf den Mechanismen der Vorgängergenerationen auf, verbessern diese jedoch in verschiedener Hinsicht. So wird es möglich, ein deutlich zuverlässigeres, belastbareres und sichereres Netz aufzubauen:

- Eine neue Schlüsselhierarchie versorgt 5G-Komponenten mit einer Reihe kryptografischer Schlüssel. Die Struktur dieser Hierarchie minimiert das Risiko, dass bei einer Kompromittierung einzelner Komponenten der Schutz insgesamt aufgehoben wird.
- „Authentication Confirmation“ (AC) sorgt bei 5G für mehr Sicherheit beim Roaming. Mit aktiver AC schickt das Endgerät des Teilnehmers einen kryptografischen Beweis über die Identität des Mobilfunkbetreibers, in dessen Netzwerk sich das Endgerät eingewählt hat, zurück an den heimischen Mobilfunkbetreiber.
- Die Langzeitidentität der Teilnehmer (IMSI) kann bei 5G auf der Luftschnittstelle verschlüsselt übertragen werden. Dies sorgt dafür, dass sogenannte „IMSI-Catcher“ nicht mehr in der Lage sind, ohne Weiteres die Langzeitidentitäten der Teilnehmer aus der Luftschnittstelle zu extrahieren.

Allerdings ist derzeit nicht absehbar, inwieweit und wann diese neuen Sicherheitsmechanismen in den kommenden Jahren zum Tragen kommen werden. Die Gründe hierfür sind vielfältig. Zunächst ist unklar, wie schnell die Mobilfunkanbieter ihre Netze zu 5G migrieren werden. Der Migrationsprozess ist weder vom Gesetzgeber, noch in den 5G-Spezifikationen fest vorgeschrieben. Daher wird jeder Mobilfunkanbieter sein Netzwerk auf eine andere

Realistisch gesehen wird die vollständige Migration zu 5G und damit zu mehr Sicherheit im Mobilfunk ein langwieriger Prozess.

Art und Weise umstrukturieren. Wie schnell migriert wird, hängt auch davon ab, wie sehr neue 5G-Anwendungen in den nächsten Jahren entstehen und angenommen werden und wie schnell sich 5G-fähige Endgeräte am Markt etablieren.

5G UND DER ÜBERGANG

In Europa werden derzeit Mobilfunknetzwerke der zweiten, dritten und vierten Generation parallel betrieben. Aus Sicht des Betreibers ist es keine einfache Entscheidung, eine gesamte Generation außer Betrieb zu nehmen, da die Anzahl der im Umlauf befindlichen Endgeräte, die nur eine bestimmte Netzgeneration unterstützen, nicht zu unterschätzen ist. Dabei geht es nicht nur um Verbraucher, sondern auch um Geschäftsverträge mit vertraglich zugesicherter Versorgung.

Solange aber neben 5G auch die Vorgängergenerationen verfügbar sind, hat dies Auswirkungen auf das tatsächlich umgesetzte Sicherheitsniveau der Verbindungen, denn ein Angreifer kann durch gezieltes Stören des 5G-Netzwerkes ein Ausweichen auf das 4G-, 3G- oder sogar 2G-Netz provozieren und die dortigen Schwächen ausnutzen. Auch wenn ein mobiles Netzwerk vollständig und ausschließlich auf 5G migriert ist, ist der Betrieb einer Vielzahl von unterschiedlich gearteten Signalisierungskanälen zu anderen Netzwerken unumgänglich, beispielsweise um weltweite Telefonie sicherstellen zu können. Signalisierungsinfrastrukturen und -Protokolle wie SS7, DIAMETER und SIP müssen unterstützt werden, damit Mobilfunknetzwerke vorheriger Generationen, aber auch das Festnetz eingebunden werden.

Aus Sicht des Sicherheitsmanagements ist diese Vielfalt in der Signalisierung ein Problem. Signalisierungsinfrastruk-

5G BRINGT MEHR PERFORMANCE

Die 5G-Netze sollen ein Mindestmaß an Performance bieten und so das Nutzererlebnis in etwa konstant halten. Und das unabhängig davon, wo sich der Nutzer aufhält: zu Hause, unterwegs, in der Stadt oder auf dem Land. Die 5G-Technik ermöglicht künftig mit neuen Verfahren hohe Datenübertragungsraten bzw. eine hohe Datenkapazität. So können bei Festen, Demonstrationen, Weihnachtsmärkten oder Fußballspielen Zehnttausende Nutzer auf engstem Raum gleichzeitig bedient werden. Denn mit einem Kleinzellennetz (Small Cells) kann das Netz an Orten mit vielen Nutzern verdichtet und so mehr Kapazität zur Verfügung gestellt werden. Mit 5G soll aber auch die Versorgungslage im ländlichen Raum weiter verbessert werden.

5G FÖRDERT DIE AUTONOME MOBILITÄT

Autos werden immer smarter. Längst sind moderne Kfz-Modelle mit SIM-Karten und Diagnose-Tools ausgestattet. Mit dem automatisierten Fahren sollen die Sicherheit im Straßenverkehr erhöht und der Verkehrsfluss verbessert werden. Fahrzeuge, die untereinander Betriebsparameter und Sensordaten austauschen (Car-to-Car-Kommunikation), erkennen Kollisionskurse oder nutzen Geschwindigkeitsdaten kooperativ für ein assistiertes Überholen. Weil die Signallaufzeiten sehr kurz sind (unter 20 ms), können sich zum Beispiel bis zu drei Autos, sehr eng hintereinanderfahrend, zum spritsparenden Konvoi zusammenschließen. Mit 5G können auch die verschiedenen Verkehrsträger besser vernetzt werden. So kann der öffentliche Nahverkehr schneller reagieren, wenn es eine erhöhte Nachfrage gibt oder eine Route aktuell nicht befahren werden kann.

DIE INDUSTRIE SETZT MIT 5G AUF ROBOTER

Die Vorzüge von 5G liegen neben der höheren Datenrate insbesondere in der geringen Latenzzeit, die reibungslose Abläufe möglich macht. Hoch individualisierte Produktionsprozesse setzen sowohl eine perfekte Rohstoff- und Warenlogistik als auch umfangreich vernetzte Maschinen voraus. In der industriellen Fertigung wird der durchgängige Datenaustausch zwischen Maschinen, Anlagen, Mensch und Robotern zunehmend an Bedeutung gewinnen. Industrieroboter können in Echtzeit gesteuert werden. Wichtig ist vor allem die wirtschaftliche Vernetzung einer Vielzahl von Sensoren. Mit 5G kann die Anzahl verbundener Geräte pro Basisstation signifikant gesteigert werden.

turen wie das weitverbreitete SS7 stehen aufgrund mangelnder Sicherheit seit Langem berechtigt in der Kritik. Hier versprechen die neuen 5G-Mechanismen wesentlich bessere Sicherheit. Sie kommen aber nur dann vollständig zum Tragen, wenn beide Teilnehmer, sowohl Anrufer sowie Angerufener, von einem 5G-Core-Netzwerk versorgt werden.

Realistisch gesehen wird die vollständige Migration zu 5G und damit zu mehr Sicherheit im Mobilfunk daher wohl ein langwieriger Prozess.

5G UND DAS INTERNET OF THINGS

Viele Anwendungen im Internet of Things (IoT) haben spezielle Anforderungen an die Übertragungstechnologien. Sie werden mit dem Begriff „massive Machine Type Communication“ (mMTC) beschrieben. Aus der Sicht des Betreibers einer IoT-Infrastruktur sind dies in erster Linie geringe Kosten, geringer Energieverbrauch und Übertragungszuverlässigkeit. Diese Anforderungen können auf Kosten von Latenz und Bandbreite bereits heute auch durch andere Low-Power-Wide-Area-Network(LPWAN)-Technologien erfüllt werden.

Auch in der Mobilfunkstandardisierung gibt es bereits Kompromisslösungen, die verschiedene der genannten Anforderungen erfüllen. Diese basieren auf bestehenden 2G-, 3G- und 4G-Netzen, wobei mit „Narrow Band IoT (NB-IoT) die konsequenteste Umsetzung ressourcenschonender Datenübertragung geschaffen wurde. NB-IoT erfüllt auch die meisten Anforderungen an ein 5G-Netz im mMTC-Kontext.

Damit sich außerdem die NB-IoT-Spezifikation am Markt etablieren kann, liegt der Fokus der Standardisierung in diesem Kontext bisher auf der Integration dieser Lösung in das 5G-Kernnetzwerk. Um für zukünftige Anwendungen in IoT-Infrastrukturen, wie z. B. in Smart Cities, qualifiziert zu sein, müssen geeignete Sicherheitsmaßnamen etabliert werden. Hierbei stehen mit passenden Hardwaresicherheitselementen und dem Network Slicing bereits verlässliche Konzepte zur Verfügung.

5G UND DAS HOCH AUTOMATISIERTE FAHREN

Für viele aktuelle Fahrzeugmodelle ist eine Internetverbindung über Mobilfunk als Sonderausstattung oder sogar serienmäßig verfügbar. Diese Verbindungen werden beispielsweise für Mehrwertdienste genutzt, die von den Herstellern individuell angeboten werden. Darüber hinaus ist seit 2018 das E-Call-System, das bei einem Unfall automatisch einen Notruf auslöst, für Neufahrzeuge verpflichtend.

In naher Zukunft werden unter der Bezeichnung „kooperative intelligente Verkehrssysteme“ (engl. Abkürzung C-ITS) weitere Kommunikationsanwendungen im Straßenverkehr Einzug halten. Durch einen direkten Datenaustausch zwischen den Fahrzeugen oder mit der Verkehrsinfrastruktur in der unmittelbaren Umgebung sollen Unfälle verhindert und soll die Effizienz des Straßenverkehrs verbessert werden. In der ersten Ausbaustufe sollen dabei Dienste, wie

etwa die Warnung vor einem Stauende oder einer Baustelle sowie Geschwindigkeitsempfehlungen für grüne Wellen eingeführt werden.

C-ITS-Anwendungen stellen hohe Anforderungen an die IT-Sicherheit. Die ausgetauschten Nachrichten müssen vor Manipulation geschützt werden, d. h., die Integrität und Authentizität der Nachrichten muss gewährleistet werden.

Derzeit existieren zwei konkurrierende Funktechnologien, mit denen diese Dienste realisiert werden können. Allerdings sind sie untereinander nicht kompatibel und können voraussichtlich nicht ohne Weiteres störungsfrei parallel betrieben werden:

- 2010 wurde der Standard IEEE 802.11p (auch als ETSI ITS-G5 bezeichnet) veröffentlicht, der eine WLAN-basierte Kommunikation für die genannten Anwendungen spezifiziert.

- Daneben wurde unter dem Namen LTE-V2X oder Cellular-V2X ein mobilfunkbasiertes Verfahren standardisiert, das neben dem üblichen Kommunikationsweg über eine Mobilfunk-Basisstation auch eine direkte Verbindung der Endgeräte ermöglicht und somit auch ohne Netzabdeckung funktionsfähig ist.

In dem von der EU-Kommission vorgelegten Regulierungsentwurf von C-ITS (delegierter Rechtsakt zur Richtlinie 2010/40/EU 2) hat nun zunächst die WLAN-basierte Technologie aufgrund der höheren Marktreife Eingang gefunden.

LTE-V2X wird derzeit im Kontext der 5G-Aktivitäten weiterentwickelt. Zukünftige Anforderungen, wie beispielsweise durch das automatisierte Fahren, sollen in der Weiterentwicklung zu einem 5G V2X berücksichtigt werden. Genannt werden in diesem Kontext als mögliche Anwendungsfälle das Platooning („die elektronische Deichsel"), bei dem mehrere Fahrzeuge mithilfe eines technischen Steuerungssystems in sehr geringem Abstand hintereinanderfahren, sowie die Übertragung von Video- und Sensordaten an andere automatisierte Fahrzeuge.

5G UND SMART GRID/SMART METERING

Unabdingbar für ein Smart Grid ist die Etablierung eines intelligenten Netzes, das Energieerzeugung, Weiterleitung, Speicherung und Verbrauch effizient verknüpft und ausbalanciert. Damit aber auf Erzeugungsanlagen und flexible Verbrauchseinrichtungen auf Basis digitaler Vernetzung steuernd eingegriffen werden kann, muss die Verfügbarkeit der kommunikativen Anbindung hohen Anforderungen genügen.

KOOPERIEREN FÜR MEHR SICHERHEIT

Im Auftrag der Bundesregierung erarbeiten das BSI als nationale Behörde für Cyber-Sicherheit und die Bundesnetzagentur (BNetzA) derzeit neue Sicherheitsstandards für den Einsatz der 5G-Mobilfunktechnologie.

- Die Bundesnetzagentur erarbeitet einen auf dem Telekommunikationsgesetz basierenden Sicherheitskatalog. Die neuen Sicherheitsregeln sehen vor, dass die Betreiber ihre Telekommunikationssysteme beschreiben und einer Gefährdungsanalyse unterziehen müssen. Insbesondere für Betreiber von öffentlichen Telekommunikationsnetzen mit erhöhtem Gefährdungspotenzial sollen die künftigen Sicherheitsanforderungen genauer definiert werden. Kritische Kernkomponenten künftiger Systeme dürfen nur noch von „vertrauenswürdigen Lieferanten" bezogen werden, die nationale Sicherheitsbetimmungen sowie Datenschutzregelungen einhalten.

- Das BSI erstellt ein Zertifizierungssystem für die konkreten Produkte, die beim Aufbau des 5G-Netzes verwendet werden dürfen. Es soll zusätzlich Standards zur Internetsicherheit entwickeln, Anforderungen an kritische Netze definieren und Sicherheitsstufen für unterschiedliche Netze entwickeln. Sicherheitsrelevante Netz- und Systemkomponenten dürfen nur noch eingesetzt werden, wenn sie von einer vom BSI anerkannten Prüfstelle auf IT-Sicherheit überprüft und vom BSI zertifiziert wurden.

Das BSI ist zudem für die mit dem 5G-Aufbau befassten Unternehmen der zentrale Ansprechpartner zur vielschichtigen Sicherheitsproblematik der 5G-Technologie. Es hat im Juli 2018 eine Projektgruppe eingerichtet, um die sicherheitskritischen Einzelaspekte der 5G-Technologie zu identifizieren und zu analysieren, Lösungsansätze zu entwickeln und die Aktivitäten des BSI in diesem Bereich zu koordinieren.

5G SPART DEN GANG IN DIE ARZTPRAXIS

Neben vielen Konzepten für eHealth-Anwendungen und Assisted Living für Ältere und Pflegebedürftige ermöglicht 5G im Gesundheitswesen vor allem telemedizinische Anwendungen. Von der Facharzt-Versorgung bis hin zur Tele-Intensivmedizin oder zur Fern-OP sind hier Anwendungen denkbar. Haushaltsroboter stellen die Kommunikation zwischen Arzt und Patient im eigenen Haus sicher. Im Notfall kann der Arzt via Echtzeit-Videoübertragung die erste Diagnose stellen und dank Steuerung des Roboters im Ernstfall weitere Erste-Hilfe-Schritte vornehmen. Auch die Vernetzung der Rettungswagen zur Übertragung von Vitaldaten an das Krankenhaus, Fernbehandlung und Telemonitoring von Langzeitpatienten, videobasierte Arztsprechstunden und telemedizinische Beratungen zwischen Ärzten in kleineren Akutkrankenhäusern und Spezialisten in anderen Kliniken können mit 5G realisiert werden.

DIE REALITÄT WIRD VIRTUELL

Augmented Reality – das Einbinden virtueller Inhalte in das reale Bild – wird bislang nur spärlich eingesetzt. 5G könnte der Technologie durch eine massive Steigerung der Übertragungsrate und Verringerung der Latzenzzeiten zum Durchbruch verhelfen. So kann zukünftig eine Möbelhauskette eine App anbieten, in der der Nutzer das gesamte Sortiment vor dem Kauf virtuell in seinen vier Wänden platziert und erst einmal schaut, ob der neue Wohnzimmerschrank überhaupt passt. Das Autohaus zeigt nur eine Karosserie und der Kunde stellt die Innenausstattung selbst zusammen. Erst dann gibt er die Bestellung auf. Tourismusbehörden bieten den Stadtrundgang via App an. Der Besucher läuft real an den Sehenswürdigkeiten vorbei, die App erkennt auf dem Bildschirm, wo er sich befindet, und gibt passgenau Tipps und Hinweise zur Umgebung.

5G HILFT BEIM ENERGIESPAREN

Die Energiewirtschaft steht vor der Herausforderung, dezentrale Stromerzeugungsanlagen und Verbraucher sicher und beherrschbar in das Stromnetz und den Strommarkt zu integrieren. Intelligente Versorgungsnetze können mit 5G-Technik so ausgebaut und gesteuert werden, dass die Aufnahmekapazität der Netze optimiert wird. Über virtuelle Kraftwerke werden Erzeuger, Netzbetreiber, Speicher und Verbraucher zusammengeschaltet. 5G ermöglicht darüber hinaus, intelligente Gebäudetechnik und intelligente Messsysteme einfacher zu implementieren oder auch Versorgungsinfrastrukturen wie Wasser- und Abwasser- oder Belüftungssystemen besser zu überwachen.

Das BSI hat mit dem Messstellenbetriebsgesetz von 2016 die Aufgabe erhalten, technische Vorgaben für eine sichere Kommunikationsinfrastruktur im Smart Grid zu entwickeln. Dabei wurde ein Infrastrukturansatz gewählt, in dem das Smart-Meter-Gateway die zentrale Rolle spielt. Als Kommunikationsplattform des intelligenten Messsystems ermöglicht es, vielfältigste Anwendungsfälle in verschiedenen Einsatzbereichen sicher umzusetzen.

Ein wesentlicher Parameter für die Funkanbindung der intelligenten Messsysteme ist die Gebäudedurchdringung der Signale. Damit kommt es vor allem auf die verwendeten Frequenzen an. Insbesondere Frequenzen unter 1 GHz sind dafür geeignet und werden von den folgenden Mobilfunkstandards bedient: GSM (GSM 900), LTE (E-UTRA Band 8, 20 und 28) und neu 5G (n8, n20, n28). Daneben werden im lizenzfreien SRD-860-Band zahlreiche offene und proprietäre Funkstandards betrieben.

Die funkbasierte Kommunikation der Messgeräte mit dem Smart-Meter-Gateway erfolgt derzeit im lizenzfreien SRD-860-Band mittels wireless-mBus. Die Vorteile sind die relativ gute Gebäudedurchdringung und der geringe Energieverbrauch der Messgeräte für die Funkübertragung. Die Technische Richtlinie des BSI TR-03109-1 ist an dieser Stelle offen für weitere Funkübertragungstechnologien, solange der Datenverkehr unter Berücksichtigung der Vorgaben an den Protokollstapel sowie an die Kryptografie übertragen werden kann.

Um das Smart-Meter-Gateway im Weitverkehrsnetz (WAN) anzubinden, kommen derzeit verschiedene TK-Technologien zum Einsatz: Breitband-Powerline, DSL oder GPRS/LTE. Der 5G-Standard wird sich in die Liste der Technologien zur Anbindung des intelligenten Messsystems einreihen. Die Anforderungen an die Kommunikationstechnologie in verschiedenen Einsatzbereichen werden weiterhin vom BSI in Studien untersucht. ■

Telefonie per Voice over IP

BSI-Studie zur Sicherheit von paketvermittelter Sprachkommunikation in Provider-Netzen

von Dr. Herbert Blum, Referat Sicherheit in Internetinfrastrukturen und -diensten

Analoge und ISDN-Telefonanschlüsse werden zurzeit flächendeckend auf „Voice over IP“ (VoIP) umgestellt. Dieser Umstieg auf eine einheitliche Technologie, um Daten und Sprache zu übertragen, bietet viele Vorteile. Er birgt allerdings auch potenzielle Risiken, die es bei der „klassischen“ Telefonie bisher so nicht gab. Eine Studie des BSI hat diese Risiken untersucht. Ihr Ziel: Maßnahmen zur Absicherung von VoIP zu erarbeiten.

ALL-IP-INFRASTRUKTUR

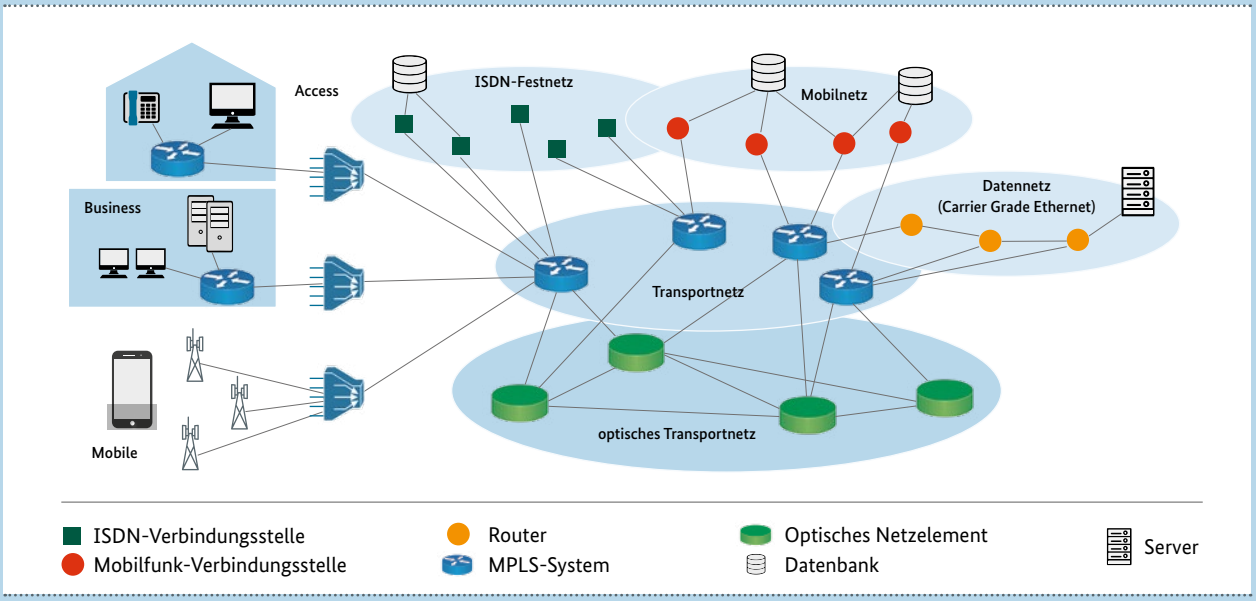
In der Vergangenheit basierten Telefonie, Mobilfunk, Internet und diverse andere Dienste auf eigenständigen Technologien, die insbesondere auf der Zugangsebene jeweils auch eine eigene physikalische Netzarchitektur erforderten (s. Abb. 1). In der neuen All-IP-Infrastruktur werden diese heterogenen physikalischen Access-Netze weitgehend virtualisiert und auf Basis einer einheitlichen Technologie zusammengefasst (s. Abb. 2). Telefonie bildet in dieser „neuen Welt“ nur noch einen Dienst unter vielen und wird über die gleiche Hardware abgewickelt wie auch die Übertragung von Internetdaten. Diese Vereinheitlichung bringt zahlreiche Vorteile. Dazu zählen eine erheblich vereinfachte Administration des Netzes, die schnellere Behebung von Störungen sowie beträchtliche Kosteneinsparungen.

KLASSISCHE TELEFONIE VS. VOIP

Obwohl die klassische Telefonie, deren Wurzeln bis in die Anfänge des letzten Jahrhunderts reichen, heute technologisch hoffnungslos veraltet ist, besaß sie doch einige Sicherheitsmerkmale, die bei VoIP aufgrund der gänzlich anderen Konzeption – zumindest ohne zusätzliche Vorkehrungen – vorderhand nicht gegeben sind. So war etwa bisher bei einem Stromausfall das Telefonieren weiterhin möglich, weil das Netz über eine redundante Stromversorgung verfügte. Auch das Abhören von Telefonaten war für einen externen Angreifer nur möglich, wenn er sich lokal direkten Zugriff auf die Übertragungsleitung verschaffte.

BSI-STUDIE ZUR SICHERHEIT VON VOIP

Insbesondere für Berufsgruppen mit besonderer Verschwiegenheitspflicht wie Ärzte, Juristen oder Steuerberater ist es wichtig, dass bei VoIP die Vertraulichkeit in gleicher Weise gegeben ist, wie man dies bisher von der klassischen Telefonie erwartete. Auch die Verfügbarkeit im Not- bzw Katastrophenfall muss gewährleistet sein. Neue Betrugsszenarien, die die Technik der IP-Telefonie ermöglicht, müssen analysiert und ausgeschlossen werden. Um diese Fragen zu klären, hat das



Aufbau klassischer Kommunikationsnetze

BSI gemeinsam mit der Firma DOK Systems aus Garbsen in einer Studie die „Sicherheit von paketvermittelter Sprachkommunikation in Provider-Netzen genauer untersucht (DOK-Projektleitung: Dr. Tim Gorgass, Mitarbeit: Felix Fehlau, Marian Jersch, Jörn Stecker und Prof. Dr. Gerd Siegmund).

VERFÜGBARKEIT

Wie die Studie zeigte, sind die internen Netze der TK-Provider durch entsprechende Notstromversorgungsanlagen selbst bei einem flächendeckenden Stromausfall über mehrere Stunden bis hin zu Tagen abgesichert. Problematische Situationen hingegen können sich an der Peripherie des Netzes ergeben. Fällt beim Kunden der Strom – und damit die Energieversorgung des Home-Routers – aus, so ist von diesem Anschluss aus auch die Telefonie über VoIP nicht mehr möglich. Hier empfiehlt sich zukünftig also auch für Privathaushalte, eine unabhängige Stromversorgung (z. B. eine gepufferte Steckdosenleiste) für den Home-Router einzurichten. Weitere kritische Komponenten in diesem Zusammenhang bilden die Zugangspunkte zum Provider-Netz, die sogenannten MSANs (Multiple-Service Access Nodes) und Multifunktionsgehäuse („Telefonkästen“ an der Straße). Hier konnten im Rahmen der Studie keine belastbaren Aussagen darüber gewonnen werden, ob diese Komponenten einen Stromausfall länger als einige Minuten überbrücken können. Gleiches gilt im Übrigen für Handymasten: Auch hier gibt es derzeit keine belastbaren Aussagen darüber, wie lange bei Stromausfall Mobilfunk möglich bleibt.

VERTRAULICHKEIT

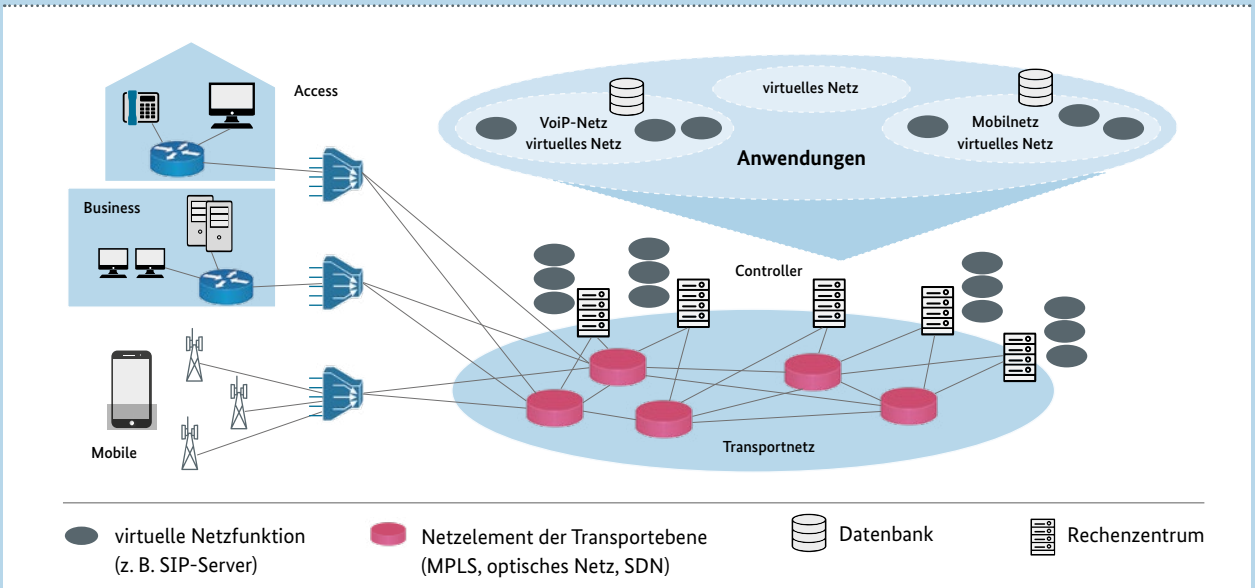
Grundsätzlich fällt die VoIP-Kommunikation in gleicher Weise wie die klassische Telefonie unter das Fernmeldegeheimnis. Um auch illegales Abhören zu verhindern, wäre es allerdings wünschenswert, wenn die Sprachdaten, wie bei IP-Daten in vielen anderen Bereichen üblich, verschlüsselt übertragen würden. Dem stehen allerdings verschiedene technische Hürden entgegen: Sprachübertragung ist eine Real-Time-Anwendung, bei der die Datenpakete möglichst synchron zu übermitteln sind, damit beim Empfänger auch wieder verständliche Sprache ankommt. Ob eine durchgängige Verschlüsselung von VoIP möglich ist, hängt daher u. a. davon ab, inwieweit die TK-Provider der jeweiligen Kommunikationspartner – z. B. über Ländergrenzen hinweg - die Übertragungsnetze technisch kontrollieren. Eine unabdingbare Voraussetzung für verschlüsseltes VoIP ist jedoch, dass es hierfür geeignete Endgeräte im Handel zu kaufen gibt. Derzeit werden so gut wie keine Home-Router mit VoIP-Verschlüsselungsoption angeboten.

AUTHENTIZITÄT

Bereits bei ISDN ist es möglich, dem Angerufenen eine vom Anrufer vorgegebene Rufnummer anzeigen zu lassen. Aufgrund der leitungsvermittelten Technologie von ISDN ist es für die TK-Provider dabei jedoch relativ einfach möglich, zu kontrollieren, ob der Anrufende ein Nutzungsrecht an der angezeigten Nummer besitzt. Bei VoIP hingegen ist es technisch aufwendig, die Nutzungsberechtigung an einer angezeigten Telefonnummer zu überprüfen, insbesondere wenn der Anruf aus einem anderen Netz (z. B. aus dem Ausland) erfolgt. Darum wird dies meist unterlassen. Dies führt dazu, dass dieses sogenannte Call-ID-Spoofing immer öfter zu betrügerischen Zwecken eingesetzt wird.

FAZIT

Die BSI-Studie hat gezeigt, dass die VoIP-Technologie gegenüber der klassischen Telefonie neben bedeutenden Vorteilen auch neue Sicherheitsrisiken birgt. Diese Risiken können jedoch durch zusätzliche technische und organisatorische Maßnahmen beseitigt oder zumindest erheblich reduziert werden. Das BSI und die Bundesnetzagentur erarbeiten derzeit Empfehlungen, wie solche Maßnahmen praktisch umzusetzen sind. ■



All-IP-Infrastruktur

Von Insellösungen zu einheitlichen Zugangsmöglichkeiten

Sicherheit von eID-Verfahren geprüft

von Dr. Thomas Schnattinger, Referat eID-Strukturen für die Digitalisierung

Das Onlinezugangsgesetz zeigt den klaren politischen Willen von Bund und Ländern, das E-Government umfassend auszubauen. Bürger sollen Verwaltungsdienstleistungen grundsätzlich auch digital nutzen können. Das BSI hat dazu Kriterien für eine bedarfsgerechte Sicherheitsbewertung von Authentisierungsverfahren ausgearbeitet.

Seit knapp zehn Jahren steuert der IT-Planungsrat die föderale Zusammenarbeit in der Informationstechnik. Momentan ist dabei die Umsetzung der eID-Strategie für das E-Government als ein Projekt von herausragender Bedeutung für die Zusammenarbeit von Bund, Ländern und Kommunen definiert. Einen akzeptablen Ausgleich zwischen Sicherheit und Nutzerfreundlichkeit zu finden ist dabei besonders wichtig.

Je nach angebotener E-Government-Dienstleistung besteht ein unterschiedlich hoher Schutzbedarf. Dies gilt besonders für die Verfahren, mit denen die Nutzer identifiziert und authentisiert werden. Hier muss stets direkt mit ihnen interagiert werden. Damit verbunden ist die Frage, welche Mindestanforderungen an die Nutzer gestellt werden müssen, z. B. hinsichtlich erforderlicher Soft- und Hardware für den Zugang oder zulässiger Passwörter. Die Sicherheit der Authentisierung ist für alle Beteiligten von zentraler Bedeutung. Die Anbieter von E-Government-Dienstleisungen benötigen einen Schutz vor manipulierten Anfragen, die legitimen Nutzer müssen vor Identitätsmissbrauch geschützt sein.

ABGESTUFTES VERTRAUENSNIVEAU

Abhängig von den im Einzelfall möglichen Betrugs- und Schadenszenarien werden für untschiedliche E-Government-Dienstleistungen abgestufte Mindestvertrauensniveaus benötigt. Grundlage für die Einschätzung des jeweils (mindestens) benötigten Vertrauensniveaus ist die europaweit gültige Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung), sowie die darauf abgestimmten nationalen Konkretisierungen in der Technischen Richtlinie TR 03107-1 des BSI über elektronische Identitäten und Vertrauensdienste. Sie beschreibt, welche Kriterien eID-Verfahren in Deutschland jeweils erfüllen müssen, damit sie das Vertrauensniveau „normal“, „substantiell“ oder sogar „hoch“ erreichen. Auf dieser Grundlage kann jeder E-Government-Anbieter unter Berücksichtigung spezifischer Gefährdungen und rechtlicher Rahmenbedingungen sicherstellen, dass für die angebotenen Dienstleistungen sowohl ausreichend gesicherte als auch praktikable Verfahren und Mechanismen eingesetzt und angeboten werden.

Für das Vertrauensniveau „normal“ mit der Kombination „Nutzername + Passwort“ und für das Vertrauensniveau „hoch“ mit der eID-Funktionalität des Personalausweises und dem elektronischen Aufenthaltstitel gibt es bereits verfügbare und verbreitete Mechanismen. Hingegen fehlt es bislang an anwendungsübergreifend akzeptierten Verfahren, die gezielt für die Anforderungen des Vertrauensniveaus „substantiell“ zugeschnitten sind.

DIE KRITERIEN DER TECHNISCHEN RICHTLINIE TR 03107 1

Um anhand der TR 03107-1 verschiedene Verfahren auf ihre Sicherheit im Hinblick auf das Vertrauensniveau „substantiell“ prüfen zu können, hat das BSI in einem Projekt zunächst eine Prüfberichtsvorlage und einen detaillierten Anforderungskatalog zu der TR 03107-1 erstellt. Nach Abschluss dieser Vorarbeiten wurden in Abstimmung mit dem IT-Planungsrat insgesamt vier Verfahren untersucht. Dabei wurden gezielt Verfahren ausgewählt, die bereits praktisch verfügbar sind. Damit können sie bei Bedarf auch sehr kurzfristig für weitere Anwendungen eingesetzt werden. Die Bewertung selbst erfolgte in sehr enger Zusammenarbeit mit den jeweiligen Verfahrensbetreibern und einem vom BSI beauftragten Dienstleister. Dabei hat es sich als unerlässlich erwiesen, dass zu den Verfahren hinreichende Dokumentationen verfügbar sind, damit auftretende Rückfragen zeitnah und präzise beantwortet werden können.

In der jeweils zunächst untersuchten Ausprägung konnte noch keines der Verfahren bei allen notwendigen Kriterien das Vertrauensniveau „substantiell“ erreichen. Indem aber bei der Analyse genau eingegrenzt wurde, bei welchen Kriterien die Anforderungen für „substantiell“ zunächst nicht erfüllt sind (oder noch nicht nachgewiesen werden konnten), können die Verfahrensbetreiber gezielt Verbesserungen vornehmen. Ebenso können E-Government-Diensteanbieter die Ergebnisse nutzen. Denn da es letztlich den Diensteanbietern obliegt, das mindestens erforderliche Vertrauensniveau festzulegen, können zum Beispiel übergangsweise auch Verfahren eingesetzt werden, die bei einzelnen Aspekten nicht das insgesamt angestrebte Vertrauensniveau erreichen. Im Einzelfall ist hier immer eine Risikoabschätzung und gegebenenfalls rechtliche Prüfung vorzunehmen.

AUSBLICK

Eine weitere Erkenntnis aus dem Projekt und den durchgeführten Verfahrensbewertungen ist, dass insbesondere der Prozess der Registrierung bzw. Erstidentifizierung sehr kritisch ist. Hier existieren noch keine allgemein für das Vertrauensniveau „substantiell“ anerkannte und allgemein verfügbare Verfahren, die ohne ein Erscheinen des Nutzers vor Ort auskommen. In diesem Zusammenhang arbeitet das BSI ebenfalls an einem Projekt, in dem, basierend auf der Technischen Richtline TR 03147, geeignete Kriterien für die Bewertung der Sicherheit von Identifizierungsprozessen ausgearbeitet werden. ■

Weitere Informationen:

BSI TR-03107 Elektronische Identitäten und Vertrauensdienste im E-Government: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html

Notifizierung von eID-Systemen gemäß eIDAS, Datenschutz und Datensicherheit (DuD) 4/2019: https://rdcu.be/bxfgN

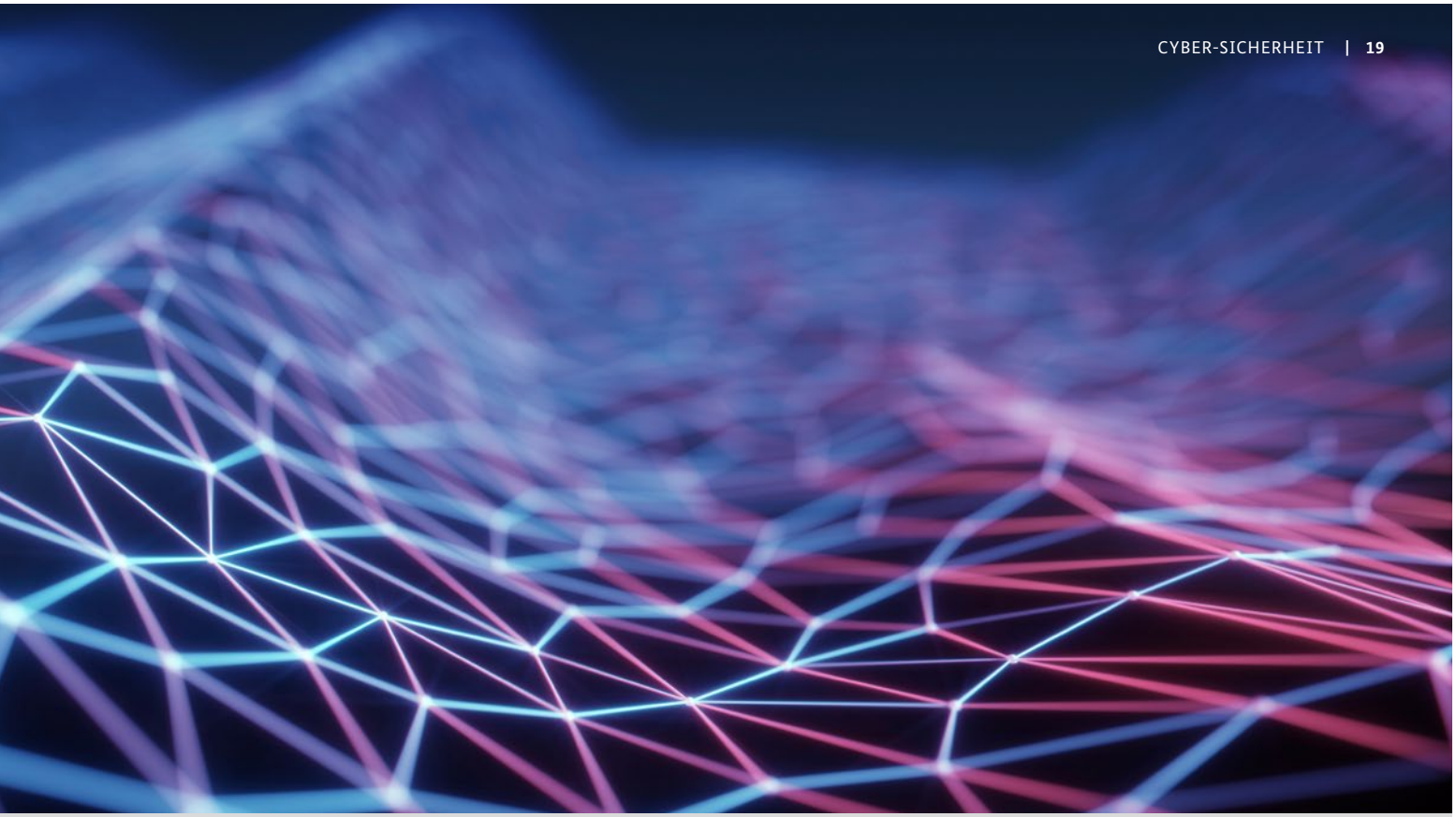
Cyber-Angriffe mit neuer Qualität

Erkenntnisse aus dem Lagebericht zur IT-Sicherheit 2019

Einmal im Jahr veröffentlicht das BSI den Bericht „Die Lage der IT-Sicherheit in Deutschland“. Die aktuelle Ausgabe mit dem Berichtszeitraum Juni 2018 bis Mai 2019 beschreibt erneut eine Vielzahl von Gefahren und kritischen Schwachstellen. Es zeigt sich: Viele Entwicklungen, die das BSI im Jahr zuvor prognostiziert hatte, sind eingetreten.

Bereits 2018 hatte das BSI vor einer neuen Qualität an Cyber-Angriffen gewarnt, und genau diese haben stattgefunden. Bereits 2018 hatte das BSI die Schadsoftware Emotet als eine der größten Cyber-Bedrohungen der Welt bezeichnet und vor einer professionellen Weiterentwicklung gewarnt. Auch darin sieht sich das BSI nach den gezielten Ransomware-Angriffen auf Unternehmen im aktuellen Berichtszeitraum bestätigt.

Auch unabhängig von Emotet zählt Ransomware nach wie vor zu den größten Bedrohungen für Unternehmen, Behörden und andere Institutionen sowie für Privatanwender. Immer wieder kommt es zu Komplettausfällen von Rechnern und Netzwerken, aber auch von Produktionsanlagen. Zudem sind zuletzt Einrichtungen des Gemeinwesens wiederholt Ziel von Ransomware-Angriffen geworden. Dazu zählen beispielsweise Krankenhäuser in Deutschland genauso wie Kommunalverwaltungen in den USA. Dabei ist ein Trend zu beobachten: Angriffe richten sich gezielt gegen zentrale Dienstleister, über die dann deren Kunden oder angeschlossene Netzwerke mit Ransomware infiziert werden können. Das Schadenspotenzial ist enorm: Die Kosten unter anderem für Produktionsausfälle, Datenverlust, Bereinigung und Wiederher-



stellung der Systeme gehen zum Teil in die Millionen, Dienstleistungen von Einrichtungen des Gemeinwesens sind nicht oder nur eingeschränkt verfügbar.

Die vom BSI zuvor prognostizierte neue Qualität der Cyber-Angriffe drückt sich auch durch mehrere große Fälle von Identitätsdiebstahl aus, die in den Jahren 2018 und 2019 für Aufmerksamkeit sorgten. Unter anderem betroffen waren Anwender von Sozialen Netzwerken und Kunden großer Hotelketten, hunderte Prominente und Politiker aus Deutschland im Zuge des Doxing-Vorfalls, der im Januar 2019 bekannt wurde, sowie hunderte Millionen andere Internetnutzer, deren Daten durch die als „Collection #1“ bis „Collection #6“ bezeichneten Vorfälle öffentlich im Internet verfügbar gemacht wurden. Bemerkenswert dabei ist nicht nur die Häufung der Vorfälle, sondern auch die riesige Menge der abgeflossenen und im Internet veröffentlichten persönlichen Daten.

Nach wie vor ist eine hohe Dynamik der Angreifer bei der (Weiter-)Entwicklung von Schadprogrammen und Angriffswegen festzustellen. Rund 114 Millionen neue Schadprogramm-Varianten wurden im Berichtszeitraum identifiziert. Das Bedrohungspotenzial von Schadprogramm-Spam steigt weiterhin an, auch wenn die Zahl der versendeten Spam-Mails gesunken ist. E-Mails mit Schadprogrammen zählen dennoch zu den am häufigsten detektierten Angriffen auf die Bundesverwaltung. Die Auswirkungen solcher Schadprogramme nehmen zu, nicht nur in der klassischen Bürokommunikation, sondern auch in Produktivbereichen der Wirtschaft.

Die Bedrohungslage durch Botnetze bleibt unverändert hoch, wobei sich auch hier die Angreifer die Digitalisierung zunutze machen und den Fokus auf mobile Endgeräte und IoT-Systeme legen. Täglich bis zu 110.000 Botinfektionen deutscher Systeme wurden registriert und vom BSI mit dem Ziel der Bereinigung an die jeweiligen Netzbetreiber gemeldet. Noch mehr Angriffspotenzial ermöglichen serverbasierte Botnetze, insbesondere vor dem Hintergrund der zunehmend genutzten Cloud-Infrastrukturen. Mehr als jede zweite Attacke wird über kompromittierte oder missbräuchlich angemietete Cloud-Server ausgeführt. Fast jeder Cloud-Dienstleister wurde demnach bereits mindestens einmal von Kriminellen zur Durchführung von DDoS-Attacken missbraucht.

Unnötig verschärft wird die ohnehin angespannte Cyber-Sicherheitslage durch die in vielen Fällen festzustellende digitale Hilflosigkeit aufseiten der Anwender. Täter nutzen Schwächen individuellen Sicherheitsverhaltens in Verbindung mit strukturell unzureichend gesicherten Produkten und Systemen gezielt aus. Abhilfe kann die konsequente Nutzung von IT-Sicherheitsmaßnahmen nach Stand der Technik sowie eine Stärkung der digitalen Eigenverantwortung jedes einzelnen Nutzers schaffen.

Eine Übersicht über wichtige Zahlen aus dem aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland finden Sie auf den folgenden Seiten. ■

Cyber-Sicherheitslage 2019

Aktion und Reaktion

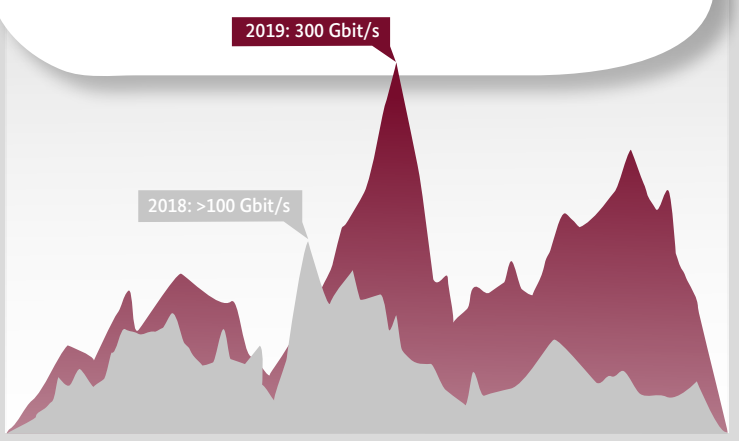
EMOTET
Hocheffizientes Social-Engineering

RANSOMWARE
Fortschrittliche Angriffstechniken führen zu massiven Konsequenzen

114 Mio.
neue Schadprogramm-Varianten

bis zu
110.000
Botinfektionen täglich in deutschen Systemen

300 Gbit/s
erreichten die Peaks in der Angriffsbandbreite über die Cloud



40 Mio. Euro
Schaden erlitt ein einzelnes Unternehmen durch einen Ransomware-Angriff

Ca. **770.000**

Mails mit Schadprogrammen in deutschen Regierungsnetzen abgefangen

11,5 Mio.

Meldungen über kompromittierte IP-Adressen verschickte das BSI an deutsche Netzbetreiber

1.500

registrierte KRITIS-Anlagen

3.700

Mitglieder der Allianz für Cyber-Sicherheit
(2018 = 2.700 Mitglieder)

2019:
252
Meldungen von KRITIS-Betreibern

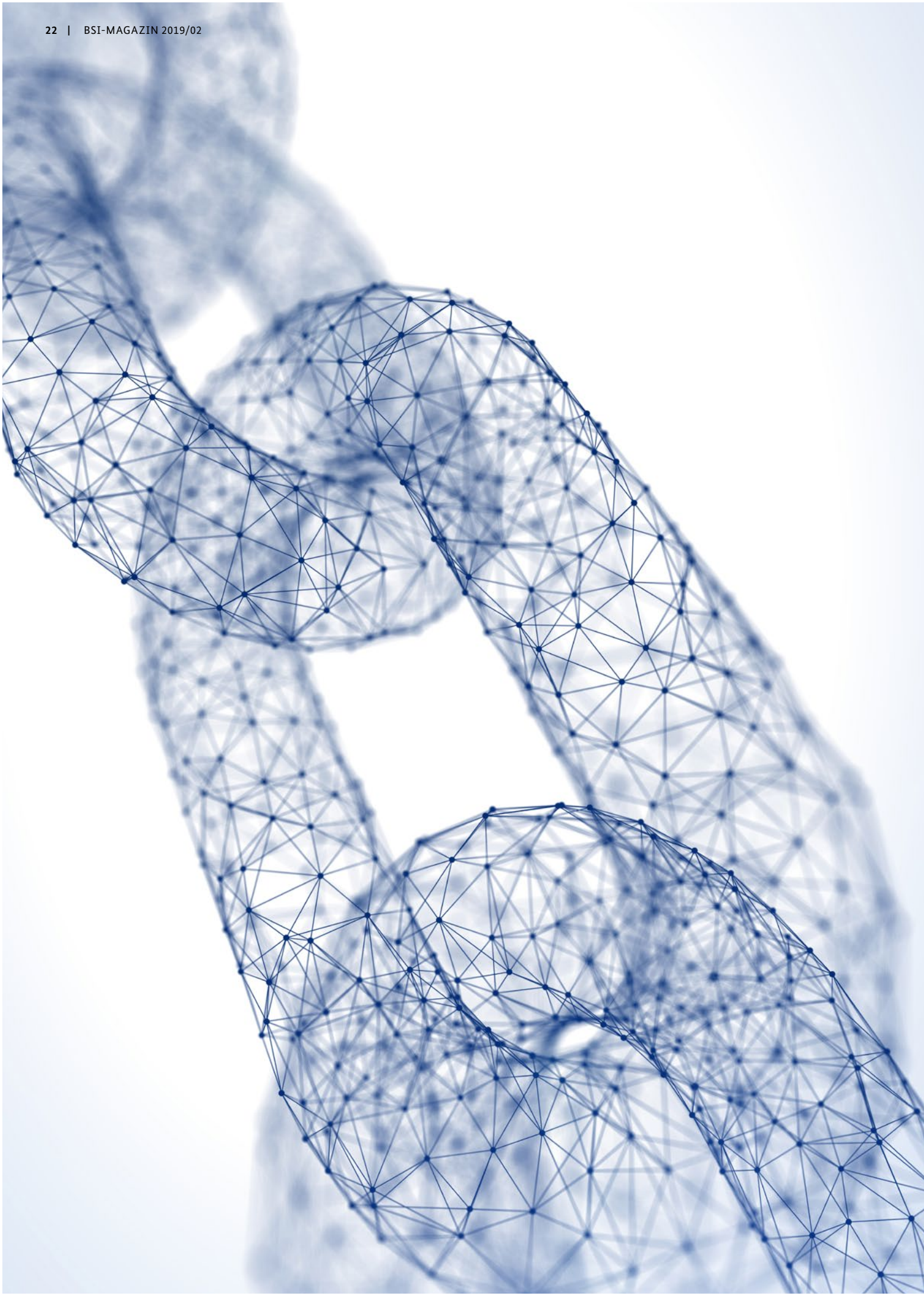
2018:
145
Meldungen

105.000

Abonnenten Bürger-CERT
(2018 = 100.000 Abonnenten)

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

Quelle: Bundesamt für Sicherheit in der Informationstechnik



Blockchain sicher gestalten

Konzepte, Anforderungen, Bewertungen

von Dr. Christian Berghoff und Dr. Ute Gebhardt, Referat Bewertungsverfahren für eID-Technologien in der Digitalisierung, sowie Dr. Manfred Lochter und Dr. Sarah Maßberg, Referat Vorgaben an und Entwicklung von Kryptoverfahren

Blockchains sind seit einiger Zeit nicht nur Experten, sondern durch häufige Erwähnung in den Medien auch der breiten Öffentlichkeit bekannt. Ihr Einsatz wird in zahlreichen Bereichen vorgeschlagen und erprobt. Im Mai 2019 veröffentlichte das BSI eine umfassende und tiefgehende Analyse der Blockchain-Technologie mit Schwerpunkt IT-Sicherheit.

Blockchain ist eine neue Technologie zur Datenhaltung, bei der durch verteilte konsensuale Datenspeicherung in Verbindung mit kryptografischen Verfahren (siehe Grafik 1) und weiteren technischen Maßnahmen Transparenz erzeugt, Manipulationen erschwert und die Abhängigkeit von einer zentralen Stelle weitestgehend eliminiert werden sollen. Diese Merkmale der Blockchain-Technologie wurden zum Anlass genommen, ihre Nutzung in Anwendungsfällen vorzuschlagen, bei denen mehrere Parteien mit unterschiedlichen Interessen involviert sind und sich nicht auf eine zentrale Stelle einigen können, die die Anwendung kontrolliert. Ebenso wurden auch Anwendungsfälle vorgeschlagen, in denen zwar eine zentrale Stelle existiert, man sich jedoch von einer unmittelbaren Interaktion der Parteien Effizienzgewinne verspricht.

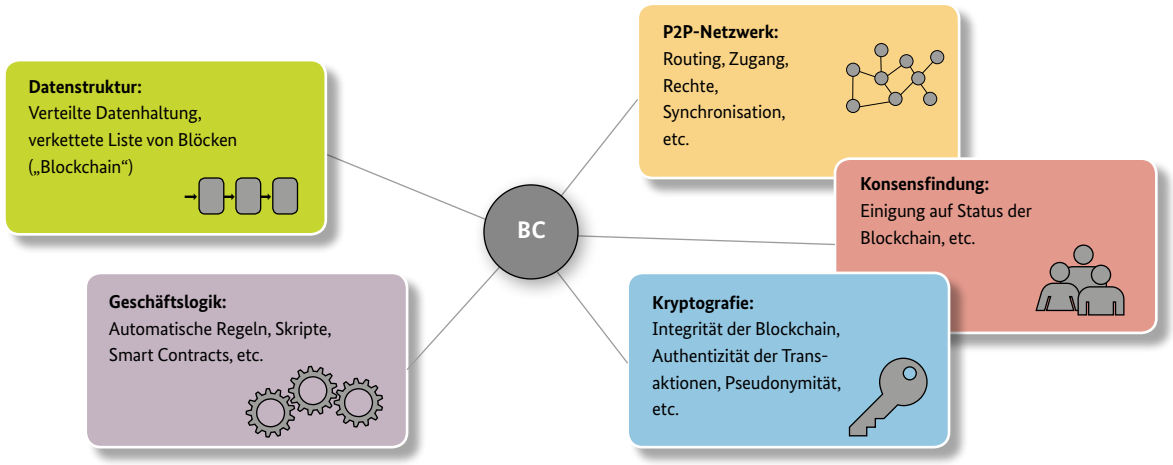
Aufgrund der von der Blockchain-Technologie erhofften Vorteile ist sie momentan zu einem Trendthema geworden, mit dem sich eine Vielzahl an Akteuren aus Forschung, Wirtschaft und Verwaltung intensiv beschäftigt. Die Verwendung der Technologie wird in vielen Bereichen diskutiert und untersucht. Bisher werden Blockchains aber nur in der Finanzbranche, insbesondere im Bereich der Kryptowährungen, in vergleichsweise großem Ausmaß praktisch eingesetzt.

ROLLE DES BSI

Das BSI beschäftigt sich bereits seit Längerem intensiv mit IT-Sicherheitsaspekten der Technologie. So veröffentlichte es zunächst im Februar 2018 eine Liste von Eckpunkten für den sicheren Einsatz von Blockchains. Im Mai 2019 folgte darauf das Dokument „Blockchain sicher gestalten. Konzepte, Anforderungen, Bewertungen“, dessen Kernaussagen der vorliegende Beitrag wiedergibt. Es richtet sich in erster Linie an potenzielle Anwender, die den Einsatz der Blockchain-Technologie erwägen und über fachliche Grundkenntnisse verfügen. Es verfolgt das Ziel, einen umfassenden und strukturierten Überblick über die Aspekte der IT-Sicherheit zu bieten, sodass Leser ihre Projektideen unter diesem Gesichtspunkt bewerten und gegebenenfalls konkrete Maßnahmen für die Gestaltung und den sicheren Betrieb ihrer Lösung ableiten können.

Daneben betrachtet das Dokument auch weitere Auswirkungen der technischen Grundkonzeption, z. B. auf die Effizienz und rechtliche Fragestellungen. Insbesondere wird in einem Beitrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) diskutiert, inwieweit datenschutzrechtliche Vorgaben erfüllt werden können. Grundsätzlich schneiden Blockchains gegenüber klassischen

GRUNDBAUSTEINE DER BLOCKCHAIN-TECHNOLOGIE



Grafik 1

zentralen Datenbanken in den Punkten Verfügbarkeit und Robustheit gegen Missbrauch positiv ab. Dem stehen auf der anderen Seite Nachteile im Bereich Vertraulichkeit und Effizienz gegenüber.

Ein Ziel des BSI ist es, bei neuen Technologien Security-by-Design zu erreichen. Mit dem Dokument wird dargelegt, welche Überlegungen Designer von Blockchain-Anwendungen in Abhängigkeit vom jeweiligen Rechtsrahmen frühzeitig anstellen sollten, um dieses Ziel zu erreichen. Mit seinen Veröffentlichungen bietet das BSI eine Grundlage, um die im Koalitionsvertrag der jetzigen Regierungskoalition vereinbarte und für den Sommer 2019 erwartete nationale Blockchain-Strategie umzusetzen.

Die Nutzung von Blockchain allein löst keine IT-Sicherheitsprobleme.

IT-SICHERHEIT ALLGEMEIN

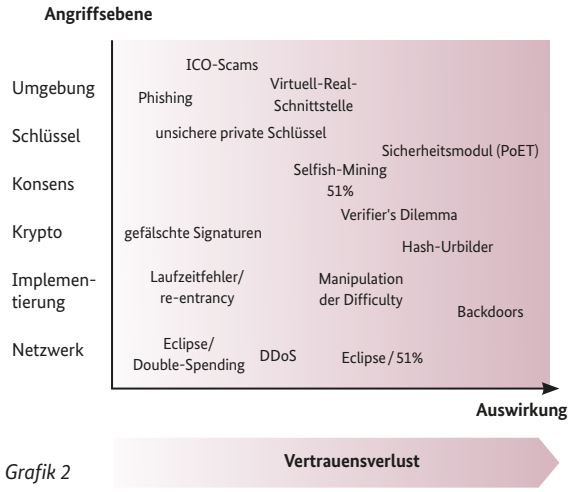
Die Nutzung von Blockchain allein löst keine IT-Sicherheitsprobleme. Vielmehr bleiben wohlbekannte Probleme wie die Sicherheit von Hard- und Software bestehen. Hinzu kommen neue Angriffsvektoren auf verschiedene Komponenten des Systems. Neben den Konsensmechanismen, mittels derer die verteilt gespeicherten Daten konsistent gehalten werden, und den sogenannten Smart Contracts, die die Ausführung von Programmen im Blockchain-Netzwerk erlauben, sind hier beispielsweise externe Schnittstellen zu nennen, über die Daten eingefügt und ausgelesen werden (siehe auch Grafik 2). Konkrete Vorfälle zeigen, dass die Angriffsmöglichkeiten nicht nur theoretischer Natur sind.

Die Blockchain-Technologie weist ein breites Spektrum an Ausgestaltungen auf. Zur Differenzierung werden hier häufig die Einsehbarkeit der Daten (Leserechte) sowie die Fortschreibbarkeit der Blockchain (Schreibrechte) herangezogen. Jedoch gibt es auch für Konsensmechanismen und Smart Contracts eine Reihe von Ansätzen mit teils sehr unterschiedlichen Eigenschaften. Sie hängen zu einem gewissen Grad mit der grundsätzlichen Ausgestaltung einer Blockchain zusammen, bieten aber weitere Freiheitsgrade. Für konkrete Anwendungen, in denen Blockchains eingesetzt werden sollen, muss daher sorgfältig analysiert werden, welche Ausgestaltung am geeignetsten ist. Es ist davon auszugehen, dass das Modell von Bitcoin, das medial die größte Aufmerksamkeit findet, für die meisten Anwendungen nicht sinnvoll sein wird.

AUSGEWÄHLTE ASPEKTE

Im Bereich der Konsensmechanismen wird die breite Diskussion von dem Verfahren Proof-of-Work (PoW) dominiert, das unter anderem von Bitcoin verwendet wird und insbesondere wegen seines immensen Energiebedarfs in der Kritik steht. PoW ermöglicht es, die Daten ohne Authentisierung der einzelnen Parteien konsistent zu halten und dabei Manipulationen zu verhindern. Unbeachtet bleibt oft die Tatsache, dass Blockchains mit strikterer Rechtevergabe und Authentisierung der Parteien, wie sie für viele Anwendungen geboten scheinen, den Einsatz von sogenannten nachrichtenbasierten Konsens-

ÜBERSICHT ÜBER ANGRIFFE AUF BLOCKCHAINS*



Grafik 2

**Die spezifischen Angriffe auf den unterschiedlichen Ebenen werden in der BSI-Veröffentlichung ausführlich dargestellt.*

mechanismen erlauben, die wesentlich effizienter und gut untersucht sind.

Verschiedene Blockchain-Systeme erlauben den Einsatz von Smart Contracts, die die manipulationssichere Abwicklung von Verträgen zwischen einander unbekannten oder misstrauenden Partnern ermöglichen sollen. Jedoch sind Smart Contracts nicht mit juristischen Verträgen gleichzusetzen, und nicht jeder Vertragsinhalt lässt sich überhaupt durch einen Smart Contract darstellen. Außerdem haben Analysen existierender Contracts eine große Zahl von Sicherheitsproblemen aufgedeckt. Sie reichen von Fehlern im Code – die technologiebedingt nicht korrigiert werden können – über manipulierbare Zufallszahlen bis hin zu fehlender Authentizität der Daten, die, aus der realen Welt kommend, im Contract verarbeitet werden. Diese Einschränkungen und Schwachstellen zu berücksichtigen ist für einen verantwortungsbewussten Umgang mit Smart Contracts unerlässlich.

Da die Sicherheit von Blockchains in starkem Maße auf den verwendeten kryptografischen Algorithmen basiert, müssen diese sorgfältig ausgewählt werden, um das angestrebte Sicherheitsniveau hinsichtlich der Schutzziele Integrität, Authentizität und Vertraulichkeit zu erreichen. Darüber hinaus ist es unabdingbar, die ausgewählten Algorithmen sicher zu implementieren sowie die von ihnen genutzten Schlüssel sicher zu erzeugen und zu verwalten. Detaillierte Empfehlungen hierzu finden sich in den im Dokument referenzierten Technischen Richtlinien des BSI.

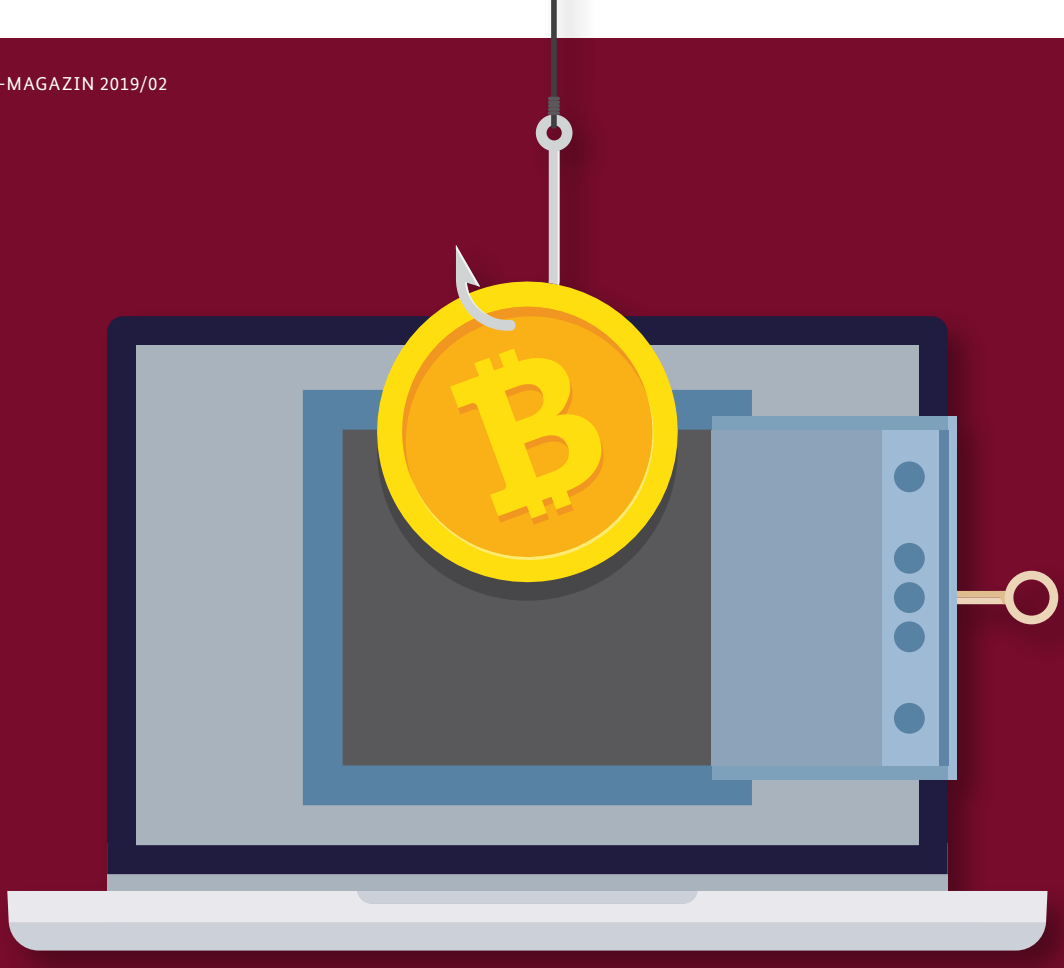
Ein wenig beachteter Aspekt ist die Langzeitsicherheit von Blockchain-Anwendungen. Um sensible Daten in einer Blockchain langfristig zu schützen, müssen Maßnahmen zur Verfügung stehen, die den Austausch kryptografischer Algorithmen ermöglichen, etwa weil deren Sicherheitseignung abgelaufen ist oder abzulaufen droht. Dabei ist unbedingt zu beachten, dass ein Austausch von kryptografischen Verfahren nicht automatisch die ursprünglichen Sicherheitsgarantien für ältere Daten erhält. Neben den kryptografischen Verfahren müssen auch die Sicherheitseigenschaften der Konsensmechanismen klar verstanden und berücksichtigt werden. Diese Aspekte sollten für Blockchain-Anwendungen von Anfang an bedacht werden.

Die rechtlichen Fragestellungen im Zusammenhang mit Blockchains resultieren unter anderem daraus, dass es keine zentrale rechtlich verantwortliche Stelle im Regelbetrieb gibt. Daraus ergeben sich vielfältige Implikationen. Dieses Thema wird gegenwärtig kontrovers diskutiert. Auch datenschutzrechtliche Probleme, wie die Umsetzung von Vorgaben der Datenschutz-Grundverordnung (DSGVO), resultieren aus der auf Blockchains gerade erwünschten Transparenz und Manipulationssicherheit und sind ebenfalls Gegenstand intensiver Beschäftigung. Eine weitere Herausforderung bilden illegale und möglicherweise verschlüsselt abgelegte Inhalte in der Blockchain.

ZUKÜNFTIGE ENTWICKLUNGEN

An Lösungen für eine ganze Bandbreite technischer Beschränkungen und Probleme der Blockchain-Technologie wird ausgiebig und kreativ geforscht. Zu den aktuellen Forschungsthemen gehören beispielsweise die Aspekte Skalierbarkeit, Effizienz, Pseudonymität und Vertraulichkeit. Ob und wann sich hier signifikante Verbesserungen ergeben werden, die über den jetzigen Stand der Technologie hinausgehen, kann gegenwärtig nicht eingeschätzt werden. Ein weiterer erwähnenswerter Punkt sind fehlende Standards im Bereich Blockchain. Dies führt zur Inkompatibilität verschiedener Blockchains und zu einer relativ unübersichtlichen Fülle an Lösungen, die die Auswahl eines konkreten Produkts für einen längerfristigen Zeithorizont für Anwender schwierig macht. ■

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



Angriff auf den Bitcoin

von Sandra Häberer, Referat IT-Sicherheits-Lagebild

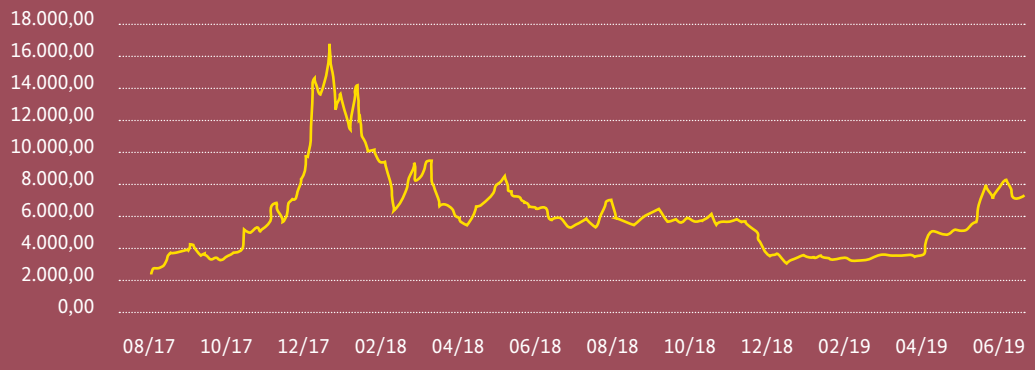
Als Bitcoin vor rund elf Jahren lanciert wurde, träumten die Anhänger digitaler Währungen von einem neuen Zahlungsmittel als Alternative zu Bargeld oder Kreditkarten. Spätestens als 2017 der starke Kursanstieg des Bitcoins von 900 auf 13.000 Euro einen Cyber-Angriff wirtschaftlich interessant machte, witterten auch Kriminelle eine große Chance. Der nachfolgende Artikel beleuchtet die verschiedenen Bedrohungsszenarien für Kryptowährungen und skizziert mögliche Abwehraktivitäten.

KRYPTOWÄHRUNGEN

Als Kryptowährung wird ein digitales Zahlungsmittel bezeichnet, bei dem Verschlüsselung essenzieller Bestandteil des Transaktionsmechanismus ist. Die erste Kryptowährung auf Grundlage einer Blockchain ist Bitcoin. Die Konzeption von Bitcoin wurde im Oktober 2008 unter dem Pseudonym Satoshi Nakamoto veröffentlicht. Seither sind viele Kryptowährungen entstanden, die auf dem Prinzip der Distributed Ledger Technologie (DLT) beruhen. Darunter versteht man ein gemeinsames Kontobuch in einer verteilten Datenhaltung. Es handelt sich um ein dezentrales Konzept verbindlicher Datenspeicherung, bei dem mehrere Transaktionsinformationen in Blöcken zusammengefasst und durch Verschlüsselung und gegenseitige Referenzen chronologisch verbunden werden.

Der Mechanismus, um Transaktionen zu validieren (Proof of Work) beinhaltet eine rechenintensive Aufgabe, die von vielen Teilnehmern konkurrierend gelöst wird und deren Lösung mit Bitcoins entlohnt wird (Mining-Reward). In Anlehnung an die Goldgräberei wird die Validierung von Transaktionen Mining genannt. Welcher Netzknoten der Blockchain dabei zuerst einen gültigen neuen Block hinzufügt und die Belohnung erhält, ist auch vom Zufall ab-

ENTWICKLUNG DES BITCOIN-KURSES



hängig. Durch eine errechnete Prüfsumme (Hash) des neuen Blocks kann schnell überprüft werden, ob die Aufgabe korrekt gelöst wurde und der Block akzeptiert wird.

ANGRIFFE IM MINING-PROZESS

Der Konsens-Mechanismus Proof-of-Work kann offensichtlich z. B. dadurch angegriffen werden, dass ein Angreifer mehr als die Hälfte der Rechenleistung des Netzwerks unter seine Kontrolle bringt. Er verfügt dann beim Mining über eine größere Erfolgswahrscheinlichkeit als der Rest des Netzwerks. Somit wird die von ihm erzeugte Kette der Blöcke nach einer gewissen Zeit länger sein als die der übrigen Knoten und gemäß dem Bitcoin-Protokoll von allen übernommen werden.

Die praktische Durchführbarkeit von 51-Prozent-Angriffen hängt von den finanziellen Ressourcen des Angreifers ab. Schätzungen zeigen, dass länger andauernde 51-Prozent-Angriffe für kleinere Kryptowährungen nur wenige Hundert oder Tausend US-Dollar kosten würden. Die reinen Stromkosten für einen 51-Prozent-Angriff auf Bitcoin werden auf rund 500.000 US-Dollar geschätzt.

Das Selfish-Mining konzentriert sich auf das Anreizsystem des Proof-of-Work. Dabei veröffentlicht der Angreifer neu gefundene Blöcke erst mit deutlicher Verzögerung. Da die übrigen Knoten die vom Angreifer zurückgehaltenen Blöcke nicht kennen, vergeuden sie Rechenleistung, schließen sich aus ökonomischen Gründen der Kette des Angreifers an, wodurch eine Manipulation durch erhöhte Rechenkapazitäten möglich wird. Für einen erfolgreichen Selfish-Mining-Angriff sind lediglich mehr als 25 Prozent der Gesamtrechenleistung erforderlich.

Um einen 51-Prozent-Angriff durchzuführen, ohne tatsächlich über diesen Anteil an der Gesamtrechenleistung zu verfügen, gibt es zudem noch weitere Strategien. Mehrfach beobachtet wurde ein DDoS-Angriff auf einen relevanten Netzwerkknoten. Denkbar ist auch, Malware zu platzieren, die die Funktion des Mining-Knotens unterbindet oder übernimmt. Weiterhin kann durch eine gezielte Manipulation von Netzwerkinformationen ein Miner vom Netzwerk abgeschnitten werden (Eclipse-Angriff).

DIEBSTAHL VON KRYPTOWÄHRUNGEN

Wer den privaten Schlüssel eines Bitcoin-Besitzers erlangt, kann dessen Coins an einen Angreifer übertragen. Zum Beispiel erfolgt dies, wie beim Online-Banking, indem Malware platziert wird. Solche Angriffe können sich nicht nur gegen einzelne Bitcoin-Besitzer, sondern auch gegen den Betreiber einer Kryptobörse richten. Der Vorfall mit der höchsten Schadenssumme in diesem Segment, bei dem NEM-Coins in einem Gegenwert von 532 Millionen US-Dollar von 260.000 Konten gestohlen wurden, betraf die Handelsplattform Coincheck. Möglich ist auch die Manipulation des öffentlichen Schlüssels, an den beispielsweise im Gegenzug zu einer Dienstleistung Gelder überwiesen werden. Dies geschieht in der Regel durch die Kompromittierung einer Webseite.

GEGENMASSNAHMEN

Die Erkenntnisse aus diesen Bedrohungsszenarien sind in die BSI-Publikation „Blockchain sicher gestalten. Konzepte, Anforderungen, Bewertungen“ eingeflossen. Sie beleuchtet die Blockchain-Technologie in ihren unterschiedlichen Ausgestaltungen ebenso wie grundsätzliche Sicherheitsfragen sowie die Fragen nach der Sicherheit der kryptografischen Algorithmen.

Konventionellen Angriffen, wie der Kompromittierung der Schlüssel oder der Störung eines Mining-Netzwerkes durch Schadsoftware oder DDoS-Angriffe, kann mit konventionellen Abwehrmaßnahmen begegnet werden, die auch das BSI in seinen vielfältigen Angeboten für Staat, Wirtschaft und Gesellschaft empfiehlt. ■

DAS BSI

„Wir sind da, wo Innovation stattfindet“

BSI als Exzellenzbehörde mit zweitem Standort in Freital/Sachsen

von Josephine Steffen, Strategische Kommunikation und Presse

Am 11. Juli 2019 unterzeichneten Bundesinnenminister Horst Seehofer und der sächsische Innenminister Prof. Roland Wöller im Rathaus von Freital in Sachsen eine Gemeinsame Absichtserklärung zur Schaffung eines zweiten Standortes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Freital. Damit baut das BSI seine Präsenz in der Fläche weiter aus, um insbesondere mit Ländern, Kommunen und der Wirtschaft vor Ort noch besser zusammenarbeiten zu können.

BSI-Präsident Arne Schönbohm, Bundesinnenminister Horst Seehofer, Prof. Dr. Roland Wöller (Staatsminister des Innern, Sachsen)

Nur wenige Kilometer von Dresdens Innenstadt entfernt befindet sich die Große Kreisstadt Freital. Zwischen Elbtal und Osterzgebirge ist die Stadt mit 40.000 EinwohnerInnen nicht nur wunderschön gelegen, sondern sie ist auch nur einen Katzensprung vom „Silicon Saxony“ im Großraum Dresden entfernt.

Sachsen ist einer der wichtigsten Standorte im Bereich der Halbleitertechnik und Mikroelektronik in Deutschland und Europa. Bereits in der DDR wurde im heutigen Chemnitz der Großrechner Robotron 300 entwickelt und gebaut. Unternehmen wie Infineon, zahlreiche Fraunhofer-Institute und die TU Dresden machen den Wirtschaftsraum Sachsen zu einem der innovativsten in Deutschland. Die Technische Universität Dresden ist erst im Juli 2019 erneut zur Exzellenzuniversität mit einer jährlichen Förderung von 15 Millionen Euro ernannt worden. Viele internationale WissenschaftlerInnen und StudentInnen kommen in den Großraum Dresden, um dort zu lehren, zu forschen, zu studieren und zu arbeiten.

Von dieser kreativen und pulsierenden Umgebung profitiert in Zukunft auch das BSI. Auf der Pressekonferenz anlässlich des Startschusses für den Standort Freital sagte der Bundesminister des Innern, für Bau und Heimat, Horst Seehofer: „Wir unternehmen große Anstrengungen als Bundesrepublik

(von links nach rechts): Prof. Dr. Roland Wöller, Horst Seehofer, Uwe Rumberg (Oberbürgermeister der Großen Kreisstadt Freital), Arne Schönbohm, Kati Hille (Vize-Landrätin des Landkreis Sächsische Schweiz-Osterzgebirge)

Arne Schönbohm, Horst Seehofer, Prof. Dr. Roland Wöller, Uwe Rumberg, Kati Hille

Deutschland, um eines der Zukunftsthemen – die Cyber-Sicherheit – für die Menschen und die Wirtschaft in diesem Land sicherzustellen. Cyber-Sicherheit ist ein großes Thema für die Gegenwart und noch ein größeres für die Zukunft. Wir haben uns als Bundesregierung überlegt, ob der Standort Bonn des BSI ausreicht, und sind zu dem Schluss gekommen, dass mehrere Stützpunkte in Deutschland sinnvoll sein können. Deshalb gründen wir heute diese größere Exzellenzbehörde mit 200 Beschäftigten hier in Freital."

Arne Schönbohm, Präsident des BSI, bekräftigte: „Wir sind gekommen, um zu bleiben. Das BSI als Thought Leader im Bereich der Cyber-Sicherheit ist wie ein Baum: Der große starke Stamm ist in Bonn. Wenn wir aber verstehen wollen, wie Digitalisierung und neue Technologie funktionieren, dann brauchen wir ein starkes Wurzelwerk. Deshalb müssen wir dahin gehen, wo die Innovationen und neue Technologien stattfinden, und das ist im Bereich Mikroelektronik der Raum Dresden. Deshalb ist Freital für uns ein geeigneter Standort. Wir können hier frühzeitig erkennen, was die neuen Technologietrends sind."

Mit dem Zweitsitz in Freital, so der Staatsminister des Innern des Freistaates Sachsen, Prof. Dr. Roland Wöller, „werden die Abwehrkräfte im Cyber-Raum gebündelt. Das wird dem Bund guttun und dem Freistaat Sachsen. Wir schaffen einerseits hochwertige Arbeitsplätze und erwarten andererseits wichtige Impulse für die Cyber-Sicherheit von Behörden und Unternehmen im Freistaat. Dabei bauen wir insbesondere auch auf die vorhandene Expertise beim Bundesamt."

Die Arbeiten zur Errichtung des BSI-Standorts Freital laufen auf Hochtouren. So schnell wie möglich soll neben der bereits bestehenden BSI-Verbindungsstelle in den Räumlichkeiten der Sächsischen Staatskanzlei in Dresden eine Liegenschaft in Freital in Betrieb genommen werden. Bis Ende 2019 sollen die ersten Mitarbeiterinnen und Mitarbeiter des BSI in Freital beschäftigt sein, bis Ende 2020 soll der Aufwuchs auf rund 200 Arbeitskräfte erfolgen. Dafür wird das BSI in der Region mit Lehreinrichtungen, Unternehmen und Behörden in Kontakt treten, um Synergien und gemeinsame Ziele für eine vernetzte Zusammenarbeit zu nutzen.

Horst Seehofer und Prof. Dr. Roland Wöller

Das BSI ist eine tragende Säule der Sicherheitsarchitektur Deutschlands und zentraler Ansprechpartner zur Cyber-Sicherheit für Staat, Wirtschaft und Gesellschaft in Deutschland. Der jahrzehntelange Aufbau und die Bündelung von Know-how sowie die Kompetenz im Bereich der Cyber-Sicherheit haben das BSI zu einer Behörde gemacht, in der die Fäden der Cyber-Sicherheit zusammenlaufen. Das BSI bietet eine effiziente integrierte Wertschöpfungskette der Cyber-Sicherheit mit dem Ziel, die Digitalisierung so zu gestalten, dass BürgerInnen, Unternehmen und Verwaltung von diesen Vorteilen profitieren und die Risiken eindämmen können. „Cyber-Sicherheit muss das Qualitätsmerkmal von „Made in Germany" sein. Das wird uns in Zukunft von anderen Playern auf dem Markt nachhaltig unterscheiden", so Schönbohm.

Befragt nach dem inhaltlichen Schwerpunkt des Zweitsitzes des BSI, sagt Arne Schönbohm: „Die endgültigen Schwerpunkte stehen noch nicht fest. Angedacht sind Aufgaben mit Bezug zu Zukunftstechnologien wie zum Beispiel sichere 5G-Infrastrukturen oder eID-Technologien. Wir werden von hier aus massiv das Thema „Beschleunigte Sicherheitszertifizierung" angehen, damit die Sicherheit der Innovationskraft der Wirtschaft in nichts nachsteht. Hinzu kommen Ableger unserer Servicebereiche. So können zukünftig auch unsere IT-Sicherheitsberatung oder unsere Penetrationstester vor Ort regional agieren. Weiterhin wird erwogen, ein Ausweich-Lagezentrum des BSI am Standort Freital georedundant aufzustellen." ■

Cyberfibel

Ein Standardwerk zur Orientierung in der digitalen Aufklärungsarbeit

von Karin Wilhelm, Referat Cyber-Sicherheit für den Bürger und Dr. Michael Littger, Deutschland sicher im Netz e. V.

Was müssen Verbraucher und Verbraucherinnen wissen, um sich sicher und selbstbestimmt in der digitalen Welt bewegen zu können? Welche Maßnahmen gehören zum Basisschutz? Welche Verhaltensweisen sind ratsam? Ende 2019 erscheint die Cyberfibel, eine Publikation, die Wissensvermittlern und Wissensvermittlerinnen eine Orientierung in der Aufklärungsarbeit gibt.

Als nationale Cyber-Sicherheitsbehörde verfolgt das BSI das Ziel, Bürgerinnen und Bürger bei der sicheren und selbstbestimmten Nutzung digitaler Geräte und Dienste zu unterstützen. Deswegen stellt es Handlungsempfehlungen und Hintergrundinformationen mit dem Webangebot „BSI für Bürger“ zur Verfügung. Dieses richtet sich jedoch in erster Linie direkt an Privatanwender und -anwenderinnen. Vereine, Stiftungen, Bildungseinrichtungen, Volkshochschulen oder Verbände, die sich in der Verbraucherbildung und -aufklärung engagieren, benötigen jedoch eine Orientierungshilfe, wie sie Inhalte vermitteln und welche sicherheitsrelevanten Empfehlungen sie geben sollen.

Aus diesem Grund haben das BSI und der Verein Deutschland sicher im Netz (DsiN) das gemeinsame Angebot Cyberfibel ins Leben gerufen. Dahinter steht die Idee, die grundlegenden Schutzkompetenzen für Multiplikatorinnen und Multiplikatoren verständlich aufzubereiten. Das Handbuch wird in einer digitalen und einer gedruckten Version erscheinen und richtet sich an alle, die in ihrer Arbeit oder in ihrem Ehrenamt Seminare, Arbeitsgruppen oder Workshops für unterschiedliche Zielgruppen zur Cyber-Sicherheit durchführen.

EIN LEBENDIGES HANDBUCH IM ALLTAGSGEBRAUCH

In der Cyberfibel fassen BSI und DsiN zahlreiche Basisinformationen als Rüstzeug für selbstbestimmtes und sicheres Handeln in der digitalen Welt zusammen. Im Zentrum steht die sichere Nutzung von Geräten wie PC, Laptop, Smartphones oder internetfähigen Fernsehapparaten. Aber auch E-Mail-Anbieter und Social-Media-Plattformen werden thematisiert.

Die Publikation ist in zwei Bereiche aufgeteilt: Im ersten Teil finden Multiplikatorinnen und Multiplikatoren über alltägliche Anwendungen aus ihren Lebenswelten Zugang zum Thema. Zudem erhalten sie methodische Hinweise und Aufgabenstellungen, die sie für ihre Vermittlungsarbeit nutzen können. Im zweiten Teil wird erklärt, wie und vor welchen Gefahren sich jeder Einzelne schützen kann. Informationen zu Funktionsweisen von Geräten und Online-Diensten ergänzen die Empfehlungen. Weiterführende Links unter jedem Kapitel ermöglichen eine vertiefte Recherche.

Zum Jahreskongress des Vereins Deutschland sicher im Netz (DsiN) am 3. Juni 2019 stellte BSI-Präsident Arne Schönbohm (2. v. r.) mit Staassekretär Klaus Vitt (2. v. l.) und DSiN-Geschäftsführer Michael Littger (ganz rechts) die zukünftige Publikation „Cyberfibel“ vor.

Die beiden Partner BSI und DsiN verstehen die Cyberfibel als ein dynamisches, wachsendes Handbuch. Aktuelle Entwicklungen werden regelmäßig eingearbeitet, Themen, die an Bedeutung gewinnen, ergänzt. Zudem arbeiteten die Beteiligten bei der Erstellung der Inhalte eng zusammen. Eine erste Kurzfassung wurde zum DsiN-Jahreskongress im Juni 2019 vorgestellt und im Plenum diskutiert. Weiteres Feedback zu Aufbau und Struktur wurde von Partnern aus Zivilgesellschaft, Wirtschaft und Wissenschaft eingeholt. Dazu zählen das Bundesnetzwerk Bürgerschaftliches Engagement (BBE), das Deutsche Rote Kreuz e. V. (DRK), eBay Kleinanzeigen GmbH, Kaspersky Labs GmbH, Samsung Electronics GmbH, Die Verbraucher Initiative e. V. (Bundesverband) und die Verimi GmbH. Diese sind Teil des Deutschland Dialog für Aufklärung, in dessen Rahmen die Cyberfibel entstanden ist. Das Format wird von DsiN koordiniert und das BSI ist Teil des Lenkungsausschusses. ■

Die Cyberfibel ist ab Winter 2019 kostenfrei bundesweit verfügbar. Es gibt sowohl eine digitale als auch eine gedruckte Version. Vorbestellungen sind möglich unter **info@cyberfibel.de**

Weitere Informationen unter **www.cyberfibel.de**

Eröffnung der Verbindungsstelle in Stuttgart: BSI-Präsident Arne Schönbohm, Beate Bube, Präsidentin des Landesamts für Verfassungsschutz Baden-Württemberg und Thomas Strobl, Stellv. Ministerpräsident des Landes Baden-Württtemberg

In Nord und Süd, in Ost und West

Das Nationale Verbindungswesen bringt das BSI in die Fläche

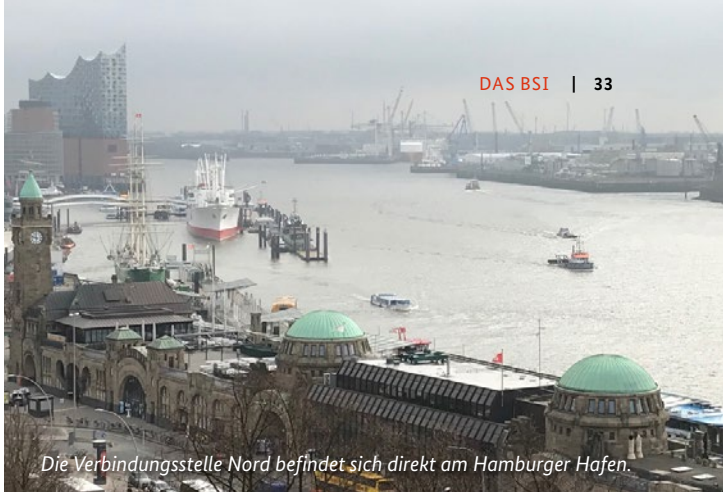
von Ariane Steinke und Philipp Gebhard, Referat Nationales Verbindungswesen

Im Februar 2019 hat das BSI zwei seiner insgesamt sechs Verbindungsstellen in Hamburg und Stuttgart eröffnet. Diese beiden Stellen sind zuständig für insgesamt acht Bundesländer. Prominente Referenten und Gäste unterstrichen den Stellenwert dieser Eröffnungen für das BSI, die Länder und die Wirtschaft der jeweiligen Regionen.

PRÄSENZ IN DER FLÄCHE

Mit den Verbindungsstellen in Hamburg und Stuttgart wird das BSI durch direkte Ansprechpartnerinnen und -partner in der Fläche besser erreichbar. Dadurch kann es seine Aufgaben stärker wahrnehmen mit dem Ziel, das Cyber-Sicherheitsniveau in Deutschland in Gänze zu erhöhen. Die erste Verbindungsstelle wurde bereits 2017 in den Räumlichkeiten des Bundeskriminalamts in Wiesbaden


Gut besuchte Eröffnungsveranstaltung in Hamburg


Die Verbindungsstelle Nord befindet sich direkt am Hamburger Hafen.

Eröffnung der Verbindungsstelle in Stuttgart

gegründet und ist für die Region Rhein-Main zuständig. Hamburg und Stuttgart sind nun zwei weitere Stationen der regionalen Diversifizierung. Im Rahmen seiner Veranstaltungsreihe „BSI im Dialog“ begrüßte das BSI zu den Eröffnungen jeweils rund 70 geladene Gäste aus Politik, Wirtschaft, Gesellschaft und Wissenschaft. Die Eröffnungsreden in Hamburg wurden vom Staatssekretär für Inneres und Sport des Landes Niedersachsens, Stephan Manke, und dem Chief Digital Officer der Freien und Hansestadt Hamburg, Christian Pfromm, gehalten. Als weiterer Gastredner konnte Norbert Wetter, Mitglied des Vorstands des Deutschen Wetterdienstes, begrüßt werden. Die Verbindungsstelle in Stuttgart wurde durch Thomas Strobl, den stellvertretenden Ministerpräsidenten des Landes Baden-Württemberg, eröffnet.

Bei einem Arbeitsfrühstück wurde über Ansätze zur Erhöhung des Cyber-Sicherheitsniveaus in den Bundesländern diskutiert. Die Teilnehmer hatten so die Möglichkeit, sich über vorhandenes Wissen, Erfahrungen und Ideen auszutauschen. Zusätzlich wurden die Angebote des Nationalen Verbindungswesens vorgestellt und Modelle zur Stärkung der regionalen Kooperation und Vernetzung beleuchtet.

HINTERGRUND

Das BSI hat in den zurückliegenden Jahren neue Zuständigkeiten erhalten. Dazu zählt auf Grundlage des Gesetzes zur Umsetzung der EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-RL) die Zusammenarbeit zwischen den Bundesländern und dem BSI zu stärken. Danach kann das BSI nunmehr zuständige Stellen der Länder auf deren Ersuchen in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik unterstützen und technische Expertise zur Verfügung stellen. Vor diesem Hintergrund wird die Beratung der Bundesländer und der Wirtschaft einschließlich der kleineren und mittleren Unternehmen (KMU) ausgebaut.

Auch der Aufbau des Nationalen Verbindungswesens des BSI seit 2016 ist in diesem Kontext zu sehen. Es hat den Auftrag, als zentrale Ansprechstelle zu allen Belangen der IT-Sicherheit zur Verfügung zu stehen und dem BSI vor Ort ein Gesicht zu geben. Inzwischen ist das als Pilotprojekt gestartete Nationale Verbindungswesen auf sechs Verbindungsstellen mit Verbindungspersonen in den Regionen Nord, Berlin, Ost, Süd, West sowie Rhein-Main angewachsen. Diese Entwicklung zeigt die Notwendigkeit und den Erfolg des Konzepts einer zentralen Ansprechstelle der nationalen Cyber-Sicherheitsbehörde in der Fläche. Die Verbindungspersonen sind jeweils für eine bestimmte Region in der Bundesrepublik zuständig. So ist es dem Verbindungswesen möglich, einen engen Kontakt in die Regionen aufzubauen und besser auf die spezifischen Bedarfe und Interessen der jeweiligen Zielgruppen einzugehen. Aber auch das BSI wird über diese Vor-Ort-Präsenz vom Know-how und Input der Bundesländer und der Wirtschaft profitieren. Informationssicherheit kann schließlich nur in einem kooperativen und komplementären Ansatz erreicht werden. ■

Die Verbindungsstellen sind über die E-Mail-Adresse BSIregional@bsi.bund.de erreichbar.

Im Studium zum BSI

Karrierewege für die MINT-Fachkräfte von morgen

von Nicolas Stöcker, Referat Personalgewinnung und -entwicklung

Um allein 2019 mehr als 350 offene Stellen im BSI zu besetzen, muss das BSI alle Kanäle nutzen. Die Fachabteilungen leisten dabei einen wesentlichen Beitrag zur Personalgewinnung. Seit über zehn Jahren binden sie Studierende aus den MINT-Fächern (Mathematik-Informatik-Naturwissenschaften-Technik) frühzeitig durch Studienförderung, Praktika, Abschlussarbeiten und die Beschäftigung als studentische Hilfskräfte. Das BSI übernimmt hier eine Vorreiterrolle für den öffentlichen Dienst und setzt durch die Erfolge dieses Angebots Maßstäbe.

Unmittelbar nach seinem Abitur im Jahr 2016 begann für Julian Bamberg-Siebert die Studienförderung beim BSI. Ein Studium mit Praxisbezug und gute Perspektiven waren dabei die ausschlaggebenden Kriterien: „Die Förderung vereint die Vorteile des dualen Studiums mit denen eines ‚normalen' Studiums. Die Vielfältigkeit des BSI hat mich gereizt, da man sich nicht direkt bei Studienbeginn festlegen muss, in welche Richtung man später gehen will."

Die Studienförderung beinhaltet ein Vollzeitstudium der Informatik an der Hochschule Bonn-Rhein-Sieg (HBRS), das mit einer monatlichen finanziellen Förderung unterstützt wird. In den Semesterferien finden kurze Praktika statt. Zum Ende erwartet die Studierenden dann ein Praxissemester und die Bachelorarbeit im BSI, so auch Bamberg-Siebert: „In meinem Praxissemester und meiner Bachelorarbeit analysiere ich Schadsoftware. Dabei werde ich vor allem in die Richtung Statistik und Clustering gehen."

Nach dem Abschluss seines Bachelorstudiums erwartet den jungen Informatiker eine unbefristete Übernahme in das Team, das sich mit der Detektion von Cyber-Angriffen beschäftigt. Wie schon viele Kollegen und Kolleginnen vor ihm, will er mit einem berufsbegleitenden Masterstudium seine Karriere im BSI fortsetzen.

Einen anderen Weg zum BSI wählte Yannick Keuler. Nach einem kurzen Studium der Chemie entschied er sich für den Wechsel in die Informatik, ebenfalls an der HBRS, was ihn schon bald mit der Behörde in Kontakt brachte: „Viele Lehrveranstaltungen in der IT-Sicherheit werden von Beschäftigten des BSI gehalten und auf der Hochschulmesse konnte ich mich aus erster Hand informieren. Ich habe dann mein Praxissemester hier geleistet und mich anschließend erfolgreich auf eine Stelle beworben."

Zu seinen Aufgaben gehört nun die Überprüfung der Betreiber Kritischer Infrastrukturen, die laut Gesetz alle

STUDIENGANG DIGITAL ADMINISTRATION AND CYBER-SECURITY (DACS)

In Kooperation mit dem BSI will die Hochschule des Bundes für öffentliche Verwaltung (HS Bund) zum Wintersemester 2020/2021 einen neuen Studiengang „Digital Administration and Cyber-Security" (DACS) etablieren. Er ist als Vorbereitungsdienst für die Laufbahn des gehobenen Dienstes eingestuft. Inhaltlicher Schwerpunkt wird neben der Digitalisierung der Verwaltung die sichere Gestaltung von IT-Systemen und Netzwerken sein. Zusätzlich sollen zwei sechsmonatige Praxisabschnitte die Studierenden auf die Herausforderungen in der IT der Bundesverwaltung vorbereiten.

Bewerbungsmöglichkeiten und weitere Informationen werden auf der Webseite des BSI veröffentlicht.

PRAKTIKA UND ABSCHLUSSARBEITEN IM BSI

Das BSI bietet Studierenden freiwillige und Pflichtpraktika an. Der Einsatz erfolgt für mindestens zehn Wochen in einem der Fachgebiete der Behörde. Ferner ist die Betreuung von Abschlussarbeiten möglich, auch in Kombination mit einem Praxisprojekt. Eine frühzeitige Bewerbung ist erforderlich, da auch die Studierenden eine Sicherheitsüberprüfung durchlaufen müssen.

zwei Jahre nachweisen müssen, angemessene Vorsorge in der IT-Sicherheit getroffen zu haben. Zusätzlich wird er derzeit in die Sektorbetreuung für die Branchen Mineralöl und Gas eingearbeitet, wodurch er auch an der Erstellung branchenspezifischer Sicherheitsstandards beteiligt ist.

Seine weitere Laufbahn hat Keuler ebenfalls schon geplant: „Ich arbeite in Teilzeit und mache nebenher noch meinen Master an einer Fernuniversität. Im Mai 2020 möchte ich mich gerne verbeamten lassen und werde mich nach Abschluss meines zweiten Studiums auf eine Stelle im höheren Dienst bewerben – dann wieder in Vollzeit."

Bereits zwei Stationen in ihrer noch jungen Karriere kann Karla Beckert vorweisen: Nachdem sie 2017 zunächst als Werkstudentin im Bereich „Internationale Beziehungen" begann, wechselte sie Anfang 2019 in das Aufgabengebiet „Entwicklung von Detektoren und SOC-Automatisierung". Dort recherchiert und evaluiert sie neue Detektionsmechanismen, um Cyber-Angriffe zu erkennen.

An ungefähr zwölf Stunden in der Woche ist Beckert in der Behörde zu finden – den Rest der Zeit widmet sie sich ihrem Master in Computer Science an der Universität Bonn. Die Frage nach ihrer Zukunft lässt sie noch offen: „Genaue Vorstellungen für die Zeit nach meinem Abschluss habe ich noch nicht. Da meine Interessenschwerpunkte aber derzeit in der IT-Sicherheit und Maschinellem Lernen liegen, hoffe ich, dass ich auch nach meinem Abschluss weiterhin in diesen Bereichen tätig sein kann." ■

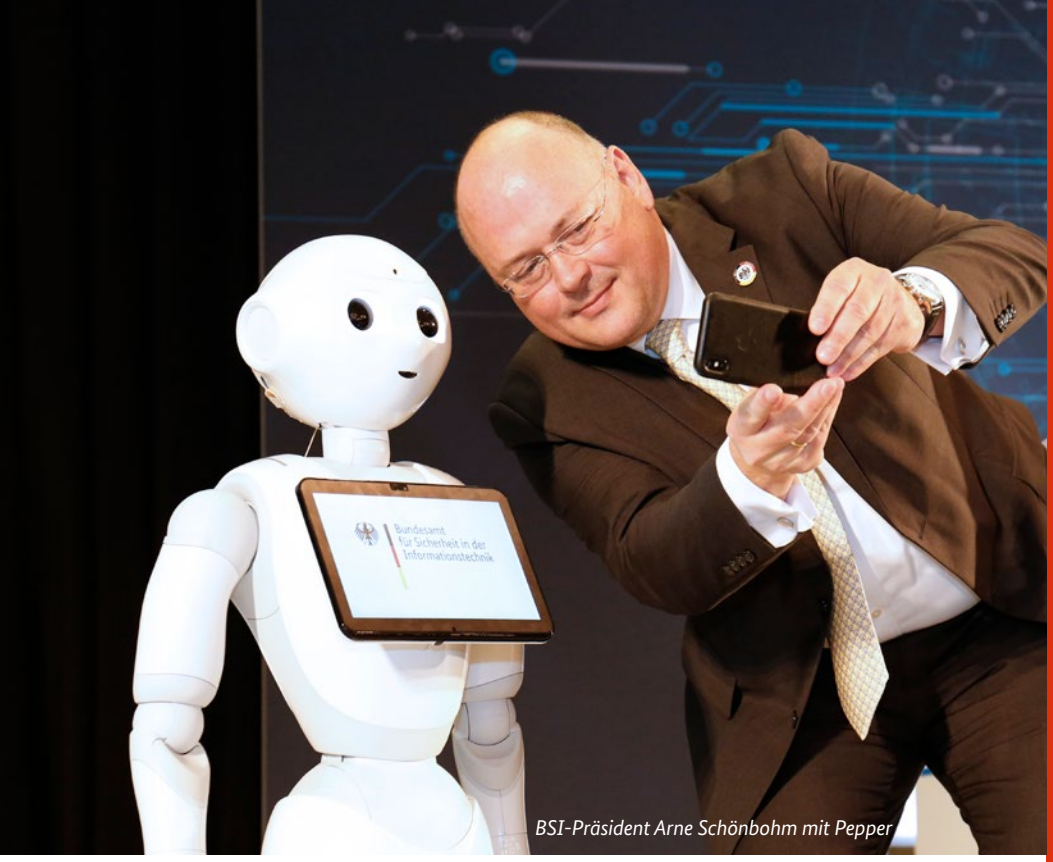
Weiterführende Informationen zu studentischen Karrierewegen im BSI: https://www.bsi.bund.de/studierende

Künstliche Intelligenz und sichere Digitalisierung

Rückblick auf den 16. Deutschen IT-Sicherheitskongress

Parlamentarischer Staatssekretär Prof. Dr. Günter Krings

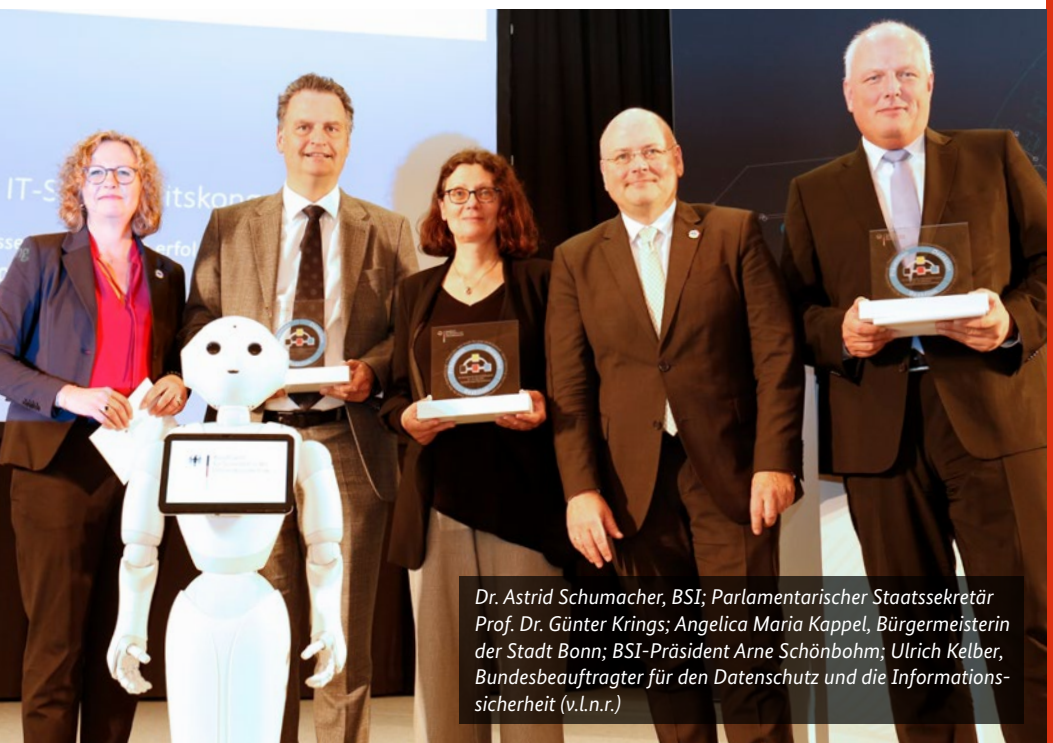
Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit



BSI-Präsident Arne Schönbohm mit Pepper


Dr. Stefan Mück, IBM


Guillaume Poupard, ANSSI


Dr. Astrid Schumacher, BSI; Parlamentarischer Staatssekretär Prof. Dr. Günter Krings; Angelica Maria Kappel, Bürgermeisterin der Stadt Bonn; BSI-Präsident Arne Schönbohm; Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationssicherheit (v.l.n.r.)

Zunehmend professionelle Cyber-Angriffe, steigende smarte Vernetzung und wachsende Abhängigkeit von funktionierenden IT-Systemen führen uns täglich vor Augen: Cyber-Sicherheit ist die Voraussetzung einer erfolgreichen Digitalisierung. Wie neue Technologien und Lösungen zur sicheren Gestaltung des digitalen Zeitalters in Staat, Wirtschaft und Gesellschaft eingesetzt werden können, diskutierte das BSI während des 16. Deutschen IT-Sicherheitskongresses mit über 700 Teilnehmerinnen und Teilnehmern in Bonn-Bad Godesberg.

Das abwechslungsreiche Kongressprogramm umfasste 48 Fachvorträge, fünf Keynotes und zwei Paneldiskussionen. Dabei standen Technologien wie 5G, Blockchain oder Post-Quanten-Kryptografie ebenso im Fokus wie neue Trends für mehr Sicherheit im Internet der Dinge, im Smart Home oder in Industriesteuerungssystemen.

Ein international besetztes Podium diskutierte über die weltweite Notwendigkeit von „Supply Chain Security in Digitalisation“. Die Diskussion und die anschließende Präsentation des deutsch-französischen Lagebilds verdeutlichen, dass Informationssicherheit ein internationales Anliegen ist, das von einer staatenübergreifenden Kooperation profitiert.

Bei einer weiteren Podiumsdiskussion tauschten sich Cyber-Expertinnen und -Experten über die Auswirkungen von Künstlicher Intelligenz (KI) auf die IT-Sicherheit aus. Neben der bereits gut funktionierenden Prognosefähigkeit sahen sie eine besondere Herausforderung in der Nachvollziehbarkeit sowie Überprüfbarkeit der Algorithmen der KI.

Abgerundet wurde der Kongress durch eine begleitende Ausstellung mit 23 Ausstellern. ■

SONDERTHEMA

Gut geschützt

Vorwort von Arne Schönbohm

25 Jahre. Das ist im Internetzeitalter fast eine Ewigkeit. Ein Sicherheitskonzept, das über diesen Zeitraum durchgehend „im Einsatz“ war, muss darum ebenso beständig wie wandlungsfähig sein. Der IT-Grundschutz des BSI ist dies. So konnte er zu einem einzigartigen Erfolgsmodell werden und ist aus dem Alltag gelebter Informationssicherheit in Behörden, Institutionen und Unternehmen nicht mehr wegzudenken.

25 Jahre. Durch zunehmende Vernetzung, das Internet der Dinge, die Digitalisierung der Arbeit und eine Client/Server-Architektur sind die Gefährdungen der Informationstechnik in diesem Zeitraum sehr komplex geworden. Herausforderungen wie Digitalisierung, Cyber-Bedrohungen oder Künstliche Intelligenz waren vor 25 Jahren noch nicht absehbar. Der IT-Grundschutz ist seit seinen Anfängen durch kontinuierliche Anpassungen mitgewachsen. Aber er ist einfach machbar geblieben. Denn nur so kann er sein Ziel erreichen: dass Verantwortliche für Informationssicherheit, ob Einsteiger oder Profi, in Behörden und Unternehmen jeder Größenordnung das Sicherheitsniveau realistisch einschätzen und die notwendigen Maßnahmen zur Absicherung umsetzen können.

25 Jahre. In dieser Zeit haben sehr viele Experten und Sicherheitsverantwortliche engagiert und verantwortlich daran mitgewirkt, dass der IT-Grundschutz gleichermaßen aktuell und fundiert den Stand der Technik widerspiegelt. Denn das ist sein Grundprinzip: Die Expertise des BSI als nationale Cyber-Sicherheitsbehörde in Deutschland wird angereichert um die Best-Practices und Erfahrungen von Anwendern aus der Unternehmens- und Behördenpraxis. Dieser Dialog ist der entscheidende Mehrwert des IT-Grundschutzes.

25 Jahre. Informationssicherheit ist ein Prozess. Der IT-Grundschutz bildet diesen Prozess mit den unterschiedlichsten Angeboten ab und ermöglicht es, durch ein systematisches Vorgehen notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards liefern hierzu bewährte Vorgehensweisen, das IT-Grundschutz-Kompendium konkrete Anforderungen. Es ist mit derzeit 94 IT-Grundschutz-Bausteinen zu den wichtigsten und aktuellen Themen für stabile und robuste Systeme und Netze das Bollwerk gegen jegliche Bedrohungen und Gefährdungen.

25 Jahre. Das ist auch ein Grund, stolz zu sein. Denn ein Angebot ist immer nur so gut wie seine Akzeptanz. Beim IT-Grundschutz wurde aus dem anfänglichen Angebot vor allem für Bundesbehörden, die IT-Systeme abzusichern und zu schützen, mit der Zeit ein immer breiteres Angebot über nahezu alle Zielgruppen und Anwendergruppen hinweg. Und es wurde immer auch von allen neuen Zielgruppen akzeptiert. Heute ist der IT-Grundschutz mehr als ein umfangreiches Portfolio von Maßnahmen und Empfehlungen zur Absicherung für Wirtschaft und Behörden. Es ist ein Referenzsystem, ein gesetzter Standard.

25 Jahre. Das ist auch eine Verpflichtung, nicht stehen zu bleiben. 2017 wurde die IT-Grundschutz-Methodik grundlegend modernisiert. Die Inhalte wurden stärker fokussiert und verschlankt, neue Themen und Aspekte wurden aufgenommen. Speziell für kleine und mittelständische Unternehmen, die meist ein eher begrenztes Budget für Informationssicherheit haben, wurden neue Angebote entwickelt. In Zukunft sollen neue Zielgruppen, auch international, erschlossen werden, neue Angebote sollen sicherstellen, dass der IT-Grundschutz weiterhin für jedes Bedürfnis die passende Lösung liefert.

Mein ausdrücklicher Dank geht daher an alle, die diese 25 Jahre zu einer Erfolgsstory werden ließen.

Konstante in der Informationssicherheit

25 Jahre IT-Grundschutz

von Holger Schildt, Referat BSI-Standards und IT-Grundschutz

Mit seiner Gründung am 1. Januar 1991 nahm das BSI die Informationstechnik in den Fokus und unterstützte zunächst Bundesbehörden bei allen Fragen rund um die IT-Sicherheit. Die Praxis zeigte schnell, dass alle Bundesbehörden von ähnlichen Bedrohungen betroffen waren. Um den individuellen Beratungsbedarf zu verringern, wurde eine Vorgehensweise entwickelt, bei der Anwender die für ihre Anforderungen essenziellen Empfehlungen auswählen und umsetzen konnten. Sie gilt bis heute und bildet das fachliche Fundament des IT-Grundschutzes.

VON DER BEHÖRDENLÖSUNG ZUM STANDARD

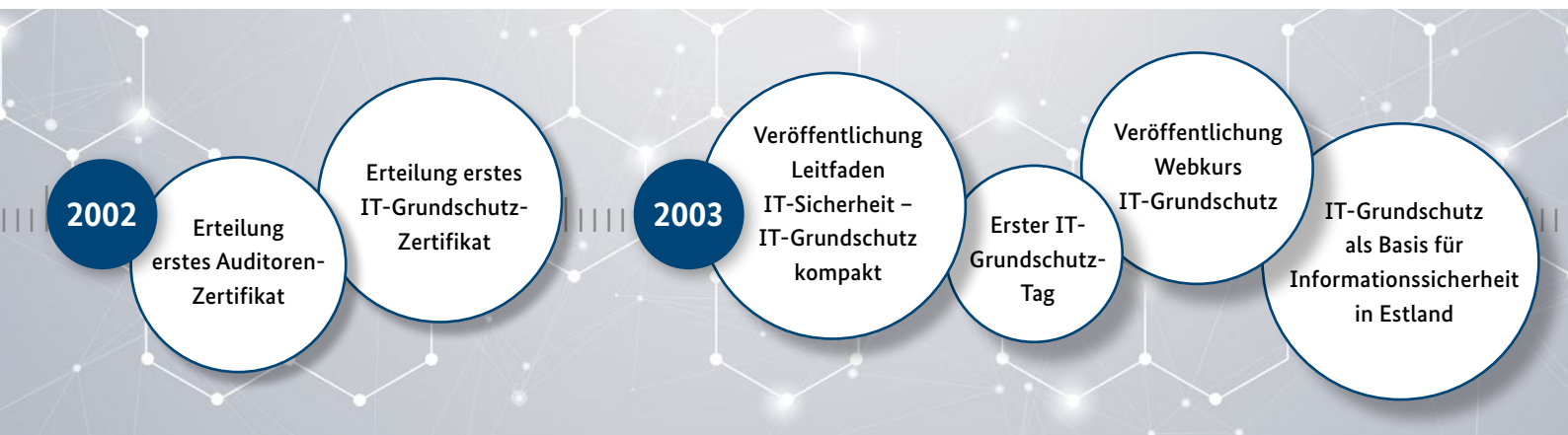
Bereits 1994 wurde die erste Version des IT-Grundschutz-Handbuchs veröffentlicht. Es umfasste die IT-Grundschutz-Vorgehensweise und erste IT-Grundschutz-Bausteine. Das IT-Grundschutz-Handbuch wurde fachlich kontinuierlich weiter ergänzt und erste Anwender aus der Praxis brachten ihre Erfahrungen in die Veröffentlichungen ein. Die erste grundlegende Überarbeitung des IT-Grundschutzes fand 2005 statt: Das IT-Grundschutz-Handbuch wurde in drei BSI-Standards zu unterschiedlichen Themen überführt, die Bausteine wurden in den IT-Grundschutz-Katalogen veröffentlicht. Die BSI-Standards, bestehend aus 100-1: Managementsysteme für Informationssicherheit, 100-2: IT-Grundschutz-Vorgehensweise sowie 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, beschrieben die Kernaspekte des IT-Grundschutzes in einer kompakten Veröffentlichung. Damit konnte sich die IT-Grundschutz-Vorgehensweise als der Standard zur IT-Sicherheit in Deutschland etablieren.

INFORMATIONSSICHERHEIT SICHTBAR MACHEN

Zertifikate und Testate nach IT-Grundschutz boten ab 2002 die Möglichkeit, Informationssicherheit gegenüber Kunden, Dienstleistern und Mitarbeitern nachzuweisen. Ein Zertifikat nach IT-Grundschutz belegt bis heute den hohen Stellenwert der Informationssicherheit in einer Institution. Zudem trug die Kompatibilität zur international weitverbreiteten ISO 27001-Norm dazu bei, dass der IT-Grundschutz zu einem angesehenen Standard in der Informationssicherheit wurde.

DYNAMISCHE ENTWICKLUNGEN – DYNAMISCHE METHODE

2017 wurden die Ergebnisse eines umfangreichen Modernisierungsprozesses vorgestellt, der in enger Beteiligung mit den IT-Grundschutz-Anwendern durchgeführt wurde. Kern dieser Modernisierung war die Aktualisierung der BSI-Standards sowie die Optimierung der IT-Grundschutz-Bausteine. Diese enthalten praxisnahe Sicherheitsanforderungen nun gebündelt auf zehn Seiten und ermöglichen damit eine noch effizientere Auseinandersetzung mit einem bestimmten Thema. ■



Ein Schutz für alle

Warum Informationssicherheit für jede Institution (über-)lebenswichtig ist

von Katrin Alberts, Referat BSI-Standards und IT-Grundschutz

Der IT-Grundschutz bietet mit seinem breiten Fundament eine systematische Herangehensweise an Informationssicherheit. Er deckt gleichermaßen technische, organisatorische, infrastrukturelle und personelle Aspekte ab, denn für umfassende Sicherheit ist gut geschultes Personal genauso wichtig wie regelmäßige Updates oder eingeschränkt vergebene Administratorrechte.

Ein Mitarbeiter in der Personalabteilung klickt in der E-Mail eines vermeintlichen Bewerbers auf einen Dateianhang, der Schadcode in das Unternehmensnetz bringt. Ein Schwelbrand im Serverraum zerstört wichtige Patientendaten in einem Krankenhaus. Im Rechenzentrum eines Logistikunternehmens hat ein Stromausfall für einen halben Tag die Warenauslieferung lahmgelegt. Sicherheitsvorfälle kosten Behörden und Unternehmen viel Zeit, Geld und Nerven. Das sind Risiken der Digitalisierung – aber sie sind beherrschbar. Denn bei einem fundierten und tragfähigen Managementsystem für Informationssicherheit (ISMS), wie es der IT-Grundschutz vorsieht, greifen alle Sicherheitsmaßnahmen ineinander und diejenigen, die sie umsetzen müssen, wissen immer, was zu tun ist.

DIE BASIS: DREI STANDARDS

Der IT-Grundschutz bietet mit den BSI-Standards 200-1, -2 und -3 die grundlegenden Veröffentlichungen für alle, die erstmalig ein ISMS in einer Institution aufsetzen möchten. Einen kompakten und übersichtlichen Einstieg dafür liefert der „Leitfaden zur Basis-Absicherung nach IT-Grundschutz: In 3 Schritten zur Informationssicherheit".

Diese Basis-Absicherung ist besonders als Einstieg für kleine und mittelständische Unternehmen und Behörden geeignet:

- Der BSI-Standard 200-1 definiert hierzu die allgemeinen Anforderungen, die ein solches ISMS erfüllen sollte.
- Im Zentrum des IT-Grundschutzes steht der BSI-Standard 200-2. Er erläutert, wie ein ISMS solide aufgebaut werden kann. Je nach Sicherheitsanforderungen kann mit einer der drei unterschiedlichen Vorgehensweisen begonnen werden.
- Der BSI-Standard 200-3 beinhaltet alle risikobezogenen Arbeitsschritte. Der Standard bietet sich an, wenn Unternehmen oder Behörden bereits erfolgreich mit der IT-Grundschutz-Methodik arbeiten und eine Risikoanalyse durchführen möchten.

Der BSI-Standard 100-4 zeigt darüber hinaus einen systematischen Weg auf, ein Notfallmanagement in einer Behörde oder einem Unternehmen aufzubauen, um die Kontinuität des Geschäftsbetriebs sicherzustellen. Er wird

IT-Grundschutz-Bausteine – bewährte Werkzeuge zum Thema Informationssicherheit

derzeit zum Thema Business Continuity Management aktualisiert und fortgeschrieben.

FUNDAMENT UND WERKZEUGKASTEN: DAS IT-GRUNDSCHUTZ-KOMPENDIUM

Im IT-Grundschutz-Kompendium können Interessierte in den IT-Grundschutz-Bausteinen Sicherheitsempfehlungen zu den unterschiedlichsten Themen nachlesen. In den Anforderungen erfahren Informationssicherheitsbeauftragte, mit welchen Stellschrauben sie das Sicherheitsniveau gezielt anheben können. Detaillierte Hinweise und Maßnahmen in den Umsetzungshinweisen zu den IT-Grundschutz-Bausteinen erleichtern Informationssicherheitsbeauftragten im Arbeitsalltag, Informationssicherheit in der Praxis anzuwenden. IT-Grundschutz-Anwender bringen ihre Erfahrungen und Know-how aus der Berufspraxis in alle Veröffentlichungen ein und reichern sie dadurch an.

Daneben bieten u. a. IT-Grundschutz-Profile wichtige Angebote für spezifische Anwendergruppen. IT-Grundschutz-Profile können von einzelnen Branchenvertretern, wie Verbänden und Unternehmen und Behörden, auf Wunsch mit Unterstützung durch das BSI zu einem bestimmten Thema erstellt und im Nachgang veröffentlicht werden. Interessierte Anwender, die sich zum Beispiel auch bei einer Kommune mit einem IT-Grundschutz-Profil auseinandersetzen wollen, können auf das bereits Veröffentlichte aufsetzen und sparen Zeit und Ressourcen. Der Austausch innerhalb der Branchen fördert zudem den Austausch von Know-how und das Networking.

Seit Mai dieses Jahres bietet das BSI zudem eine Personenzertifizierung zum IT-Grundschutz-Berater an. Ziel des neuen Angebotes ist es, ein einheitlich hohes Niveau in der Ausbildung zum IT-Grundschutz und zum Thema Informationssicherheit zu gewährleisten. Zertifizierte IT-Grundschutz-Berater können die Empfehlungen und Maßnahmen fundiert und kompetent in der Praxis bei Unternehmen und Behörden weitergeben.

EIN IT-GRUNDSCHUTZ FÜR ALLE ANWENDER (-GRUPPEN)

Die Prozesshaftigkeit und das Entwicklungstempo in der Informationssicherheit bedingen, dass der IT-Grundschutz kontinuierlich weiter aktualisiert wird. Bestehende Veröffentlichungen werden überprüft, zu neuen Entwicklungen werden zum Beispiel neue Bausteine verfasst. Ob der Informationssicherheitsbeauftragte einer Behörde, der CISO eines großen Unternehmens oder der Geschäftsführer eines klein- oder mittelständischen Unternehmens: Sie alle können im neuen Angebot des IT-Grundschutzes passend zu den Anforderungen ihrer Institution nach Informationssicherheit geeignete Informationen finden. ■

2008 Veröffentlichung BSI-Standard 100-4

2009 Veröffentlichung Webkurs Notfallmanagement

2010 Gründung IT-Grundschutz-Gruppe bei Xing

„Die Freunde und Förderer wurden schnell zahlreicher“

Interview mit Isabel Münch, Fachbereichsleiterin Kritische Infrastrukturen

Frau Münch, Sie gehören mit Dr. Hartmut Isselhorst zu den Kolleginnen und Kollegen im BSI, die den IT-Grundschutz 1994 aus der Taufe gehoben haben. Wie kam es damals dazu?

Bei der Gründung des BSI 1991 steckte das Thema IT- und Informationssicherheit bei den Behörden noch in den Kinderschuhen. Die Behörden waren aufgefordert, ihre Sicherheitskonzepte auf Basis des sehr komplexen IT-Sicherheitshandbuches zu erstellen. Da die Verantwortlichen für jedes Objekt eine Risikoanalyse durchführen und sich tief einarbeiten mussten, war das aufwendig und langwierig. Mehrfach wurden Sicherheitskonzepte schon während der Erstellung durch die Einführung neuer IT-Anwendungen überholt. Wir stellten fest, dass die Anwender alle weitestgehend dieselben Fragen bewegten. Der Anfang des IT-Grundschutzes war dann eine FAQ-Liste, die immer weiter ergänzt wurde und schließlich in dem Ansatz mündete, den Anwendern über ein modulares Baukastenkonzept Hilfe zur Selbsthilfe zu geben.

Wie sahen die ersten Schritte aus?

Gestartet haben wir mit einer kleinen Projektgruppe, die von Dr. Isselhorst geleitet wurde, ich war seine Vertreterin. Dabei sind auch die ersten 15 Pilot-Bausteine entstanden, die wir auch damals schon in enger Kooperation mit diversen Fachreferaten verfasst haben. Aus der Projektgruppe wurde das Referat Beratung und IT-Grundschutz. Wir waren ein recht kleines Team für die Aufgaben und viele damalige Mitarbeiter sind dem Thema bis heute verbunden, sei es im BSI, im Bundesinnenministerium oder als selbstständiger Auditor.

Können Sie sich noch an Herausforderungen und Hürden erinnern, die Sie nehmen mussten?

Hürden gab es schon einige: Im ersten Schritt musste natürlich das BMI als unsere vorgesetzte Behörde von dem Vorhaben überzeugt werden. Größeren Respekt hatten wir damals auch davor, den Bundesrechnungshof und den Bundesbeauftragten für den Datenschutz an Bord zu holen. Das hat letzten Endes aber super geklappt und die Datenschützer haben sich im weiteren Verlauf immer sehr dafür eingesetzt, den IT-Grundschutz als Grundlage für Datenschutzkonzepte zu nutzen.

Auch intern gab es kontroverse Diskussionen, da sich einige Fachkollegen beispielsweise vorrangig mit Hochsicherheit beschäftigten und zunächst nicht den Ansatz der Basis-Absicherung beim IT-Grundschutz mitgehen wollten. Aber die Freunde und Förderer des IT-Grundschutzes wurden schnell zahlreicher.

Was wünschen Sie dem IT-Grundschutz für die Zukunft?

Ich wünsche mir, dass seine Angebote und die praktikablen und hilfreichen Empfehlungen weiterhin vielen Anwendern bei der Auseinandersetzung mit dem Thema Informationssicherheit helfen oder Neulingen im Thema den Einstieg erleichtern. Auch die stärkere Etablierung des IT-Grundschutzes im europäischen Raum und international ist aus meiner Sicht wünschenswert. Ein Erfolgsmodell wird der IT-Grundschutz auf jeden Fall bleiben! ■

25 Jahre IT-Grundschutz

2012 Veröffentlichung Umsetzungs-Rahmenwerk (UMRA) zum BSI Standard 100-4

2014 IT-Grundschutz-Twitterkanal

„Informationssicherheit aus einer Hand“

Interview mit Holger Schildt, Referatsleiter BSI-Standards und IT-Grundschutz

Herr Schildt, wo steht der IT-Grundschutz heute?

Er ist gelebte Informationssicherheit in Behörden und Unternehmen; ein etablierter Standard, der sowohl die Grundlagen als auch konkrete Empfehlungen zu allen Fragen der Informationssicherheit zur Verfügung stellt. Und er ist zugleich die bewährte Lösung für alle, die sich mit dem Aufbau eines Managementsystems für Informationssicherheit (ISMS) befassen wollen.

Auf diesen Erfolgen ruhen wir uns aber nicht aus. Ein Beispiel dafür ist die 2017 abgeschlossene Modernisierung. Ein anderes ist ein neues Qualifizierungsverfahren zum IT-Grundschutz-Berater, das wir in diesem Jahr etabliert haben. Der IT-Grundschutz ist damit auch nach 25 Jahren noch genau so dynamisch wie die Entwicklungen, die er abbildet.

Auf welche dieser erfolgreichen Ansätze wollen Sie künftig aufsetzen, welche Angebote ausbauen?

Der IT-Grundschutz ist flexibel anwendbar und kann optimal auf den individuellen Sicherheitsbedürfnissen einzelner Institutionen angepasst werden. Aus der erwähnten Modernisierung sind beispielsweise die Basis-Absicherung und IT-Grundschutz-Profile hervorgegangen. Beide ermöglichen besonders kleinen und mittelständischen Unternehmen (KMU) einen leichteren Einstieg in das Thema Informationssicherheit. Um die erste Hürde noch weiter zu senken, bietet das IT-Grundschutz-Referat gemeinsam mit der Allianz für Cyber-Sicherheit Workshops an, um IT-Grundschutz-Profile zu erstellen. Zusätzlich arbeiten wir daran, den IT-Grundschutz noch stärker im internationalen Umfeld zu positionieren sowie weitere Zielgruppen zu gewinnen.

Wie sehen Sie das Angebot des IT-Grundschutzes im Vergleich zu anderen ISMS-Angeboten?

Unser oberstes Ziel ist es, die Informationssicherheit in Deutschland zu erhöhen. Daher begrüße ich jedes Engagement, das zum Thema ISMS von anderen Anbietern kommt. Der Vorteil des IT-Grundschutzes liegt in der Modularität und Vielseitigkeit des Angebotes, Anwender können für sich die geeigneten Veröffentlichungen wie aus einem Werkzeugkasten auswählen. Durch das Zusammenspiel mehrerer Vorgehensweisen kann Informationssicherheit ohne Reibungsverluste ausgebaut werden, indem beispielsweise an die Basis- direkt die Standard-Absicherung angeschlossen wird. Der IT-Grundschutz liefert Informationssicherheit aus einer Hand. Ein großer Pool von BSI-Experten und Anwendern aus der IT-Grundschutz-Community liefert fachliche Expertise als auch aktuelle Kenntnisse aus der beruflichen Praxis in den Veröffentlichungen.

25 Jahre liegen heute hinter dem IT-Grundschutz. Wo sehen Sie ihn in 25 Jahren?

Die Entwicklungen im Bereich der IT-Sicherheit sind so rasant, dass sich selbst vor zehn Jahren niemand vorstellen konnte, was technisch heute möglich ist. Prognosen darüber, wie die Welt in 25 Jahren aussehen wird, möchte ich nicht abgeben, aber unabhängig davon: Was auch immer im Bereich der Digitalisierung und Informationstechnik passieren wird, die Entwicklungen werden Eingang in den IT-Grundschutz finden. ■

2016 IT-Grundschutz-Kataloge umfassen 100 Bausteine

2017 Veröffentlichung BSI-Standards 200-1, 200-2 und 200-3

Nachgewiesene Informationssicherheit

Warum ein Zertifikat nach IT-Grundschutz sinnvoll ist

von Birger Klein und Alexander Nöhles, Referat BSI-Standards und IT-Grundschutz

Um die erfolgreiche Umsetzung des IT-Grundschutzes nach außen transparent zu machen, können sich Unternehmen oder Behörden nach ISO 27001 auf der Basis von IT-Grundschutz zertifizieren lassen. Mit diesem Zertifikat wird bestätigt, dass das IT-Sicherheitskonzept die Anforderungen nach ISO 27001 erfüllt.

Das BSI hat hierzu ein Zertifizierungsschema für Informationssicherheit entwickelt, das die Anforderungen an ein Managementsystem für Informationssicherheit (ISMS) aus ISO/IEC 27001 berücksichtigt und als Prüfkataloge das IT-Grundschutz-Kompendium sowie die BSI-Standards 200-x zugrunde legt. Dies wird deshalb als ISO 27001-Zertifizierung auf Basis IT-Grundschutz bezeichnet. Eine solche Zertifizierung ist für die IT-Grundschutz-Vorgehensweisen Standard-Absicherung und Kern-Absicherung durchführbar. Bei der Basis-Absicherung reichen die erfüllten Sicherheitsanforderungen nicht für eine Zertifizierung aus, können aber als Einstieg für eine der anderen beiden Vorgehensweisen dienen. Für den Nachweis einer erfolgreichen Umsetzung der Basis-Absicherung bietet das BSI ein Testat an.

Das Zertifikat belegt somit auf transparente und einfach nachvollziehbare Weise, dass

- Informationssicherheit in dieser Institution ein anerkannter Wert ist,
- ein Sicherheitsmanagement vorhanden ist und praktiziert wird sowie außerdem
- kontinuierlich an Aufbau und Verbesserung des Sicherheitsmanagements gearbeitet wird.

VOM AUDIT ZUM ZERTIFIKAT

Grundlage für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist die Durchführung eines Audits durch einen externen, beim BSI zertifizierten Auditor. Das Ergebnis des Audits ist ein Auditbericht, welcher der Zertifizierungsstelle vorgelegt wird. Diese entscheidet über die Vergabe des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz. Das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz bietet Unternehmen und Behörden somit die Möglichkeit, ihr Engagement zur Informationssicherheit transparent zu machen. Das Zertifikat dient damit sowohl gegenüber Kunden als auch Geschäftspartnern als Qualitätsmerkmal und Wettbewerbsvorteil. ■

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

https://www.bsi.bund.de/gs-zertifizierung

„Informationssicherheit ist Chefsache“

Interview mit Bernd Kowalski, Abteilungsleiter Standardisierung und Zertifizierung beim BSI

Was sind aus Ihrer Sicht die größten Vorteile des IT-Grundschutzes?

Der IT-Grundschutz ist die Lösung, wenn es um den Aufbau und Betrieb eines fundierten Managementsystems zur Informationssicherheit geht – eine Lösung, auf die Behörden und Unternehmen seit Jahren setzen. Das Angebot kann jede Organisation verwenden: von der Kommunal- bis zur Bundesbehörde, vom DAX-Konzern bis zum Mittelständler. Die IT-Grundschutz-Methodik ist dabei Fundament und Werkzeug zugleich, wenn sich Verantwortliche für Informationssicherheit mit aktuellen Sicherheitsanforderungen für die Belange in ihren Häusern befassen.

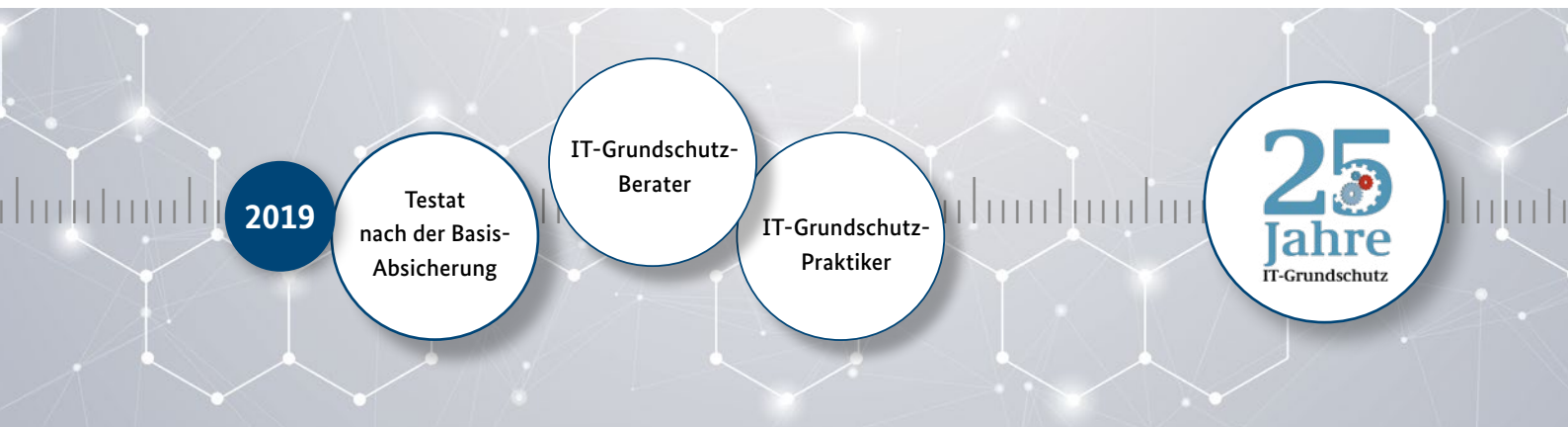
Welche Bedeutung haben ISO 27001-Zertifikate auf der Basis des IT-Grundschutzes für Behörden und Unternehmen im Markt?

Ohne Informationssicherheit kann die Digitalisierung in Verwaltung und Wirtschaft nicht erfolgreich vorangetrieben werden. Ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz belegt eindrucksvoll, dass Informationssicherheit in einer Institution ein anerkannter Wert ist. Zudem verdeutlicht ein Zertifikat, dass Informationssicherheit als „Chefsache“ angesehen wird. Unternehmen und Behörden können mit einer Zertifizierung nach IT-Grundschutz ihr Engagement für Geschäftspartner oder Kunden sichtbar machen und sich dadurch einen Wettbewerbsvorteil im Markt verschaffen.

Welche Themen stehen in naher Zukunft auf der Agenda des IT-Grundschutzes?

Mit der Modernisierung des IT-Grundschutzes wurde ein neues Konzept für IT-Grundschutz-Profile entwickelt. Ein IT-Grundschutz-Profil ist ein Muster-Sicherheitskonzept, das als Schablone für Institutionen mit ähnlichen Rahmenbedingungen dient, beispielsweise in einer bestimmten Branche. Das BSI unterstützt aktuell zahlreiche Branchen und Anwendergruppen bei der Erstellung von IT-Grundschutz-Profilen. So hat die Reedereibranche bereits ein IT-Grundschutz-Profil für den Landbetrieb veröffentlicht und erarbeitet aktuell ein Profil für den Seebetrieb. Auch die Kommunalverwaltungen haben ein IT-Grundschutz-Profil vorgelegt.

Als nationale Cyber-Sicherheitsbehörde beschäftigt sich das BSI auch mit Sicherheitsfragen bei Zukunftstechnologien. So spielt der IT-Grundschutz bei dem aktuellen Thema 5G-Mobilfunk eine wichtige Rolle – bereits jetzt sind Empfehlungen im Sicherheitskatalog der Bundesnetzagentur verankert. ■



IT-SICHERHEIT
IN DER PRAXIS

Digitalbarometer – Bürgerbefragung zur Cyber-Sicherheit

Potenzial von Schutzmaßnahmen sollte stärker genutzt werden

von Karin Wilhelm, Referat Cyber-Sicherheit für den Bürger

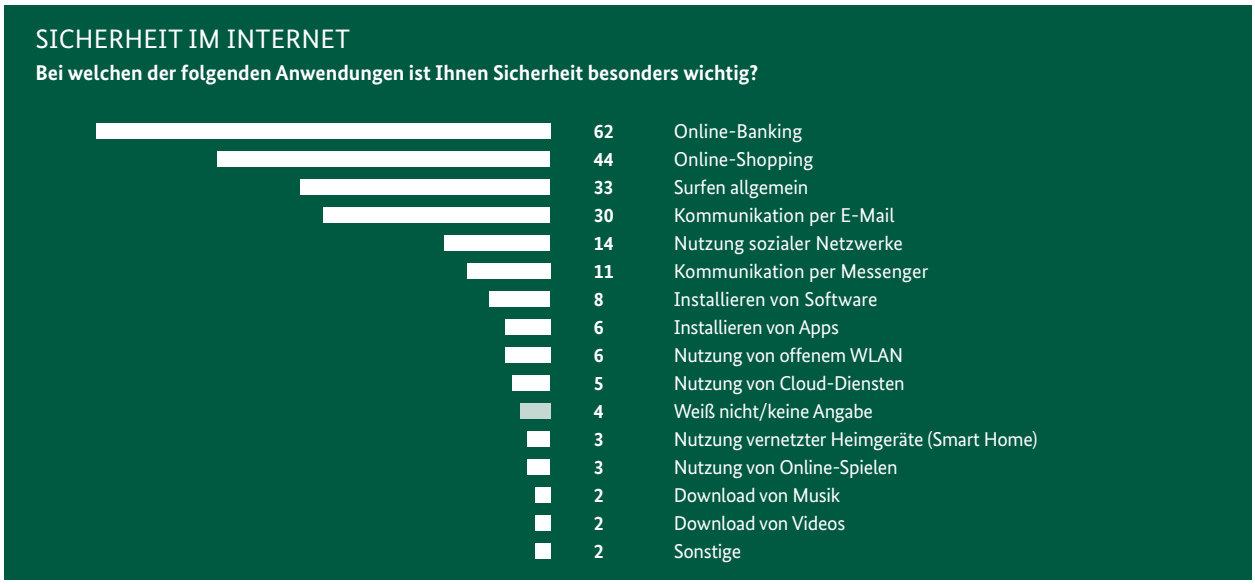
Fast jeder Vierte (24%) war bereits Opfer von Kriminalität im Internet. Das zeigen die Ergebnisse einer repräsentativen Online-Umfrage des BSI und des Programms Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) . Dennoch werden wichtige Schutzmaßnahmen von den Befragten nur partiell umgesetzt: Nur 61 Prozent haben Antivirenprogramme und 58 Prozent sichere Passwörter. Maßnahmen wie die sofortige Installation verfügbarer Updates (36%) und die Verschlüsselung von E-Mails (19%) werden ebenfalls unterschätzt.

Das BSI und ProPK verfolgen das Ziel, Bürgerinnen und Bürger umfassend über Cyber-Risiken und entsprechende Schutzmöglichkeiten aufzuklären, um die Digitalisierung erfolgreich und sicher mitzugestalten. Aus diesem Grund schlossen die beiden Partner 2017 eine Vereinbarung über eine strategische Zusammenarbeit bei der Aufklärungsarbeit. Bedeutender Baustein dieser Kooperation ist eine repräsentative Online-Umfrage, die den aktuellen Kenntnisstand von Bürgerinnen und Bürgern zum Thema IT-Sicherheit erheben soll. Diese wurde 2019 überarbeitet und professionalisiert. Zu den Leitfragen gehören unter anderem: Welche Bedeutung hat Sicherheit im Internet bei Privatanwendern? Wie schützen sie sich vor den Gefahren der digitalen Welt? Wo informieren sich die Befragten über Schwachstellen und Risiken?

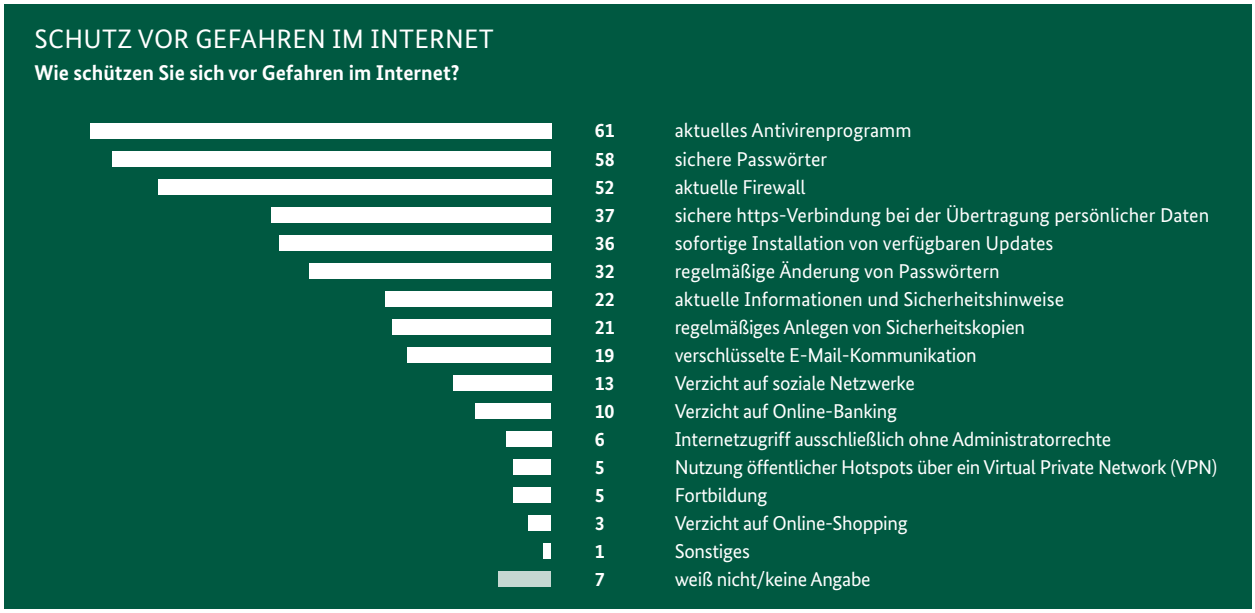
JEDER VIERTE BETROFFEN

24 Prozent der Befragten gaben an, bereits Opfer von Kriminalität im Internet gewesen zu sein. Dabei handelte es sich vor allem um Betrug beim Online-Shopping (36 %), Phishing-Vorfälle (28%), das heißt das Ausspionieren vertraulicher Daten, und Schadsoftware-Angriffe durch Viren oder Trojaner (26%). Dieser Bedrohungslage steht jedoch das Informationsverhalten der Befragten gegenüber. Nur ein Drittel (31%) informiert sich regelmäßig über Internetsicherheit, die meisten hingegen erst im Problemfall. Zwar kennt die Hälfte der Befragten die aktuellen Sicherheitsempfehlungen zum Schutz vor Kriminalität im Internet, doch lediglich 36 Prozent setzen diese dann direkt um. Dies ist zudem abhängig von Alter: Fast die Hälfte aller 60- bis 66-Jährigen wird sofort aktiv (49%), während es bei den 16- bis 29-Jährigen nur etwa jeder Vierte (26%) ist.

Das Thema Sicherheit im Internet ist einem Großteil wichtig (80%) – die Intensität variiert jedoch: Die Hälfte (51%) macht sich eher selten Sorgen, nur knapp jeder Dritte (31%) häufig oder fast immer. Besonders wichtig sind den Befragten alle Aktivitäten, bei denen es ums Geld geht wie beim Online-Banking (62%) und Online-Shopping (44%). Als weitere relevante Themen werden das allgemeine Surfen (33%) und die E-Mail-Kommunikation (30%) genannt. Weniger bedeutend ist die Sicherheit bei der Nutzung sozialer Netze (14%) und bei der Kommunikation per Messenger (11%). Geht es um automatisierte Vorgänge wie dem Installieren von Apps, dem Nutzen eines offenen WLAN (jeweils 6%) oder dem Herunterladen von Dateien (2%) spielt Sicherheit eine fast verschwindende Rolle (vgl. Grafik 1). Dabei können diese Vorgänge Einfallstore für Schadprogramme oder Hacker sein. Ebenfalls angreifbar machen sich alle, die keinen großen Wert auf die sichere Nutzung vernetzter Heimgeräte legen (3 %) – denn immerhin mehr als die Hälfte der Befragten geben beispielsweise an, einen internetfähigen Fernseher (57 %) zu besitzen.



Grafik 1 – Quelle: Digitalbarometer, Basis: alle Befragten (n=2.000), Angaben in Prozent



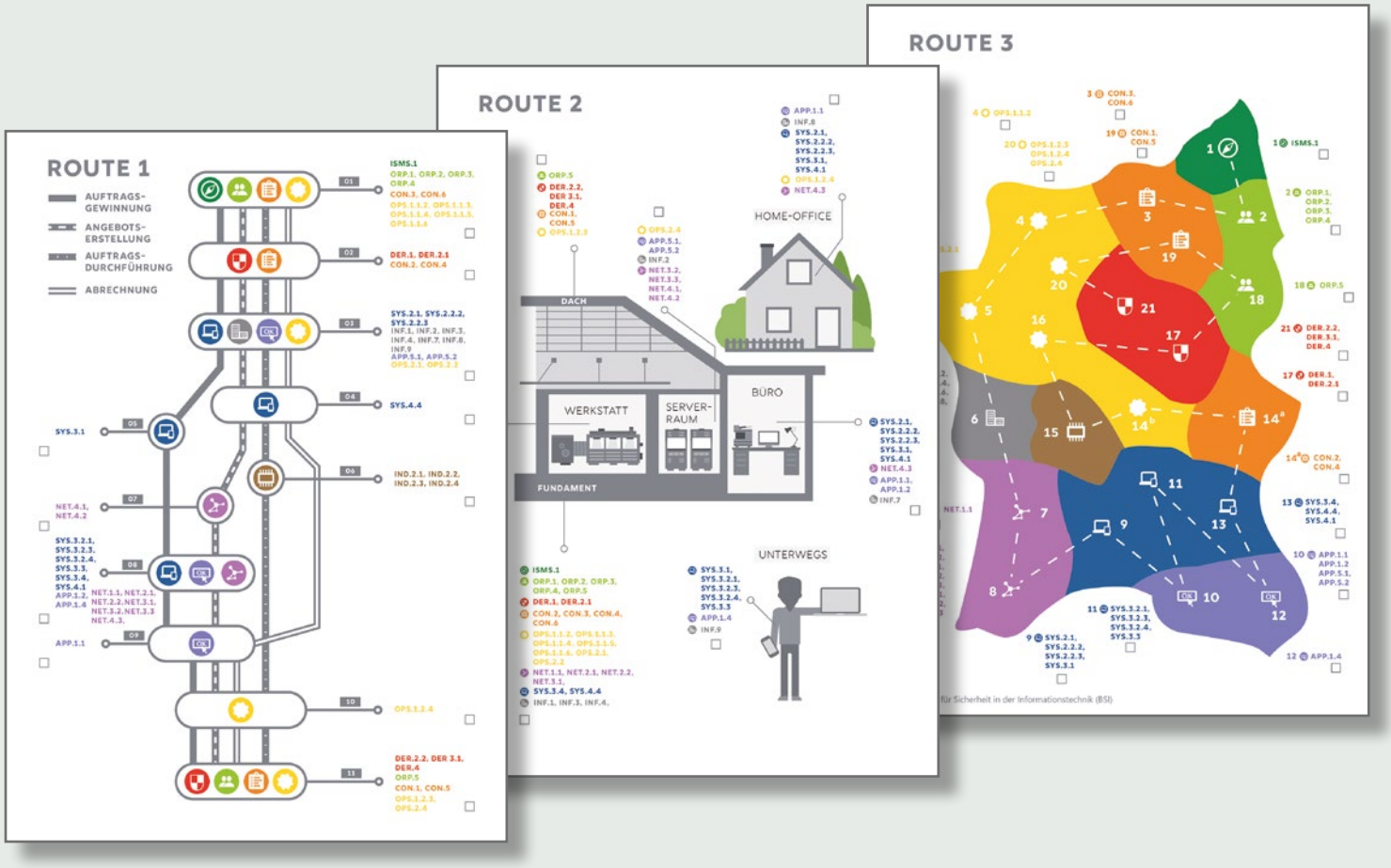
Grafik 2 – Quelle: Digitalbarometer, Basis: Befragte, die sich Sorgen um ihre Sicherheit im Internet machen (n=1.737), Angaben in Prozent

UNTERSCHÄTZE SCHUTZMASSNAHMEN

Wer sich um die Sicherheit im Internet sorgt, schützt sich vor allem mit Antivirenprogrammen (61%), sicheren Passwörtern (58%) und einer aktuellen Firewall (52%) (vgl. Grafik 2). Das bedeutet im Umkehrschluss aber auch, dass fast die Hälfte der Befragten diese Maßnahmen nicht nutzt, auch wenn sie unumgänglich für den Basisschutz sind. Darüber hinaus werden weitere Sicherheitsempfehlungen unterschätzt: Nur 36 Prozent wenden sofortige Installationen von verfügbaren Updates an, obwohl die Durchführung oftmals lediglich wenige Minuten dauert. Digitale Kommunikation wird von einem Drittel als wichtig eingestuft, jedoch setzen nur 19 Prozent auf Verschlüsselung bei E-Mails.

BSI und ProPK sind sich einig: Die Aufklärungsarbeit wird auf Basis der Ergebnisse weiter ausgebaut. Neben neuen Sensibilisierungsaktivitäten zu den Wunschthemen der Befragten – vor allem Online-Banking, Surfen und Online-Shopping – soll auch der Bekanntheitsgrad bereits bestehender Angebote ausgebaut werden. Immerhin 40 Prozent der Befragten kennen bereits die Informationen des BSI oder der Polizei zum Thema IT-Sicherheit. ■

Weitere Informationen: https://www.bsi-fuer-buerger.de und https://www.polizei-beratung.de



Die drei Routen: betrieblich, räumlich und thematisch

Destination: Cyber-Sicherheit

Der Routenplaner „Cyber-Sicherheit für Handwerksbetriebe“

von Stefan Wunderlich, Referat Cyber-Sicherheit für die Wirtschaft und Allianz für Cyber-Sicherheit

Im Rahmen des 27. Cyber-Sicherheits-Tags der Allianz für Cyber-Sicherheit wurde im März 2019 in Frankfurt am Main der Routenplaner „Cyber-Sicherheit für Handwerksbetriebe“ vorgestellt. Damit erhalten Betriebe eine praktische Arbeitshilfe, die sie Schritt für Schritt durch den Sicherheitsprozess gemäß IT-Grundschutz des BSI führt. Das Ziel: Ein individueller Fahrplan, um das Sicherheitsniveau im eigenen Betrieb zu erhöhen – branchenspezifisch, bedarfsgerecht und geeignet auch für kleine und mittlere Betriebe.

Das im März 2019 veröffentlichte IT-Grundschutz-Profil für Handwerksbetriebe bietet insbesondere kleinen und mittelständischen Unternehmen (KMU) eine praktikable Lösung, um mit einem überschaubaren personellen und finanziellen Aufwand die Informationssicherheit im Betrieb zu erhöhen. Das vom Zentralverband des deutschen Handwerks (ZDH) herausgegebene IT-Grundschutz-Profil ist das Ergebnis einer im Rahmen der Allianz für Cyber-Sicherheit (ACS) und des IT-Grundschutz durchgeführten Workshop-Reihe. Es handelt sich dabei um ein Muster-Sicherheitskonzept, das als Schablone für Betriebe mit vergleichbaren Rahmenbedingungen dienen kann. Durch die Beteiligung von Entscheidern und IT-Fachleuten konnten Branchen- und IT-Sicherheits-Expertise gleichermaßen in den Erstellungsprozess einfließen.

Vorstellung des Routenplaners: Holger Schwannecke, Generalsekretär des ZDH; Prof. Dr. Kristina Sinemus, Hessische Ministerin für Digitale Strategie und Entwicklung; Dr. Timo Hauschild, BSI

CYBER-SICHERHEIT HANDFEST

Im IT-Grundschutz-Profil für Handwerksbetriebe werden diejenigen Bausteine aus dem IT-Grundschutz-Kompendium des BSI beschrieben, die anzuwenden sind, um die Informationssicherheit in einem „typischen" Handwerksbetrieb zu erhöhen. Dies sind unter anderem Bausteine für die Absicherung von Anwendungen, von IT-Systemen oder auch von physischen Räumen.

Wie aber nun bahnt sich ein Betrieb den Weg durch die verfügbaren Bausteine? Wo soll man beginnen, in welcher Reihenfolge soll man die Bausteine abarbeiten und in welchem Tempo, um mit überschaubarem Aufwand einen größtmöglichen Effekt zu erzielen? Gerade Handwerker mögen es hier gerne möglichst „handfest". Vor dem Hintergrund dieser häufig gestellten Fragen entstand daher die Idee, eine Art Gebrauchsanleitung oder Handbuch als ergänzende Arbeitshilfe für die konkrete Umsetzung des IT-Grundschutz-Profils herauszugeben. Auftritt: Routenplaner!

BETRIEBLICH, RÄUMLICH ODER THEMATISCH?

Der Routenplaner zum IT-Grundschutz-Profil für Handwerksbetriebe bietet dem Nutzer verschiedene Einstiegspunkte in den Sicherheitsprozess nach IT-Grundschutz. Die Frage lautet hier, aus welchem Blickwinkel man sich der Thematik nähern will und welche Herausforderungen im Blick auf den individuellen Schutzbedarf die drängendsten sind:

- Wenn der Nutzer von den zentralen Geschäftsprozessen ausgehen möchte, die kritisch für den Erfolg seines Betriebs sind – im Handwerk typischerweise Auftragsgewinnung, Angebotserstellung, Auftragsdurchführung oder Abrechnung –, ist Route 1 (betrieblich) die richtige.
- Stehen gerade die Renovierung der Büroräume oder ein Umbau an, bietet Route 2 (räumlich) einen idealen Startpunkt.
- Route 3 (thematisch) schließlich bietet die Möglichkeit, das IT-Grundschutz-Profil für Handwerksbetriebe nach Themen sortiert von Anfang bis Ende umzusetzen.

Hat sich der Nutzer erst einmal für die passende Route entschieden, durchläuft er verschiedene „Stationen" mit Bausteinen, die nach und nach abgearbeitet werden müssen. Gibt es die benannten IT-Systeme oder -Anwendungen nicht im Betrieb, werden die entsprechenden Bausteine einfach ausgelassen. Besonders praktisch: Für jede Route gibt es eine Checkliste zum Abhaken der erledigten Bausteine. Das erleichtert den Überblick darüber, was bereits geschafft ist – und was noch zu tun ist.

DER ROUTENPLANER IM PRAXISTEST

Wie sich der Routenplaner in der Praxis schlägt, wird aktuell in einem Testlauf in Kooperation mit dem ZDH und dem Kompetenzzentrum Digitales Handwerk (KDH) erprobt. Dabei setzen drei ausgewählte Unternehmen das IT-Grundschutz-Profil für Handwerksbetriebe auf Grundlage des Routenplaners um. Begleitet werden sie auf diesem Weg durch Experten des KDH. Der Startschuss für das Projekt fiel im Rahmen einer Veranstaltung der Handwerkskammer Hamburg im Juni 2019. Die gesammelten Erfahrungen und Best Practices sollen im dritten Quartal 2020 vorgestellt werden.

Die Digitalisierung von Geschäftsabläufen und Produktionsprozessen und die damit einhergehende Erhöhung von Cyber-Risiken stellt alle Bereiche der Wirtschaft vor große Herausforderungen – auch KMU, die häufig nur über begrenzte Ressourcen für IT-Sicherheit verfügen. Am Beispiel des Handwerks zeigt das Paket aus IT-Grundschutz-Profil und Routenplaner gerade diesen Betrieben einen machbaren Weg auf, wie sie Informationssicherheit zielgerichtet und grundsolide angehen und umsetzen können. ■

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

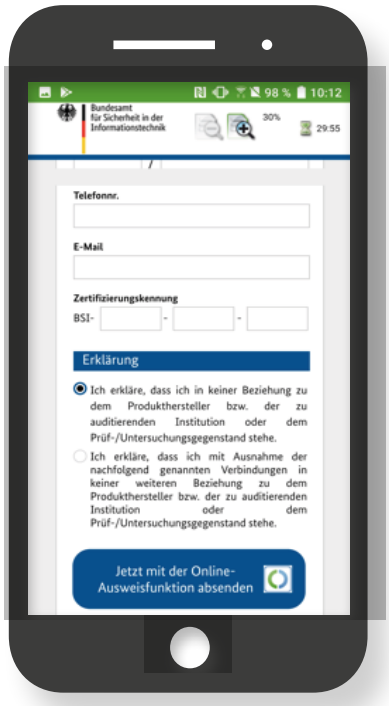
Prozesse mit dem Personalausweis digital umsetzen

von Jennifer Breuer, Referat eID-Lösungen für die digitale Verwaltung

Mit der Online-Ausweisfunktion des Personalausweises (eID) existiert eine sichere und attraktive Lösung, sich online zu identifizieren und zu authentisieren. Dafür gibt es bereits unterschiedlichste Anwendungsbeispiele. Das BSI als nationale Cyber-Sicherheitsbehörde möchte weitere Behörden und Unternehmen bei der sicheren Integration der Funktionen rund um die eID des Personalausweises unterstützen.

DER PERSONALAUSWEIS UND WAS ER KANN

Der seit 2010 ausgegebene Personalausweis im Scheckkartenformat kann mehr als sein Vorgänger: Mittels der auf dem Chip gespeicherten Daten (eID) kann sich der Ausweisinhaber online ausweisen und sich damit beispielsweise den Gang zur Behörde sparen. Statt einen Antrag auszufüllen und zu unterschreiben, kann die Online-Ausweisfunktion genutzt werden, um den Antrag rechtsverbindlich und medienbruchfrei zu stellen. Durch die sichere Zwei-Faktor-Authentisierung – das heißt Besitz des Ausweises und Wissen der PIN – erreicht der Personalausweis (ebenso wie auch der elektronische Aufenthaltstitel und die geplante eID-Karte für EU-Bürger) ein sehr hohes Sicherheitsniveau.



Unabhängigkeits- und Unparteilichkeitserklärung

Medienbruchfreiheit ist auch das Schlagwort, wenn es um das seit 2017 mögliche Vor-Ort-Auslesen geht. Hierbei kann der Personalausweis mittels Eingabe der aufgedruckten Zugangsnummer (CAN) vor Ort von einer berechtigten Stelle ausgelesen werden, um Fehler bei der Übertragung der Daten zum Beispiel in ein Formular zu vermeiden. Das Vor-Ort-Auslesen bringt jedoch noch einen weiteren Vorteil: Das Dokument wird im Hintergrund gleichzeitig auf Validität und eventuelle Sperrung geprüft.

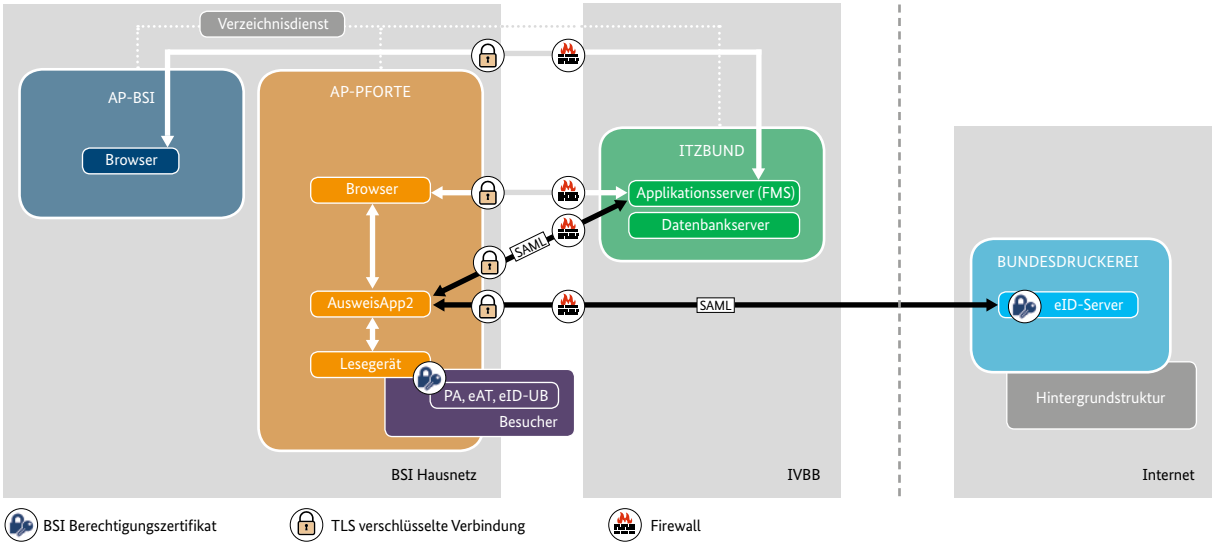
DAS FORMULAR-MANAGEMENT-SYSTEM DES BUNDES

Das Formular-Management-System des Bundes (FMS) basiert auf dem Produkt Lucom Interaction Platform (kurz: LIP) und gestattet es, Formulare und selbst komplette Workflows digital umzusetzen. In Kombination mit der Online-Ausweisfunktion ist es dann zum Beispiel möglich, diese Daten direkt an eine Behörde zu versenden und damit die gesetzliche Schriftformerfordernis zu ersetzen. Mit den richtigen Schnittstellen zum Fachverfahren entfällt auch die lästige Datenübertragung durch einen Mitarbeiter.

FMS-ANWENDUNGEN DES BSI

Das BSI nutzt das FMS in Verbindung mit der Online-Ausweisfunktion bereits für mehrere Formulare, die bisher entweder postalisch oder per De-Mail eingereicht werden mussten. Eines dieser Formulare ist die Unabhängigkeits-

TECHNISCHE LÖSUNGSARCHITEKTUR FÜR DAS BESUCHERMANAGEMENT IM BSI MIT INTEGRIERTEM VOR-ORT-AUSLESEN



und Unparteilichkeitserklärung für Auditoren und Prüfstellen. Die Erklärung musste bisweilen von Hand unterschrieben werden. Nun kann sie nicht nur am Desktop ausgefüllt und abgeschickt werden, sondern wurde auch für die mobile Nutzung optimiert (siehe Abbildung linke Seite, unten). Damit kann die Erklärung etwa direkt auf einem kompatiblen Smartphone oder Tablet ausgefüllt und mittels Online-Ausweisfunktion übertragen werden.

Das Vor-Ort-Auslesen des Personalausweises in Kombination mit dem FMS kann zudem für die Digitalisierung von Prozessen verwendet werden. Im BSI wurde dies prototypisch für das Besuchermanagement umgesetzt. Bei der Besucheranmeldung werden nach der Identitätsprüfung die Daten des Personalausweises ausgelesen und validiert. Die ausgelesenen Daten werden dann automatisch mit den Daten der registrierten Besucher abgeglichen und nach dem entsprechenden Datensatz gefiltert. Auf diese Weise wurde der gesamte Prozess des Besuchermanagements digitalisiert.

FMS-UMSETZUNG IN KOMBINATION MIT DEM PERSONALAUSWEIS

Bei der Umsetzung eines Formulars oder eines Workflows im FMS sollte zuerst der Istzustand betrachtet werden. Hier kann es nötig sein, einige Anpassungen vorzunehmen, um den Prozess benutzerfreundlich gestalten zu können. Im Gegensatz zu Papierformularen macht es das FMS möglich, den Anwender durch die eingebauten Bedingungen und Verknüpfungen bei der Formularausfüllung zu leiten.

Die Anbindung der Online-Ausweisfunktion ist bereits im FMS integriert, trotzdem werden für die Nutzung noch weitere Komponenten benötigt. Die Abbildung oben veranschaulicht die Architektur, die für das Vor-Ort-Auslesen benötigt wird.

Das BSI unterstützt Institutionen, die den Personalausweis in ihre Fachverfahren oder digitalisierten Prozesse einbinden möchten. Hilfestellung gibt das Referat DI 15 „eID-Lösungen für die digitale Verwaltung“ unter **referat-DI15@bsi.bund.de.**

Zum einen wird das Berechtigungszertifikat benötigt, je nach Anwendung entweder für die Online-Ausweisfunktion oder das Vor-Ort-Auslesen. Es kann erst nach Genehmigung durch das Bundesverwaltungsamt (BVA) erteilt werden. Denn nur berechtigte Stellen dürfen den Personalausweis elektronisch auslesen. Der Nutzer selbst muss eine Software installiert haben, die eine sichere Verbindung zwischen dem Kartenlesegerät, dem Personalausweis und dem Diensteanbieter herstellt, zum Beispiel die AusweisApp2. Zudem wird ein eID-Server benötigt, um unter anderem die Authentizität und Gültigkeit des Personalausweises festzustellen. Dieser kann für Behörden als eID-Service etwa von der Bundesdruckerei in Anspruch genommen werden. Zur Nutzung des FMS im Behördenumfeld stellt das ITZ Bund die Anwendung bereit und übernimmt das betriebliche Hosting. ■

Weitere Informationen: https://www.ausweisapp.bund.de/mobile-geraete

DIGITALE GESELLSCHAFT

Standardisierungsstrategie gibt Richtung für weitere Einsatzbereiche vor

Cyber-Sicherheit für die Digitalisierung der Energiewirtschaft

von Stefan Vollmer, Referat Cyber-Sicherheit für die Digitalisierung der Energiewirtschaft

Gemeinsam mit dem Bundesministerium für Wirtschaft und Energie (BMWi) hat das BSI eine Standardisierungsstrategie zur sektorübergreifenden Digitalisierung der Energiewende erarbeitet und veröffentlicht. Auf ihrer Basis können nun gemeinsam mit den Verbänden und den Unternehmen der Energiewirtschaft die wesentlichen technischen Eckpunkte und die daraus resultierenden Anforderungen für ein sicheres, intelligentes Energienetz (Smart Grid) der Zukunft festgelegt werden.

Ohne eine kontinuierliche Fortentwicklung der rechtlichen und technischen Rahmenbedingungen ist die Migration des heute passiven Energienetzes zu einem sicheren und aktiven Smart Grid nicht denkbar. Dies gilt insbesondere für die Integration und Vernetzung von steuerbaren Erzeugungsanlagen, flexiblen Verbrauchseinrichtungen, mobilen und stationären Energiespeichern und modernen Messeinrichtungen in das intelligente Energienetz. Denn mit der Vernetzung aller relevanten Smart-Grid-Komponenten werden zugleich Cyber-Angriffe auf diese digitale Infrastruktur wahrscheinlicher. Um diesen möglichen Angriffen zu begegnen, sind nachweislich sichere und standardisierte Produktkomponenten und Systeme im Netz sowie eine sichere Kommunikationsinfrastruktur entscheidend.

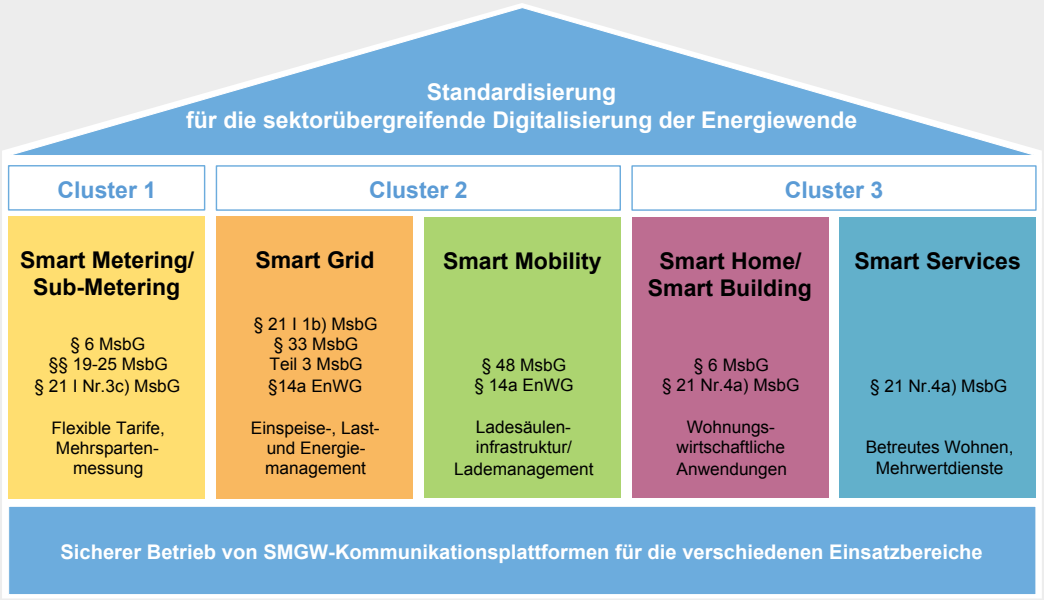
ROADMAP ZUR WEITERENTWICKLUNG DER TECHNISCHEN BSI-STANDARDS

Die BMWi-BSI-Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nimmt diese Herausforderung an. Sie zeigt, basierend auf den Rahmenbedingungen des Gesetzes zur Digitalisierung der Energiewende (GDEW), auf, wie mit der Weiterentwicklung der technischen Standards des BSI der stufenweise Rollout von intelligenten Messsystemen und weiteren standardisierten Mess- und Steuerungseinrichtungen für das zukünftige Smart Grid gefördert wird. Im Zentrum des intelligenten Messsystems steht das zertifizierte Smart-Meter-Gateway (SMGW) als sichere Kommunikationsplattform, dessen stufenweise Einführung im Messstellenbetriebsgesetz (MsbG) geregelt wird.

STUFENWEISER AUSBAU DER INTELLIGENTEN MESSSYSTEME UND ANDERER KOMPONENTEN

Der Rollout von intelligenten Messsystemen (iMSys) umfasst u. a. Letztverbraucher mit einem Jahresstromverbrauch ab 10.000 kWh und Erzeuger zwischen 7 kW und 15 kW Leistung. Mit der Zertifizierung des ersten Smart-Meter-Gateways im Dezember 2018 haben bereits mehrere Messstellenbetreiber mit dem Einbau intelligenter Messsysteme bei Kunden begonnen. Die gesetzliche Verpflichtung zum

FAHRPLAN DES GESETZES ZUR DIGITALISIERUNG DER ENERGIEWENDE (GDEW)



Einbau von Smart-Meter-Gateways greift jedoch erst dann, wenn drei Geräte unterschiedlicher Hersteller vom BSI zertifiziert wurden. Auf diese Weise wird eine Infrastruktur etabliert, die das Prinzip „Security-by-Design" von Beginn an erfüllen wird.

Gemäß der Standardisierungsstrategie steht das BSI bereits in Kontakt mit Herstellern und Anwendern von intelligenten Messsystemen, um erste Erweiterungen der Anforderungen zum Funktionsumfang zu konsolidieren und somit erste Software-Updates für die zertifizierten Smart-Meter-Gateways zu bestimmen. So werden u. a. Vorgaben zur Netzzustandsdatenerhebung konkretisiert. Dadurch können Mehrwert und Nutzen dieser neuen Mess-, Steuer- und Kommunikationsinfrastruktur für eine Vielzahl der Akteure – beispielsweise für Netzbetreiber und Vertrieb – weiter ausgebaut werden. Dies ermöglicht insbesondere im Niederspannungsnetz, den Netzzustand sicher zu überwachen und Verbraucher, Speicher und Erzeuger zu steuern, um drohende Netzengpässe abzuwenden. So kann die bestehende Netzinfrastruktur effizienter ausgenutzt und ein kostenintensiver Netzausbau verhindert werden.

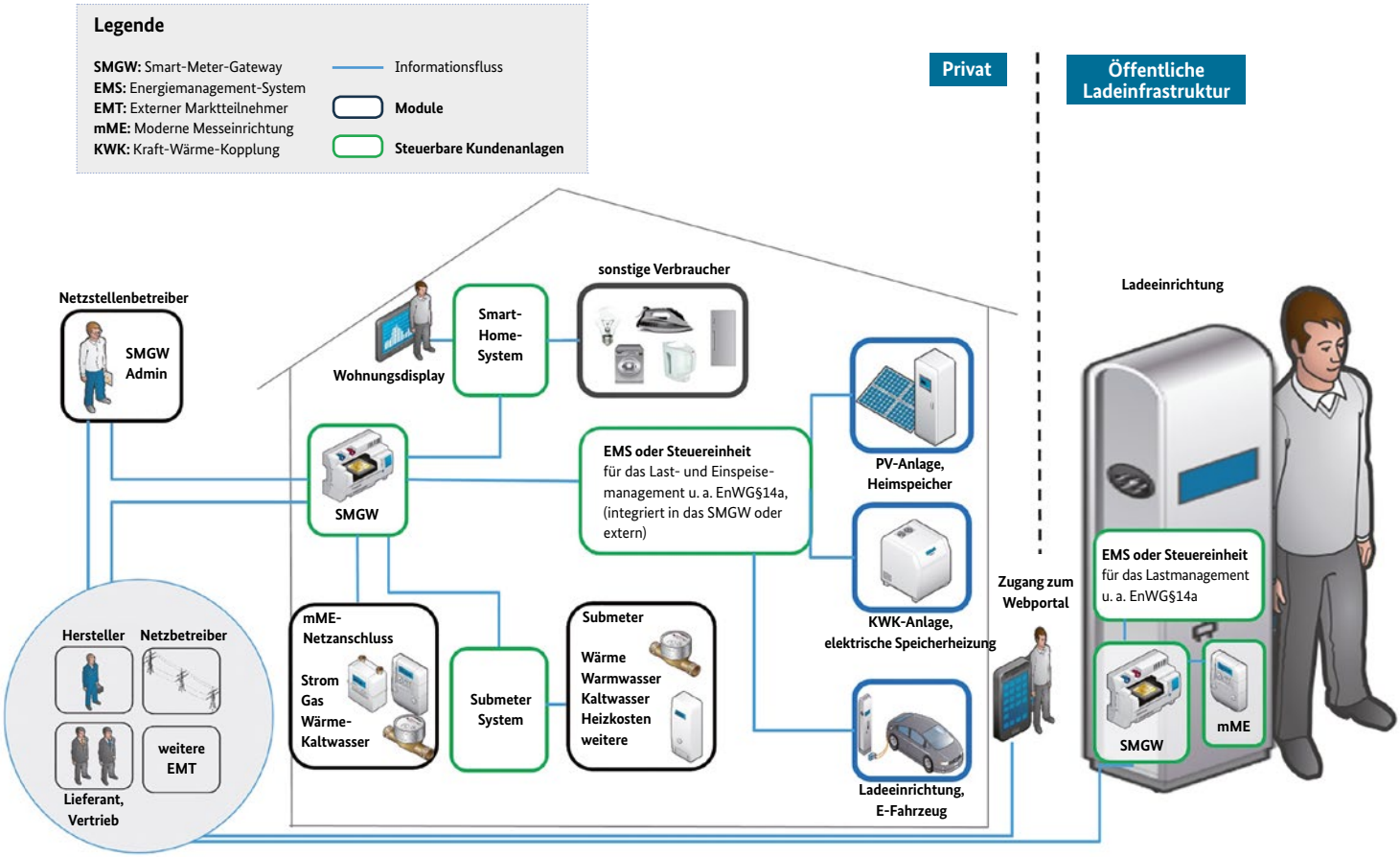
WEITERE BSI-STANDARDS FÜR DIE SEKTORÜBERGREIFENDE DIGITALISIERUNG

Für eine sektorübergreifende Digitalisierung der Energiewende bedarf es aber weiterer Standards für ein sicheres Smart Grid, die zukünftig mit der Energiewirtschaft abgestimmt werden müssen. Insbesondere werden durch den Roadmap-Prozess weitere Einsatzbereiche für die Smart-Meter-Gateway-Kommunikationsplattform aufgezeigt, die im Vorfeld der Vorgabenentwicklung analysiert werden müssen:

- Smart Metering mit Mehrsparten- und Untermessung (Sub-Metering)
- Smart Grid mit Steuerung und Monitoring von Einspeise-, Verbrauchs-, Speicher- und Netzeinrichtungen
- Smart Mobility mit Netzintegration der Ladeinfrastruktur, sicheres Lademanagement und datenschutzkonforme Abrechnung
- Smart Building mit Steuerung und Monitoring von energietechnischen Einrichtungen
- Smart Home mit digitaler Verbraucherinformation und Energieeffizienz
- Smart Services mit weiteren Diensten der SMGW-Kommunikationsplattform

HERLEITUNG DER TECHNISCHEN UND REGULATORISCHEN ECKPUNKTE

Um für die Weiterentwicklung von technischen Standards des BSI eine solide Basis und Akzeptanz im Markt zu schaffen, hat das BSI ein Projekt zur „Produkt- und Systemarchitektur-Analyse für die fortschreitende Digitalisierung des intelligenten Netzes der Energiewende" gestartet. Es soll technische Eckpunkte beschreiben, die für die Weiterentwicklung der technischen Standards als Grundlage dienen. Zum einen setzt die Analyse dabei auf die sektorübergreifenden Themen der Standardisierungsstrategie auf. Zum anderen berücksichtigt sie Arbeits-



Themenlandkarte des Roadmap-Prozesses

ergebnisse des BMWi-Projekts „Digitalisierung der Energiewende: Barometer und Topthemen", das parallel die regulatorischen Eckpunkte zu den verschiedenen sektorübergreifenden Themen analysiert. Seitens des BMWi wird das Ziel verfolgt, entsprechende Rechtsverordnungen (§ 46 und § 74 MsbG) zu entwickeln. Sowohl die technischen Eckpunkte als auch die Rechtsverordnungen stellen somit die Rahmenbedingungen für die Weiterentwicklung der BSI-Vorgaben in den kommenden Jahren dar.

DIE PRODUKT- UND SYSTEMARCHITEKTUR-ANALYSE

Damit die parallelen Arbeiten, mit denen die technischen und regulatorischen Eckpunkte ermittelt werden, zielgerichtet verfolgt werden können, werden die Gutachter des BMWi-Projekts bei der Durchführung der Analyse eng einbezogen. Um eine aktive Einbeziehung der Energiebranche zu gewährleisten, ist zu Beginn des Projekts ein Branchen-Input-Prozess vorgesehen.

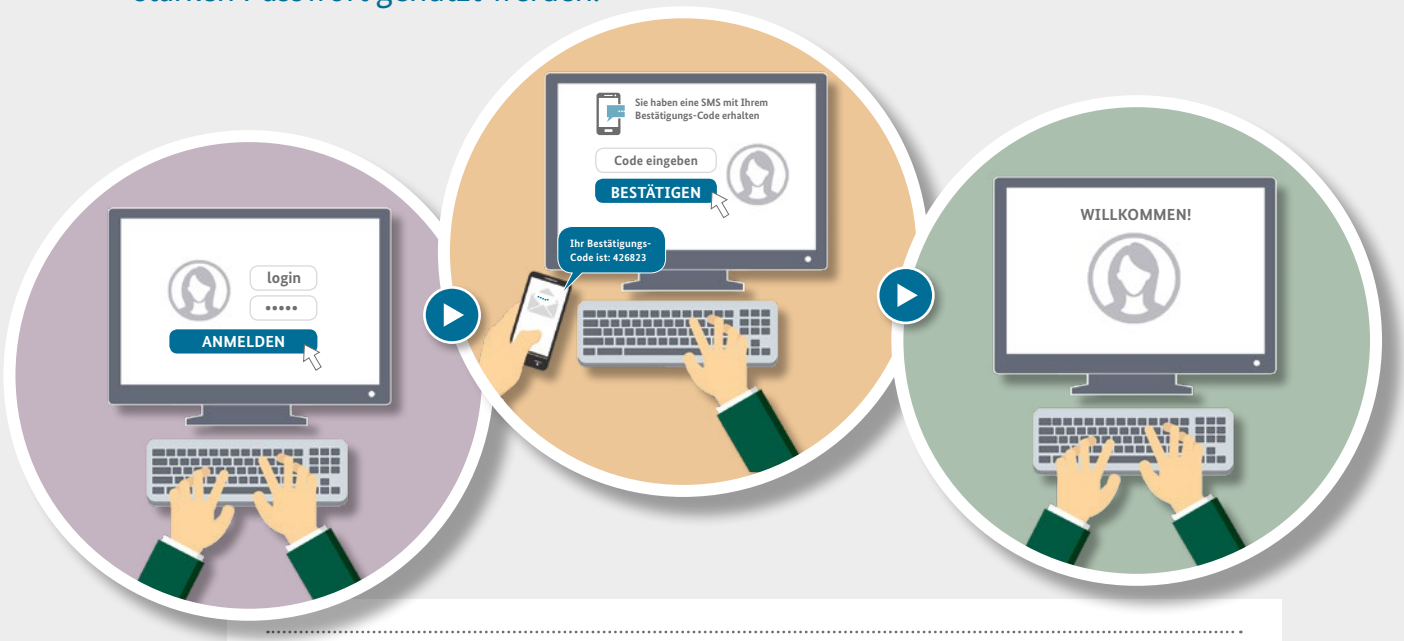
Der Prozess staffelt sich in eine Befragungs-, eine Interview- und eine Task-Force-Phase, um den Input aller Vertreter aus der Energiebranche berücksichtigen zu können. Die Weiterentwicklungsschwerpunkte (System- und Kommunikationsarchitekturen, Produktprofile mit Anwendungsfällen und grundlegenden Sicherheitsfunktionen) werden auf Basis der Branchen-Input-Ergebnisse, der BMWi-Gutachter-Ergebnisse sowie einer durch das BSI erarbeiteten Marktsicht der eingesetzten Produkt- und Systemlösungen der Mess- und Steuerungsinfrastruktur ermittelt und anschließend in technischen Eckpunkten veröffentlicht. Mit der Publikation der technischen Eckpunkte endet die erste Analyse- und Planungsphase für weitere BSI-Standards. Im Roadmap-Prozess folgen nun die Spezifikationsphase zur Entwicklung von Schutzprofilen und Technischen Richtlinien und die eigentliche Umsetzungsphase. ■

Weitere Informationen: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/smartmeter.html

Zwei-Faktor-Authentisierung für höhere Sicherheit

BSI-Basistipp

Mittlerweile bieten viele Online-Dienstleister Verfahren an, mit denen sich die Nutzer oder Nutzerinnen zusätzlich zur Passworteingabe identifizieren können, wenn sie sich in ein Konto einloggen. Bei dieser sogenannten Zwei-Faktor-Authentisierung (2FA) gibt es zahlreiche Varianten. Sie reichen vom individuellen Code per SMS bis zum Einsatz einer Hardware-Komponente wie einer Chipkarte oder einem speziellen USB-Stick. 2FA bietet ein hohes Maß an Sicherheit und sollte wenn möglich ergänzend zu einem starken Passwort genutzt werden.



WARUM MACHT ZWEI-FAKTOR-AUTHENTISIERUNG LOG-IN-PROZESSE SICHERER?

- Passwörter können leicht in falsche Hände geraten, etwa durch Phishing oder Hacks.
- Die Nutzung eines zusätzlichen Faktors erhöht die Sicherheit deutlich.
- 2FA kombiniert Faktoren aus den unterschiedlichen Kategorien Wissen (z. B. Passwort), Besitz (z. B. Mobiltelefon) oder biometrische Merkmale (z. B. Fingerabdruck).
- Vor allem hardwaregestützte Verfahren bieten ein hohes Maß an Sicherheit.
- Für einen unautorisierten Zugang müssten Dritte über beide Faktoren verfügen, also z. B. sowohl über das Passwort als auch über das zusätzlich genutzte Gerät. Das erschwert einen Angriff deutlich.

Das BSI empfiehlt daher grundsätzlich den Einsatz einer Zwei-Faktor-Authentisierung.

Weitere Informationen: https://www.bsi-fuer-buerger.de/2fa

Sicherheitsstandard für das Internet der Dinge

von Kilian Mitterweger, Referat Cyber-Sicherheit in Smart Home und Smart Cities

Der Trend, vernetzte Alltagsgegenstände, Sensor- und Steuerungselemente oder digitale Assistenzsysteme im privaten Umfeld einzusetzen, wird im Sprachgebrauch oft mit den Begriffen „Smart Home“ und „Consumer IoT“ beschrieben. Dieser Trend verändert neben dem Alltagsleben der Nutzer auch die Bedrohungslage im Cyber-Raum. Nationale und internationale Organisationen arbeiten deshalb seit einiger Zeit an geeigneten Sicherheitsstandards für das Internet of Things (IoT).

Ein eindrucksvolles Beispiel für die neue Bedrohungslage im IoT liefert der in diesem Zusammenhang häufig erwähnte Mirai-Vorfall im Oktober 2016. Bei diesem wurde ein Internetdienstleister durch eine Distributed-Denial-of-Service-Attacke (DDoS-Attacke) angegriffen. Von diesem Dienstleister abhängige Webseiten wie Amazon, Twitter, Spotify, Netflix und Paypal waren für ein bis zwei Stunden nicht mehr verfügbar. Als Angriffswerkzeug wurde ein Mirai-Botnetz verwendet, das zu diesem Zeitpunkt vermutlich aus einer sechsstelligen Anzahl gekaperter Geräte bestand. Darunter waren auch IP-Kameras, die direkt aus dem Internet erreichbar waren und durch die Verwendung von Standardpasswörtern und einfach auszunutzenden Schwachstellen in großer Zahl kompromittiert wurden. Diese Geräte stellten so nicht nur eine Gefahr für die Internetinfrastruktur als Ganzes, sondern auch für die Privatsphäre der eigentlichen Besitzer dar.

NICHT JEDER KANN SPEZIALIST FÜR IT-SICHERHEIT IM IOT SEIN

Diese Risiken erfordern, geeignete Sicherheitsstandards einzuführen. Bei der Entwicklung von Standards im Consumer-Umfeld bestehen besondere Anforderungen. Ein zentraler Punkt ist dabei die „Security by Default“. Dieser Begriff beschreibt die Anforderung, dass ein IoT-Gerät ohne besondere Sicherheitskonfiguration durch den Nutzer in einem auf Sicherheit ausgelegten Zustand betrieben werden kann. Das bedeutet im Idealfall unter anderem

- eine dem Zugriff über potenziell von Angreifern erreichbare Schnittstellen wie z. B. Funk- und IP-Schnittstellen stets vorgeschaltete Authentisierung und
- einen automatischen Updatemechanismus, der auf Updates zu etwaigen Sicherheitslücken (z. B. durch Fehler in der Implementierung) hinweist oder diese automatisch ohne aktives Handeln des Nutzers durch Update-Installation schließt.

SICHERHEIT VON ANFANG AN

Ein weiteres generelles Sicherheitsprinzip bei der Entwicklung von IT-Lösungen, das auch im Consumer-IoT-Umfeld anzuwenden ist, ist „Security by Design“. Dabei wird Sicherheit nicht nur als Gerätefunktionalität begriffen, sondern auch als Grundlage für Anforderungen an den Entwicklungsprozess und die Geräte- und Infrastrukturarchitektur eines Produkts. Hinsichtlich einer Gerätearchitektur bedeutet dies unter anderem

- die Beschränkung des Zugriffs von Nutzern und Gerätefunktionen auf interne Systemressourcen und Funktionen auf das für die angestrebte Funktionalität minimal notwendige Maß und

- die Auswahl und Implementierung von Sicherheitsfunktionalitäten nach dem Stand der Technik (z. B keine Standardpasswörter oder produktübergreifende Standardschlüssel), wie diese in etablierten Sicherheitsstandards wie BSI TR-02102 oder SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms beschrieben werden.

KLEINER EINBLICK IN DIE WELT DER STANDARDS

Ein Beispiel eines solchen Sicherheitsstandards für ein leistungsfähiges IoT-Gerät wie ein Smart TV ist die DIN SPEC 27072, deren Entwicklung das BSI als Autor mitgestaltet hat. Das Dokument beinhaltet konkrete Anforderungen an ein IoT-Gerät, deren Formulierung auf Testbarkeit ausgelegt ist. Geräte, die diese Anforderungen erfüllen, bieten für den Supportzeitraum des Herstellers ein Basissicherheitsniveau, das sie vor skalierbaren Cyber-Angriffen aus dem Internet schützen kann, wie sie etwa mit der Schadsoftware Mirai durchgeführt werden. Dazu gibt das Dokument Herstellern konkrete Anhaltspunkte für die Umsetzung von „Security by Design“ und „Security by Default“. Diese Prinzipien sollten generell bei der Konzeption und Entwicklung von Produkten eingehalten werden. Dabei wird der komplette Produktlebenszyklus inklusive Auslieferung, Inbetriebnahme, Individualisierung und Außerbetriebnahme berücksichtigt.

Mit ETSI TS 103 645 existiert ein in der Tiefe weniger konkreter, dafür aber breiter gefasster Standard. Dieser beinhaltet auch Anforderungen an Herstellerprozesse zum Beispiel hinsichtlich Schwachstellenmanagement und IoT-Infrastrukturanforderungen.

CYBER-SICHERHEIT IM EUROPÄISCHEN BINNENMARKT

Die Einführung der DIN SPEC 27072 im Mai 2019 war ein wichtiger Meilenstein zur Einführung von Mindestsicherheitsstandards für Smart-Home-Geräte. Letztendlich ist sie aber nur ein Schritt auf dem langen Weg zu einem leistungstungsfähigen europäischen Binnenmarkt für nachweisbar sichere IT-Produkte. Mit dem „Cyber Security Package“ hat die EU-Kommission den hierfür erforderlichen rechtlichen Rahmen geschaffen. Ziel ist, die Cyber-Sicherheit in Europa zu stärken. Über den darin enthaltenen Cyber Security Act soll insbesondere die Harmonisierung von Prüf- und Zertifizierungsverfahren gewährleistet werden.

Für den Consumer-Markt wäre es wichtig, wenn IoT-Geräte und -Infrastrukturen, nach sicherheitstechnisch leistungsfähigen Europäischen Normen konzipiert, hergestellt und im europäischen Binnenmarkt verbreitet und betrieben würden. Basis hierfür könnten insbesondere sicherheitszertifizierte technische Plattformen sein, die in einer Vielzahl von IoT-Produkten verbaut werden. Solche Plattformen können IoT-Produkten die notwendige Sicherheitsfunktionalität (zum Beispiel Schlüsselspeicher oder kryptografische Funktionen) bereitstellen. So kann eine solide Grundlage für die Digitalisierung des alltäglichen Lebens als Teil des europäischen Weges in eine sichere digitale Gesellschaft geschaffen werden. ■

Den Verbraucher im Blick

von Dr. Angelika Praus, Projektgruppe Digitaler Verbraucherschutz

Mit dem Koalitionsvertrag der Bundesregierung von Februar 2018 hat das BSI die Aufgabe des Digitalen Verbraucherschutzes zugewiesen bekommen. Eine neu eingerichtete Projektgruppe steuert und koordiniert künftig die Aktivitäten in diesem Bereich.

Die Digitalisierung bietet in fast allen Bereichen des Alltags neue Möglichkeiten und größeren Komfort. Zugleich birgt sie aber für jeden Einzelnen auch vielfältige Risiken – insbesondere im Hinblick auf die Cyber-Sicherheit. Als herstellerunabhängige und kompetente technische Stelle unterstützt das BSI die Verbraucher bei der Risikobewertung von Technologien, Produkten, Dienstleistungen und Medienangeboten. Neben einem besseren Schutz des Einzelnen wird damit gleichzeitig auch die gesellschaftliche Widerstandsfähigkeit gegen Cyber-Gefahren jeglicher Art erhöht.

Um den digitalen Verbraucherschutz zu stärken und das Thema gezielt voranzutreiben, hat das BSI mit der Umorganisation des Amtes im April 2019 die Projektgruppe „Digitaler Verbraucherschutz“ eingerichtet. Sie soll die bereits vorhandenen Aktivitäten in diesem Bereich abteilungsübergreifend bündeln und weitere initiieren. Ausgehend von den bereits bestehenden Kontakten, baut sie die Zusammenarbeit mit Partnern des Verbraucherschutzes aus und gestaltet so Informationssicherheit mit einem ausgeprägt kooperativen Ansatz.

Konkret soll die Projektgruppe die strategischen Ziele aus dem im Jahr 2018 formulierten Verbraucherschutzkonzept vorantreiben: Erhöhung des Risikobewusstseins, der Beurteilungsfähigkeit und der Lösungskompetenz der Verbraucher. Dazu sind verschiedene Maßnahmen geplant, die zum Teil auf bereits bestehenden Aktivitäten aufsetzen. So sollen u. a. Sensibilisierungsmaßnahmen zielgruppenspezifisch ausgestaltet, ein kontinuierlicher Verbraucherschutzdialog mit Herstellern und Dienstanbietern implementiert und Aktivitäten im Bereich Marktbeobachtung und Stand der Technik systematisiert werden. ■

TRANSPARENZ SCHAFFEN

Das IT-Sicherheitskennzeichen, dessen Einführung im Koalitionsvertrag 2018 angekündigt wurde, soll dem Verbraucher produktspezifische Eigenschaften der Informationssicherheit transparent darstellen und diese zum Bestandteil seiner Kaufentscheidung machen. Grundlage für die Vergabe des IT-Sicherheitskennzeichens ist die freiwillige Zertifizierung oder eine Herstellererklärung. Sie umfasst auch eine für den Verbraucher verständliche Beschreibung der Sicherheitseigenschaften des Produkts. Eine konkrete Ausprägung wird das IT-Sicherheitskennzeichen mit dem IT-Sicherheitsgesetz 2.0 erhalten. Hier wird ein neues Verfahren konzipiert, um die Sicherheitseigenschaften von Produkten und Dienstleistungen aus dem Verbrauchermarkt zu berücksichtigen. Die Ausgestaltung des Verfahrens wird derzeit im BSI im Rahmen einer Projektgruppe erarbeitet.

VERMITTLUNGSFORMATE AUSBAUEN

Mit dem Start eines eigenen YouTube-Kanals hat das BSI sein Informationsangebot ausgebaut. Hier finden Verbraucher Tipps und Hinweise zum Thema Cyber-Sicherheit und zur Arbeit des BSI. Auch ein Video, das sich explizit mit dem Thema „Digitaler Verbraucherschutz“ befasst, ist dort eingestellt: **https://www.youtube.com/BundesamtfürSicherheit-inderInformationstechnik.** In der Videoreihe „IT-Sicherheit verständlich erklärt“ geben BSI-Experten alltagstaugliche Empfehlungen und vermitteln Hintergrundwissen. Animierte Clips machen komplexe Themen wie zum Beispiel E-Mail-Verschlüsselung nachvollziehbar. Das Angebot wird kontinuierlich erweitert, neue Formate sind in Planung.

KOOPERATIONEN ETABLIEREN

Der themenbezogene Austausch mit Mitgliedern des Netzwerks Verbraucherforschung, das vom Bundesministerium der Justiz und für Verbraucherschutz unterstützt wird, ist ein wichtiger Baustein, um einen kontinuierlichen Verbraucherschutzdialog zu etablieren. Gemeinsam mit Vertretern des Netzwerks entwickelt das BSI Kompetenzprofile für den Bereich des Digitalen Verbraucherschutzes, um die Personalgewinnung und Kompetenzentwicklung in diesem Aufgabenfeld weiter zu stärken.

Auch mit wissenschaftlichen Einrichtungen strebt das BSI einen derartigen Dialog an. Auf dem gemeinsam organisierten Verbraucherforschungsforum „Digital Nudging – Ein Ansatz zur Verbesserung der Informationssicherheit?“ im September 2019 in Bonn diskutierten Experten aus dem Bereich der Informationssicherheit und Wissenschaftler aus dem Verbraucherschutz auch über den Transfer von konkreten Ansätzen der Wirksamkeit.

GERÄTESICHERHEIT FÖRDERN

Das Smartphone ist das am häufigsten genutzte internetfähige Gerät und wird im Alltag auch für den Zugang zu sensiblen Bereichen (Online-Banking, Gesundheit) eingesetzt. Gleichzeitig befinden sich im Handel Smartphones, die über gravierende Sicherheitslücken verfügen und nicht mehr vom Hersteller mit Updates versorgt werden. Das BSI setzt sich aktiv für eine Verbesserung der Sicherheit von Smartphones ein. Mit seiner technischen Expertise (Sicherheitstests und -analysen) unterstützt es zum einen Abmahnungen und Klagen zum Beispiel der Verbraucherzentrale Nordrhein-Westfalen in dem Bereich. Außerdem führt das BSI Gespräche mit Providern, um gemeinsam Möglichkeiten zu erarbeiten, wie die Sicherheit von Smartphones verbessert werden kann, die diese als Verkäufer in Umlauf bringen.

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 bislang rund 940 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

Bestellen Sie Ihr BSI-Magazin!

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Referat Cyber-Sicherheit für den
Bürger und Öffentlichkeitsarbeit

Postfach 20063
53133 Bonn
Telefon: +49 (0) 228 99 9582 0
Telefax: 0228 99 9582-5455
E-Mail: bsi-magazin@bsi.bund.de

Zweimal im Jahr gibt das BSI-Magazin „Mit Sicherheit“ Einblick in nationale und internationale Cyber-Sicherheitsthemen, die digitale Gesellschaft sowie IT-Sicherheit in der Praxis. Lassen Sie sich jetzt direkt nach Erscheinen zur Hannover Messe im April und zur it-sa im Oktober die aktuellste Ausgabe bequem per Post zusenden, indem Sie sich mit unten stehendem Formular für den Abo-Verteiler anmelden.

Ich möchte die folgende BSI-Publikation im Abo erhalten:

☐ BSI-Magazin „Mit Sicherheit“ (2 x im Jahr, Print)
☐ Die Lage der IT-Sicherheit in Deutschland (1 x im Jahr, Print)

Name, Vorname

Organisation

Straße

PLZ, Ort

E-Mail

Datenschutzrechtliche Einwilligung:
Ich stimme zu, dass meine oben angegebenen personenbezogenen Daten durch das BSI als verantwortliche Stelle für den Versand bzw. die Übermittlung der oben genannten Publikationen genutzt, elektronisch gespeichert und verarbeitet werden. Eine Weitergabe an Dritte findet nicht ohne Zustimmung statt.

Datum/Unterschrift:

Verantwortliche Stelle für die Verarbeitung Ihrer oben genannten personenbezogener Daten ist das Bundesamt für Sicherheit in der Informationstechnik, Postfach 200363, 53133 Bonn. Die von Ihnen angegebenen Daten werden ausschließlich für die Verwaltung des Versands bzw. der Übermittlung der Informationen verwendet, zu denen Sie oben zugestimmt haben. Sie können diese Einwilligung jederzeit widerrufen. Hierzu genügt eine E-Mail an bsi-magazin@bsi.bund.de. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Weitere Informationen darüber, wie wir Ihre personenbezogenen Daten bei uns verarbeiten und welche Rechte Ihnen diesbezüglich zustehen, können Sie den beigefügten „Datenschutzrechtlichen Hinweisen“ zur Bestellung von BSI-Publikationen entnehmen. Einfach das Formular per Fax oder E-Mail einsenden:
Telefax: 0228 99 9582-5455 | E-Mail: bsi-magazin@bsi.bund.de

Oder Sie melden sich direkt online an: https://www.bsi.bund.de/BSI-Magazin

Wenn Sie die BSI Publikationen nicht mehr erhalten möchten, schicken Sie uns einfach eine E-Mail an **bsi-magazin@bsi.bund.de**.

Folgen Sie dem BSI auch auf Facebook und Twitter!
www.facebook.com/bsi.fuer.buerger | twitter.com/bsi_presse
Weitere Informationen sowie Checklisten und Tipps rund um Cyber-Sicherheit finden Sie unter:
www.bsi.bund.de | www.bsi-fuer-buerger.de | www.allianz-fuer-cybersicherheit.de
Datenschutzrechtliche Hinweise: https://www.bsi.bund.de/datenschutzrechtliche-hinweise

IMPRESSUM

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI) 53175 Bonn
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Referat WG24 – 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 2019
Texte und Redaktion:	Nora Basting und Mark Schulz, 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:	Appel und Klinger Druck & Medien GmbH Bahnhofstraße 3 96277 Schneckenlohe Internet: www.ak-druck-medien.de
Artikelnummer:	BSI-Mag 19/710-1
Bildnachweise:	Titel: Fotolia © kran77; S. 2: Stephan Kohzer/BSI; S. 4, oben: Trägergesellschaft Süd-West mbH; S. 4, unten: Fotolia © Maksim_Kabakou; S. 5, oben: BSI; S. 7: Prof. Dr. Reinhard Posch; S. 8: GettyImages © sarayut; S. 14/15: BSI; S. 16: AdobeStock; S. 18/19: GettyImages © KTSDESIGN; S. 19: BMI/René Bertrand; S. 22: AdobeStock; S. 24/25: BSI; S. 26: AdobeStock; S. 28: Sächsisches Staatsministerium des Innern; S. 29: Bundesministerium des Innern; S. 31: DsiN; S. 32: Lichtgut/Leif Piechowski; S. 33: Lichtgut/Leif Piechowski, Frank Kahl (Auditorium und Hamburg-Panorama); S. 34: Fotolia ©Jacob Lund; S. 35: Fotolia ©kasto, Fotolia ©contrastwerkstatt; S. 36-37: BSI; S. 38-45: BSI; AdobeStock (Hintergrundbild); S. 48-49: BSI; S. 50: BSI; S. 51: BSI; S. 53: BSI; S. 54: BSI; S. 55: R. Winkler; S. 56: AdobeStock; S. 58: AdobeStock; S. 60: Fink & Fuchs, Fotos iStock.com/Grafissimo; iStock.com/Krasyuk

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

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

www.bsi.bund.de