Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

BSI-Magazin 2020/02

Mit Sicherheit

Im Blickpunkt:
Cyber-Sicherheit im Gesundheitswesen

EDITORIAL

Das Ausnahmejahr

Die Corona-Pandemie ist allgegenwärtig und wird bleibende Spuren hinterlassen. Sie führt uns die grundlegende Bedeutung von Gesundheit jeden Tag aufs Neue vor Augen. Gleichzeitig hat die Pandemie wirtschaftliche, gesellschaftliche und Transformationsprozesse beschleunigt und sorgt für einen nie dagewesenen Digitalisierungsschub in Deutschland und weltweit.

In diesem Zusammenhang gewinnt auch die Frage nach einer hochwertigen, zukunftsfähigen Gesundheitsversorgung an Bedeutung. Die Digitalisierung des Gesundheitswesens birgt enormes Potenzial für eine nachhaltige Verbesserung der medizinischen Versorgungsqualität: Krankenhäuser, Arztpraxen und vor allem Patientinnen und Patienten können von digitalen Technologien und einer besseren Vernetzung profitieren und innovative Behandlungs- und Pflegemöglichkeiten anbieten bzw. in Anspruch nehmen. Die Digitalisierung im Gesundheitswesen bringt aber auch eine ganze Reihe an Herausforderungen mit sich. Dabei ist klar: Ohne Informationssicherheit kann sie nicht gelingen. Die vorliegende Ausgabe des BSI-Magazins widmet sich dem Schwerpunktthema Cyber-Sicherheit im Gesundheitswesen und beleuchtet aktuelle Ansätze des BSI auf diesem Gebiet. Denn als zentrales Kompetenzzentrum für Informationssicherheit in Deutschland gestaltet das BSI die sichere Digitalisierung auch in diesem für die Gesellschaft so wichtigen Bereich.

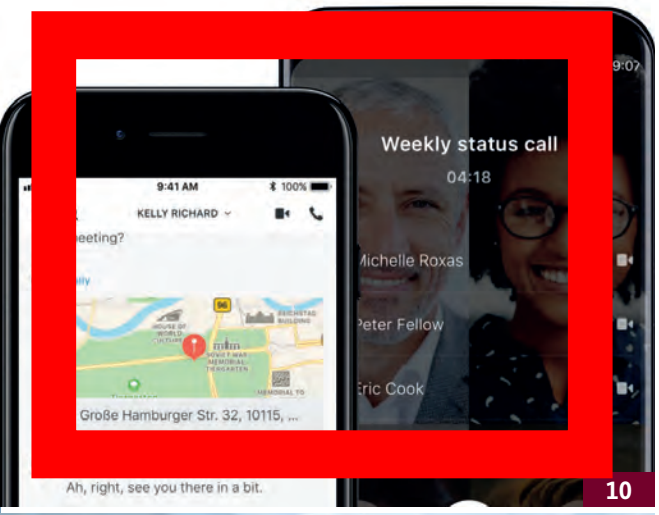
Darüber hinaus möchten wir in dieser Ausgabe das 30-jährige Bestehen des BSI nutzen, um einen Blick zurück zu werfen. Seit seiner Gründung am 1. Januar 1991 beschäftigt sich das BSI mit der Bewältigung von IT-Bedrohungen und IT-Sicherheitsrisiken. Mit einem steten Aufgabenzuwachs und einer Ausweitung auf die drei heutigen Zielgruppen Staat, Wirtschaft und Gesellschaft hat es sich zur zentralen Cyber-Sicherheitsbehörde des Bundes und zentralen Stelle der Cyber-Sicherheitsarchitektur Deutschlands entwickelt.

Die Kompetenzen des BSI sind gerade in Zeiten fortschreitender Digitalisierung gefragt, denn Informationssicherheit und Digitalisierung gehören untrennbar zusammen: Sie sind zwei Seiten derselben Medaille. Das BSI steht für beides, denn es zeigt auf, wie Informationssicherheit als neues Qualitätsmerkmal einer Digitalisierung „Made in Germany“ funktionieren kann.

Ich wünsche Ihnen eine interessante Lektüre

Ihr

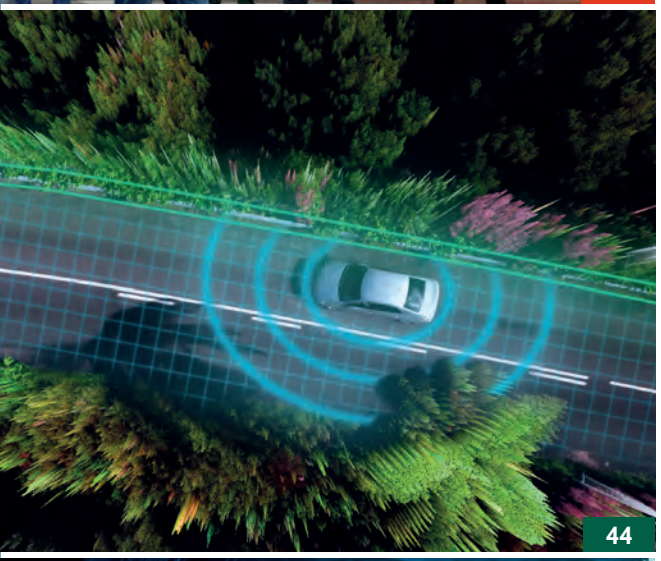
Arne Schönbohm
Präsident des Bundesamts für Sicherheit in der Informationstechnik



10


20


24


44


54

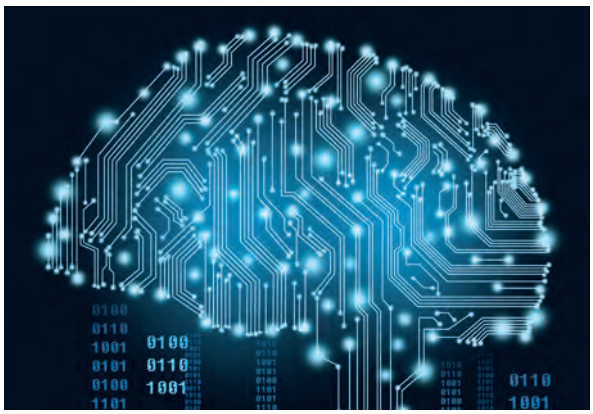
INHALT

AKTUELLES

BSI FÜR BÜRGER

BSI mit eigenem Podcast: Update verfügbar

„Update verfügbar“ ist der neue Podcast des BSI. Er versorgt Hörerinnen und Hörer immer am Ende des Monats für eine halbe Stunde mit Wissenswertem zu Cyber-Vorfällen und den neuesten Innovationen, mit skurrilen Fakten und natürlich mit Informationen zu den wichtigsten Updates. Das Moderatoren-Team wirft einen objektiven Blick auf die Ereignisse der jeweils vorausgegangenen vier Wochen aus Netzwelt, Technologie und Internetkriminalität. Dabei sprechen die beiden Journalisten Ute Lange und Michael Münz in jeder Ausgabe über Ereignisse oder Fragen, die sie besonders beschäftigt haben. Sie erzählen von aktuellen Geschehnissen, reden über ihre Befürchtungen und erklären Hintergründe. Wer sich nicht in komplizierten Artikeln verlieren möchte, hört ab sofort die wichtigsten Nachrichten zur IT-Sicherheit in „Update verfügbar“. Neue Folgen stehen immer kostenlos bei Spotify, Deezer, iTunes, Google Podcasts und YouTube zur Verfügung.



WETTBEWERB

Erfolg bei CHES-Challenge

Auch in diesem Jahr veranstaltete die International Association for Cryptologic Research im Rahmen der CHES (Cryptographic Hardware and Embedded Systems) die CHES-Challenge. Bei diesem kryptographischen Wettbewerb ging es darum, versteckte kryptographische Implementierungen durch Seitenkanäle anzugreifen. Das diesjährige BSI-Team bestand aus acht Mitarbeiterinnen und Mitarbeitern der Abteilungen Krypto-Technik und IT-Management sowie Technikkompetenzzentren und räumte dabei alle Preise ab, die bei der Challenge vergeben wurden.

Die CHES ist die weltweit größte und renommierteste hardwarenahe Kryptographietagung. Die jährlich durchgeführten CHES-Challenge sind prestigeträchtig.

#CYBERCONFERENCE2020

EU-Ratspräsidentschaftskonferenz ein voller Erfolg

Am 9. November 2020 fand die gemeinsam vom Bundesministerium des Innern, für Bau und Heimat und dem Bundesamt für Sicherheit in der Informationstechnik durchgeführte EU-Cybersicherheitskonferenz statt – Corona-bedingt im hybriden Format. Das Fachpublikum aus den Behörden der Mitgliedstaaten und EU-Institutionen diskutierte in drei Foren über strategische Fragen und aktuelle Legislativvorhaben der europäischen Cybersicherheitspolitik, die europäische Zusammenarbeit in der Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle sowie die Gewährleistung von Sicherheit im Bereich des Internet of Things (IoT). Zusätzlich gab es Interviews mit BSI-Präsident Arne Schönbohm zur derzeitigen Bedrohungslage und der Rolle des BSI sowie mit Juhan Lepassaar, Exekutivdirektor der European Union Agency for Cybersecurity (ENISA), zur Rolle von ENISA im europäischen Zertifizierungsprozess für Cybersicherheit.

IT-GRUNDSCHUTZ

Cyber-Sicherheit an Bord – IT-Grundschutz für Schiffe unter deutscher Flagge

Mit der Resolution MSC.428(98) sind die Vertragsstaaten der International Maritime Organization (IMO) angehalten, ab 2021 Cyber-Risiken angemessen zu adressieren. Das soll im Rahmen des vorgeschriebenen Safety Management Systems (SMS) in den maritimen Unternehmen sowie im Umgang mit sicherheitsrelevanten Ereignissen (ISPS-Code) an Bord erfolgen. In Vorbereitung darauf hat das BSI bereits seit Anfang 2018 gemeinsam mit verschiedenen maritimen Akteuren einen Prozess zur Steigerung der Cyber-Sicherheit in der Seeschifffahrt initiiert. Aus diesem Engagement sind die beiden „IT-Grundschutz-Profile für Reedereien“ - Landbetrieb (2018) sowie - Schiffsbetrieb (Anfang 2020) entstanden.

Darauf aufbauend haben nun das BSI und die beiden für Schiffe unter deutscher Flagge zuständigen Behörden, die Berufsgenossenschaft Verkehrswirtschaft Post-Logistik Telekommunikation (BG Verkehr) sowie das Bundesamt für Seeschifffahrt und Hydrographie (BSH), das Arbeitspapier „SM CYBER SECURITY 2020“ herausgegeben. Die bereits etablierte Empfehlung der BG Verkehr zur Umsetzung des SMS wurde dabei um Aspekte zur Informationssicherheit gemäß IT-Grundschutz erweitert und mit praktischen Umsetzungshinweisen aus den IT-Grundschutz-Profilen sowie dem ISPS-Code ergänzt. Damit sind alle gemeinsamen Anforderungen (wie z.B. die Risikoanalyse) konsolidiert und in der etablierten Methodik (SMS) vereint, um so den Aufwand für Anwenderinnen und Anwender aus den Reedereien zu minimieren und Doppelungen zu vermeiden.

CYBER-SICHERHEIT

Sicher durch die Krise mit IT-Grundschutz

Neuer BSI-Standard 200-4: Business Continuity Management

von Cäcilia Jung und Daniel Gilles, Referat BSI-Standards und IT-Grundschutz

Die ersten Auswirkungen der COVID-19-Pandemie im Frühjahr dieses Jahres haben nahezu alle Institutionen vor die Herausforderung gestellt, ihren Geschäftsbetrieb unter erschwerten Bedingungen aufrecht zu erhalten. Ein Notfallmanagementsystem bzw. Business Continuity Management System (BCMS) ist hierzu das Werkzeug der Wahl. Der modernisierte BSI-Standard 200-4 liefert Institutionen eine praxisnahe und adaptierbare Anleitung zum Aufbau und dauerhaften Betrieb eines BCMS.

Tritt in einer Institution eine Krise oder ein Notfall auf, ist meist schnelles Handeln erforderlich. Menschliches Leben muss gerettet, Schadensereignisse eingedämmt, alternative Lieferanten gefunden und der Geschäftsbetrieb „irgendwie“ fortgeführt werden, damit eine Institution ein Schadensereignis übersteht.

Wurden im Vorfeld keine Vorkehrungen getroffen, müssen in der Krise ad hoc schnellstmöglich Lösungen gefunden werden. Die Strukturen im normalen Geschäftsbetrieb, kurz AAO, haben oft zu lange Entscheidungswege, um adäquat reagieren und existenzbedrohende Lagen abwenden zu können. Um dies zu vermeiden, wird im BCM eine Stabsstruktur (Besondere Aufbauorganisation – BAO) etabliert, so dass die Institution auch im Notfall reagieren und entscheiden kann.

ÜBERSICHT ÜBER DIE NOTFALLBEWÄLTIGUNG

Neben der BAO werden in einem BCM für die zeitkritischsten Prozesse alle Voraussetzungen geschaffen, um im Notfall in einen geregelten Notbetrieb zu gelangen und damit die Existenz der Institution zu gewährleisten. Hierzu werden im Vorfeld Pläne erstellt und Kontinuitätslösungen umgesetzt, um den Ausfall von Ressourcen (z.B. Mitarbeiterinnen und Mitarbeiter, Gebäude oder IT) zu kompensieren. Der Stab koordiniert die Aktivitäten, um in den Notbetrieb zu gelangen und diesen fortzuführen, bis der Normalbetrieb wieder möglich ist. Abbildung 1 zeigt beispielhaft, wie ein Schadensereignis mit Hilfe einer BAO und entsprechenden Notfallplänen mitsamt Kontinuitätslösungen in unterschiedlichen Phasen bewältigt werden kann. Nähere Details können den Beschreibungen aus dem BSI-Standard 200-4, Kapitel 2.3 „Ablauf der Notfallbewältigung“ entnommen werden.

SYNERGIEMÖGLICHKEITEN

Im Gegensatz zum BSI-Standard 100-4 zeigt der BSI-Standard 200-4 zahlreiche Synergiemöglichkeiten mit angrenzenden Themen und Managementsystemen in den Bereichen der Informationssicherheit (und hier insbesondere der BSI-Standard 200-X Reihe), der IT-Service Continuity und des Outsourcings auf. So können Ressourcen über die unterschiedlichen Disziplinen gebündelt werden. Der BSI-Standard 200-4 ist alleine oder in Kombination mit der BSI-Standard 200-x Reihe anwendbar.

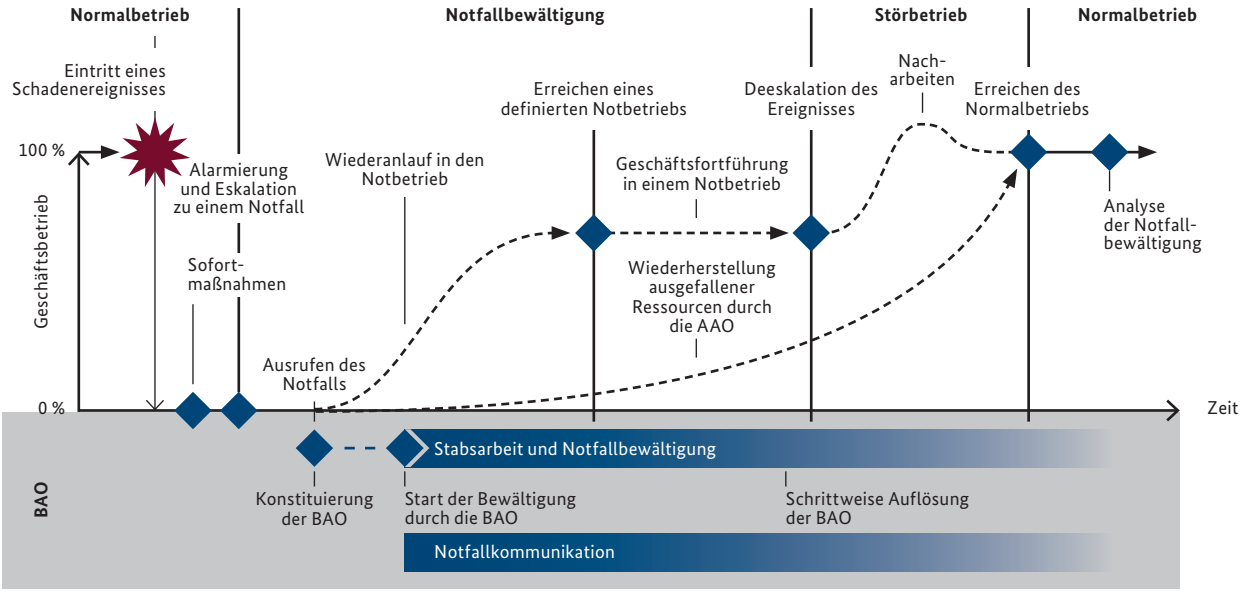


Abbildung 1: Bewältigung eines schwerwiegenden Schadensereignisses mit BCM

STUFENMODELL

Um den Anforderungen von großen Konzernen, mittelständischen Unternehmen und auch Behörden gerecht zu werden, führt der BSI-Standard 200-4 zusätzlich ein Stufenmodell ein, das besonders weniger erfahrenen Anwendern den Einstieg in das BCM erleichtert. Abbildung 2 zeigt die drei Stufen eines BCMS: Reaktiv-BCMS, Aufbau-BCMS und Standard-BCMS:

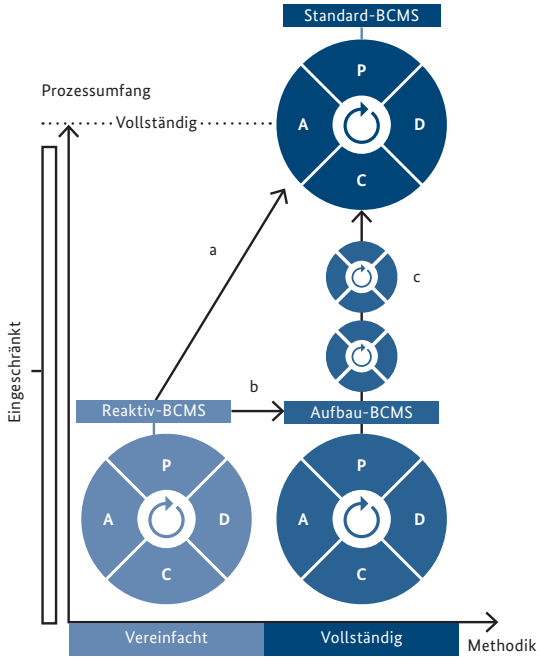


Abbildung 2: Übersicht über das Stufenmodell des BSI-Standards 200-4

Die jeweiligen Stufen unterscheiden sich hinsichtlich der anzuwendenden Methodik sowie des zu berücksichtigenden Prozessumfangs: Das **Reaktiv-BCMS** fokussiert einen möglichst schnellen Einstieg, in dem aufgrund einer stark vereinfachten Methodik nicht verweilt werden darf.
Es handelt sich um eine schnell realisierbare Einstiegsstufe, die eine Institution ohne zuvor implementiertes BCMS zu einer rudimentären Notfall- und Krisenbewältigung befähigt. Das **Aufbau-BCMS** erlaubt den schrittweisen Aufbau eines BCMS, um nicht in einem einzigen großen Schritt alle Geschäftsprozesse betrachten zu müssen. So können schneller wichtige Ergebnisse erreicht und die eigenen Ressourcen besser eingeteilt werden. Das Aufbau-BCMS fokussiert erst die zeitkritischsten Geschäftsprozesse, um dann sukzessive den Prozessumfang zu erhöhen, bis schlussendlich im Standard-BCMS alle Geschäftsprozesse untersucht und damit verbunden alle zeitkritischen Geschäftsprozesse auch angemessen abgesichert werden. Das **Standard-BCMS** stellt ein vollumfängliches, ISO 22301:2019 kompatibles BCMS dar. Das BSI empfiehlt ausdrücklich, über den zeitlichen Verlauf ein Standard-BCMS anzustreben, da nur so eine vollumfängliche, bedarfsgerechte Absicherung aller zeitkritischen Geschäftsprozesse sichergestellt werden kann. ■

IN KONTAKT BLEIBEN

Der Standard kann während der Community Draft-Phase kommentiert werden. Feedback können Sie gerne an grundschutz@bsi.bund.de richten. Weitere Informationen über alle BSI-Aktivitäten zum Thema BCM erhalten Sie über die BCM-Info-Gruppe.

Anmeldung zum Newsletter unter:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Weitere Informationen zum BSI-Standard 200-4 unter:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Brückenschlag zwischen CC-Zertifizierung und dem BSI-Zulassungsschema

Neue Methode regelt, wie vom BSI zertifizierte Produkte erfolgreich zugelassen werden können

von Dr. Frank Sonnenberg, Referat Zulassung von VS-Produkten

Das BSI ist gemäß § 4 Sicherheitsüberprüfungsgesetz (SÜG), §§ 51 und 52 Verschlusssachenanweisung (VSA) und § 3 BSI-Gesetz beauftragt, die Stärkung und Aufrechterhaltung der IT-Sicherheit im VS-Umfeld zu gewährleisten. Hierzu erteilt das BSI für IT-Sicherheitsprodukte, die zum Schutz von Verschlusssachen (VS) eingesetzt werden sollen, auf der Grundlage zuvor systematisch durchgeführter Evaluierungen jener Produkte Zulassungen. In Erfüllung dieses Auftrags steht das BSI jedoch einer tendenziell größer werdenden Herausforderung gegenüber.

Die IT-Sicherheit entwickelt sich in Zeiten voranschreitender Digitalisierung in immer kürzer werdenden technologischen Innovationszyklen weiter. Zeitgleich muss sich der bestehende kleine Markt zugelassener Produkte einer sich stets verändernden Bedrohungslage entgegenstellen. Dies gelingt zumindest zum Teil nicht mehr in angemessenem Umfang. Nicht zuletzt aufgrund der wachsenden Produktkomplexität ist eine zeitgerechte, vollständige Produktevaluierung und damit bedarfsgerechte Bereitstellung zugelassener IT-Sicherheitslösungen nicht immer möglich.

Um dieser Anforderung gerecht werden zu können, wird der Zulassungsprozess fortwährend weiterentwickelt, um enthaltene Optimierungspotentiale zu identifizieren und kürzere Reaktionszeiten zur Deckung des Bedarfs an VS-IT-Produkten zu ermöglichen („Time-To-Market“). Neben dem bereits seit 2017 erfolgreich etablierten Qualifizierten Zulassungsverfahren wurde 2019 erstmals eine Brücke zwischen der Zertifizierung von Produkten nach Common Criteria (CC) und dem BSI-Zulassungsschema geschlagen.

Dazu wurde das BSI-Zulassungsschema um einen ergänzenden Teilprozess – die sog. „Delta-Evaluierung“ – erweitert. In diesem werden die in einer früher positiv durchlaufenen BSI-Zertifizierung gewonnenen Evaluierungsergebnisse für die noch ausstehendenden Prüfaspekte im Rahmen der Zulassung wiederverwendet.

Das bedeutet, dass bereits zertifizierte Produkte, sofern diese grundsätzlich für den VS-Markt geeignet sind, ins Zulassungsschema überführt werden können. Diese Vorgehensweise ist sinnvoll, da die Zertifizierungsbeiträge zum einen schon den Großteil des Zulassungsaufwands ausmachen und zum anderen aufgrund gemeinsam verwendeter Kriterien und Methoden in ihrer Aussagekraft grundsätzlich vergleichbar sind.

Ebenso sind das grundsätzliche Evaluierungsprozedere und die Evaluierungsphilosophie von IT-Sicherheitsprodukten bei der Zertifizierung und Zulassung sehr ähnlich. Bestehende Abweichungen haben ihren Ursprung weniger in den Prüfkriterien selbst, als vielmehr in der

auf die jeweiligen Zielgruppen ausgerichteten Nutzung, Interpretation und Anerkennung der CC-Kriterien und ihrer Methodologie.

Während die Zertifizierung ihre Produktbewertungen i. d. R. im Sinne einer besseren Vergleichbarkeit an vordefinierten sog. „Assurance Packages“ gemäß EAL-Tabelle der CC ausrichtet, orientieren sich die Vertrauenswürdigkeitsaspekte in der Zulassung nach den Geheimhaltungsgraden des SÜG, bzw. der VSA.

Die besondere und erstmalig mit diesem Verfahren erfüllte Herausforderung liegt darin, die unterschiedlichen Paradigmen von Zertifizierung und Zulassung einander anzugleichen. Dazu wird die in der Zertifizierung geforderte normative Beschreibung der Sicherheitsfunktionalität auf Basis von „Security Functional Requirements“ aus den CC Part 2 in die deskriptive Formulierung von Sicherheitsanforderungen und -funktionen, wie sie in VS-Anforderungsprofilen und „Security Targets“ für die Zulassung definiert sind, überführt. Die für das Integrationsverfahren definierten Kriterien erlauben nach dieser Transition die Wiederverwendung der in der Zertifizierung gewonnenen Evaluierungserkenntnisse für die Zulassung in effizienter Weise.

Prüfaspekte, die nicht Gegenstand einer CC-Zertifizierung sind, jedoch für eine Zulassung essenzielle Bedeutung haben, werden mittels einer Delta-Evaluierung im Rahmen eines Zulassungsverfahrens ergänzend bewertet. In der Regel ist der dabei zusätzlich anfallende Aufwand signifikant geringer als bei einer herkömmlichen Zulassung nicht-zertifizierter Produkte. Die auf der Zertifizierung aufbauenden Prüfaspekte betreffen dabei Nachweisführung und Evaluierung hinsichtlich folgender Zulassungskriterien:

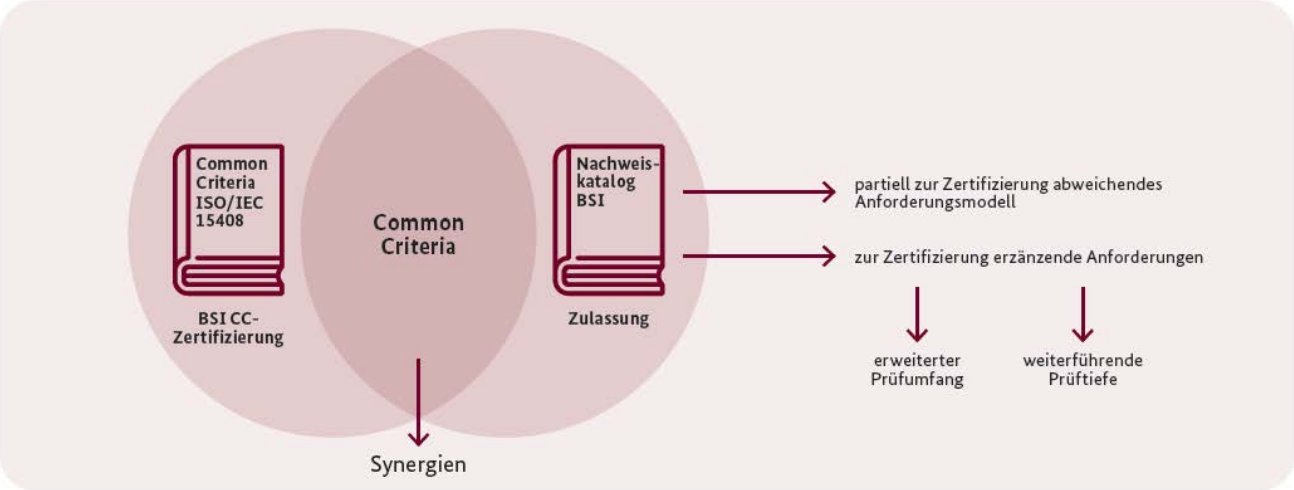
- Erfüllung gültiger VS-Anforderungsprofile
- Stärke bzw. Wirksamkeit der implementierten Kryptografie
- Anforderungen an die unterliegende Ablaufplattform
- Abstrahlsicherheit (VS-VERTRAULICH und höher)
- Vertrauenswürdigkeit von Produktherstellern

Initiiert werden kann ein solches Integrationsverfahren, wie jedes Zulassungsverfahren, nur dann, wenn ein Bedarf des bereits zertifizierten IT-Sicherheitsproduktes auch für das VS-Umfeld vorhanden ist. Hier findet der im Zulassungsschema dokumentierte herkömmliche Antrags- und Genehmigungsprozess für Zulassungsverfahren Anwendung.

Die Vorteile einer Nutzung bereits vom BSI zertifizierter IT-Sicherheitsprodukte liegen auf der Hand:

- Die Nutzung bereits aus der BSI-CC-Zertifizierung bekannter und geprüfter IT-Sicherheitsprodukte zur Bedarfsdeckung des VS-Marktes.
- Eine effektive und zeitnahe Erweiterung des VS-Produktkatalogs durch Berücksichtigung eines ursprünglich nicht im VS-Fokus stehenden IT-Sicherheitsmarktes.
- Eine effiziente Methode zur Generierung von Evaluierungsergebnissen für die Zulassung durch Nutzung von Synergieeffekten aus dem Zertifizierungs- und Zulassungsschema.

In ersten Validierungsverfahren konnte bereits nachgewiesen werden, dass eine Überführung der bereits in der Zertifizierung erzielten Prüfergebnisse in das Zulassungsschema leicht möglich ist, und so mit der Durchführung einer minimalen Delta-Evaluierung eine Zulassungsaussage für das IT-Sicherheitsprodukt erreicht werden kann. Dies bedeutet eine signifikante Reduzierung des erforderlichen Prüfaufwands und der Verfahrensdauer im Vergleich zur Durchführung eines vollständigen Zulassungsverfahrens. ■



Prinzipielle Aspekte zulassungsspezifischer Anforderungen zur Integration CC-zertifizierter Produkte in das Zulassungsschema des BSI

Sichere, zeitgemäße Kommunikation innerhalb der Netze des Bundes mit Wire

Bereits mehr als 30 Ministerien und Behörden nutzen den Messenger Wire für VS-NfD, Tendenz steigend

von Dr. Friederike Laus, Referat Prüfung von Kryptoverfahren, und Dr. Matthias Peter, Referat Sichere mobile Lösungen – Technologiebereich II

Moderne Messenger sind aus unserem Alltag nicht mehr wegzudenken. Für einen VS-NfD-zugelassenen Einsatz in Bundesbehörden evaluiert das BSI seit Ende Februar den Messenger Wire. Während der Einsatz von Wire zunächst auf die Netze des Bundes beschränkt ist, soll die Nutzung in einer weiteren Phase des Projektes auch auf das offene Netz ausgeweitet werden.

VIELFALT AN MESSENGERLÖSUNGEN

Nicht zuletzt die COVID-19-Pandemie hat den meisten von uns die große Vielfalt an Messengern und Audio/Video-Konferenzlösungen eindrucksvoll vor Augen geführt. Die Auswahl reduziert sich jedoch drastisch, wenn neben Benutzerfreundlichkeit auch Aspekte wie IT-Sicherheit oder Datenschutz eine Rolle spielen und Informationen ausgetauscht werden sollen, die nach der VSA „VS - Nur für den Dienstgebrauch“ eingestuft sind. Für eine sichere Kommunikation zwischen Teilnehmerinnen und Teilnehmern innerhalb der Netze des Bundes (NdB) und dem offenen Netz bleibt schließlich keine der modernen Lösungen übrig. Insbesondere die letzten beiden Aspekte haben Ende Februar zum Start des Projektes „Wire für VS-NfD“ geführt, in dessen Zusammenhang sich seitdem mehrere Referate des BSI intensiv mit dem Messenger Wire beschäftigen. Tatsächlich stammt die ursprüngliche Initiative für den Anstoß des Projektes aus dem Bundeskanzleramt, welches den Wire-Messenger für eine zeitgemäße VS-NfD-Kommunikation im Rahmen der EU-Ratspräsidentschaft, deren Vorsitz Deutschland im zweiten Halbjahr 2020 innehat, verwenden wollte.

MESSENGER WIRE UND DAS DOUBLE-RATCHET-PROTOKOLL

Bei Wire handelt es sich um einen Instant Messenger, der auf Smartphones und Tablets sowie auf Windows-, macOS- und Linux-Computern verwendet werden kann.

Im Kontext der Evaluierung wird die Enterprise-Version der Wire-App betrachtet, die sich jedoch in den wesentlichen kryptographischen Bestandteilen nicht von der Standardversion unterscheidet. Die Hauptfunktionalität der Wire-App ist das Versenden von Nachrichten, Bildern oder anderen Dateien zwischen zwei Nutzerinnen oder Nutzern, auch Gruppenchats sind möglich. Sämtliche Nachrichten zwischen den am Chat Teilnehmenden sind Ende-zu-Ende-verschlüsselt und werden auf bis zu acht Nutzerendgeräten synchronisiert. Die Kommunikation zwischen der App und dem Backend-Server in den NdB ist ferner TLS-verschlüsselt. Für die Nachrichtenverschlüsselung wird das vom Messenger-Signal bekannte Double-Ratchet-Protokoll [1] verwendet, welches mit leichten Modifikationen auch in anderen Messengern zum Einsatz kommt und heutzutage von mehr als einer Milliarde Menschen weltweit genutzt wird. Das Protokoll besteht im Wesentlichen aus drei Phasen: einem initialen Schlüsselaustausch (X3DH, „Extended Triple Diffie-Hellman“) zur Erzeugung eines gemeinsamen Geheimnisses sowie einer asymmetrischen und einer symmetrischen „Ratsche“, die dem Protokoll auch seinen Namen geben. Eine der grundlegenden Ideen des Protokolls ist, mit jeder Nachricht auch immer wieder neue Schlüssel auszutauschen. Das Schlüsselmaterial wird also quasi „vorwärtsgeratscht“, so dass es für einen Angreifer nicht möglich ist, von einem späteren zu einem früheren Zeitpunkt zurückzukehren und vorangegangene Nachrichten zu entschlüsseln. Eine vereinfachte Darstellung der asymmetrischen Ratsche ist in Abbildung 1 erläutert. Die Sicherheit des Protokolls, welches derzeit als State-of-the-Art im Bereich des Messagings gilt, wurde inzwischen in einer Reihe von Forschungsarbeiten analysiert (u. a. [2], [3]). Ferner ist es mit Wire möglich, Ende-zu-Ende verschlüsselte (Gruppen-) Telefonate sowie in kleinem Rahmen auch Videokonferenzen zu führen. Hierbei kommt das WebRTC-Protokoll zum Einsatz.

REFERATSÜBERGREIFENDE ZUSAMMENARBEIT

Nicht nur theoretisch, sondern auch praktisch wurde die Wire-App intensiv getestet, und so konnte rechtzeitig vor Beginn der EU-Ratspräsidentschaft Anfang Juni eine VS-NfD-Freigabeempfehlung für den On-Premise-Einsatz von Wire in der Bundesverwaltung erteilt werden. Diese erstreckte sich zunächst auf die Nutzung der App auf Desktop-PCs sowie SecuSUITE for Samsung

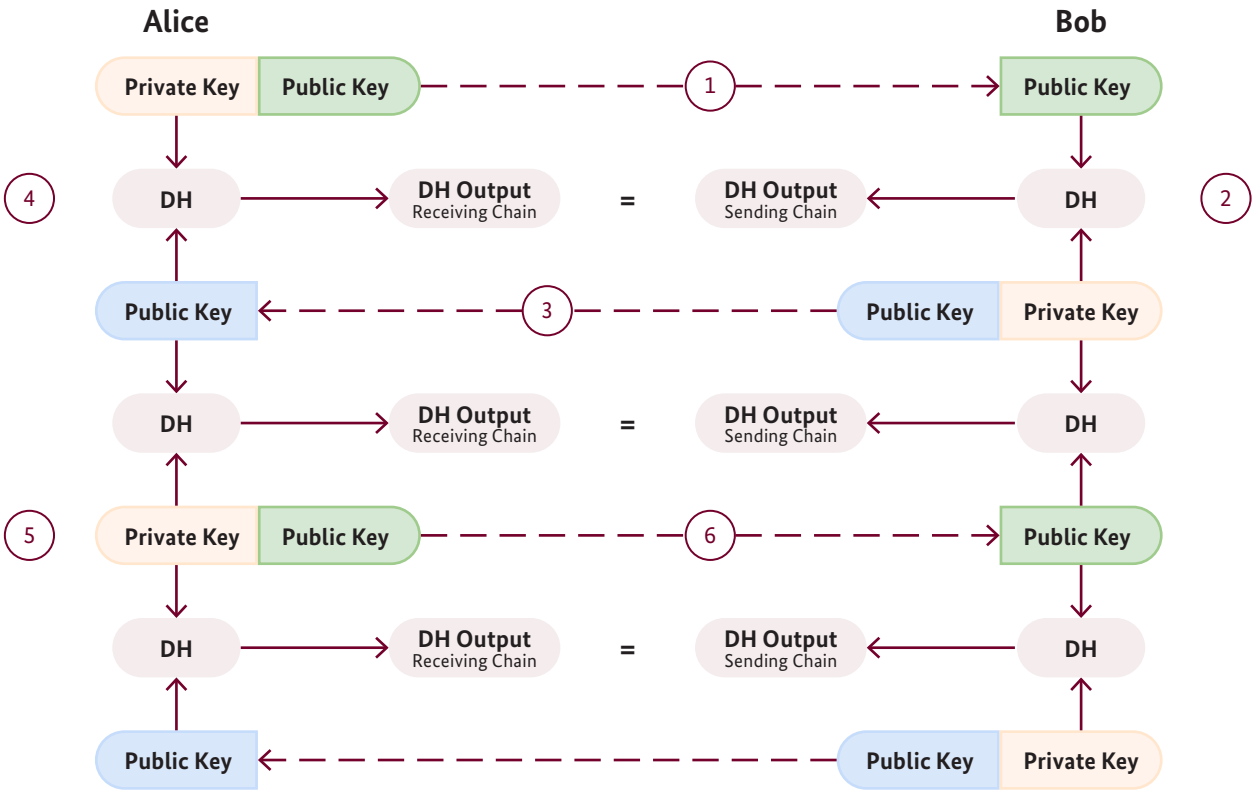


Abbildung 1: Die gemeinsamen Diffie-Hellman-Geheimnisse werden genutzt, um mit Hilfe der symmetrischen (Sending und Receiving) Ratschen Schlüssel zum Ver- und Entschlüsseln der Nachrichten zu berechnen. Dabei entspricht Alices Sending Ratsche Bobs Receiving Ratsche und umgekehrt.

1.) Alice sendet eine Nachricht zusammen mit ihrem Public Key an Bob
2.) Bob berechnet mit Alices Public Key und seinem Private Key ein gemeinsames Diffie-Hellman-Geheimnis
3.) Bob sendet seinen Public Key zusammen mit seiner nächsten Nachricht an Alice
4.) Alice berechnet mit Bobs Public Key und ihrem Private Key das gemeinsame Diffie-Hellman-Geheimnis
5.) Alice generiert ein neues Key Pair
6.) Alice sendet eine Nachricht zusammen mit ihrem neuen Public Key an Bob

Knox-Geräten (Android) und wurde Anfang Oktober um SecurePIM Government SDS (iOS-Systemlösung) erweitert. Der Messenger stieß auf erfreulich positive Resonanz und war bereits nach kurzer Zeit vielerorts im Einsatz. Derzeit wird er in 30 Ministerien und Behörden von insgesamt rund 5.000 Nutzerinnen und Nutzern verwendet (Stand: Oktober 2020); darunter ist auch das BSI. Gleichzeitig ist das Projekt auch ein gutes Beispiel für eine gelungene, referatsübergreifende Zusammenarbeit. Seien es Referat KM 12 hinsichtlich Zulassungsfragen, Referat KM 15 für Aspekte der VS-IT, Referat KM 22 für kryptographische Themen, die Referate KM 23 (iOS) und KM 24 (Android) von Seiten der mobilen Lösungen, Referat KM 13 für EU/NATO-Belange oder die Referate BL 33 und BL 34 für die Netzanbindung – viele Kolleginnen und Kollegen waren und sind in das Projekt involviert und mit großem Engagement bei der Sache. In der Tat wäre der knappe Zeitplan nicht einzuhalten gewesen, wenn nicht jede und jeder Einzelne auch mal über Referatsgrenzen hinweg Aufgaben übernommen und Unterstützung geleistet hätte.

WEITERE PROJEKTENTWICKLUNG

Mit dem Erteilen der Freigabeempfehlung ist das Projekt Wire aber noch lange nicht abgeschlossen. Aktuell stehen eine Weiterentwicklung des Produktes sowie eine deutlich tiefergehende Evaluierung an, die eine VS-NfD-Zulassung zum Ziel hat und aufgrund der Kürze der Zeit zuvor nicht möglich war In diesem Kontext soll beispielsweise das Double Ratchet-Protokoll durch den so genannten MLS-Standard (Messaging Layer Security) ersetzt werden. [4] Eines der Hauptanliegen bei der Entwicklung des Standards war, verschiedene Messaging-Protokolle soweit zu vereinheitlichen, dass unterschiedliche Anwendungen den Quellcode wiederverwenden können und insbesondere einheitliche Sicherheitsanalysen einfacher möglich werden. Neben der Firma Wire sind an der Erstellung des Standards eine Reihe namhafter Unternehmen (u. a. Mozilla, Twitter, Cisco, Google, Facebook) sowie Forschungseinrichtungen (INRIA) und Universitäten (MIT, University of Oxford) beteiligt.

Als weiterer Meilenstein des Projektes ist schließlich die Föderation mit dem offenen Netz geplant, so dass nicht nur innerhalb der Behördennetze, sondern auch netzübergreifend kommuniziert werden kann.
Zwar sind bis dahin noch einige Herausforderungen zu meistern, doch am Ende des Weges steht hoffentlich ein modernes Produkt, das eine zeitgemäße und gleichzeitig sichere Kommunikation zwischen Behörden und Bürgerinnen und Bürgern ermöglicht. ■

Abbildung 2: Beispiel für einen Chatverlauf in Wire.

Weitere Informationen zum Projekt und den Ergebnissen unter:

https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf

https://eprint.iacr.org/2018/1037.pdf

https://eprint.iacr.org/2016/1013.pdf

https://datatracker.ietf.org/wg/mls/about/

BSI IM GESUNDHEITSWESEN

Sonderthema: Cyber-Sicherheit im Gesundheitswesen

Vorwort von Bernd Kowalski, Leiter der Abteilung Cybersicherheit in der Digitalisierung und für elektronische Identitäten

Am 10. September 2020 kam es zu einem IT-Sicherheitsvorfall im Universitätsklinikum Düsseldorf. Ein Cyber-Angriff legte die Notfallversorgung der Klinik lahm, die daraufhin 13 Tage von der Akutversorgung abgemeldet war. Das BSI richtete sofort einen kontinuierlichen Kontakt zwischen dem Universitätsklinikum Düsseldorf und dem Cyber-Abwehrzentrum ein und unterstützte die Verantwortlichen des UKD vor Ort mit einem mobilen Einsatzteam.

Der Vorfall zeigte erneut, welch herausragende Bedeutung der Gestaltung der Cyber-Sicherheit im Gesundheitswesen zukommt. Nicht nur bedrohen IT-Sicherheitsvorfälle in diesem Bereich der Kritischen Infrastrukturen im Ernstfall Leib und Leben. Sondern von einer sicher gestalteten Digitalisierung profitieren alle Akteure im Gesundheitswesen – von den Patienten über die Kliniken bis zu den Krankenkassen. Digitale Gesundheitsfürsorge kann das Leben der Menschen erleichtern, lange Wege und Wartezeiten minimieren und im Krankheitsfall oder Notfall schnell unterstützen. Deshalb ist die Digitalisierung des Gesundheitswesens ein zentrales Zukunftsthema. Doch alle Vorteile von eHealth sind ohne Informationssicherheit nicht denkbar.

In dieser Ausgabe des BSI-Magazins möchten wir einige der Anwendungsfelder vorstellen, die aktuell im Fokus unserer Arbeit für die Digitalisierung im Gesundheitswesen stehen: die Corona-Warn-App, die Weiterentwicklung der elektronischen Gesundheitskarte, das Notfalldatenmanagement und der elektronische Medikationsplan im Zusammenhang mit der Arzneimitteltherapiesicherheit , die elektronische Patientenakte , die Telematikinfrastruktur sowie die IT-Sicherheit von Medizinprodukten mit dem Projekt ManiMed - Manipulation von Medizinprodukten.

Das BSI unterstützt in all diesen Anwendungsfeldern mit Vorgaben, Technischen Richtlinien sowie Hilfe für Behörden und Unternehmen, um zügig zu praktikablen und zugleich sicheren Lösungen zu finden. Eine enge Zusammenarbeit mit Partnern wie der gematik, dem Bundesministerium für Gesundheit (BMG), dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie dem Bundesinstitut für Arzneimittel und Medizinprodukte ist dabei selbstverständlich. Damit auch und gerade im Gesundheitswesen die Chancen der Digitalisierung sicher genutzt werden können.

Transparent, sicher, sinnvoll

Digitale Gesundheitsanwendungen

von Tim Griese, Stab Strategische Kommunikation und Presse, Dr. Dina Truxius, Alexandra Mayer, Emanuel Müller und Christian Kleinmanns, Referat Cyber-Sicherheit im Gesundheits- und Finanzwesen

Der Gesundheitsbereich ist ein Schwerpunkt der Digitalisierung in Deutschland. Die elektronische Patientenakte, die Messung, Speicherung und Auswertung von Gesundheitsdaten per App und die Video-Sprechstunde – das sind nur einige Beispiele für digitale Technologien, die derzeit die deutsche Gesundheitswirtschaft umgestalten. Auch die bereits 17 Millionen Mal heruntergeladene Corona-Warn-App gehört in diese Kategorie von Anwendungen. Das BSI stand den Entwicklern von Anfang an beratend zur Seite, um bei jedem Schritt ein Höchstmaß an IT-Sicherheit zu gewährleisten.

Nach § 33a Sozialgesetzbuch Fünf (SGB V) haben gesetzlich Krankenversicherte unter bestimmten Voraussetzungen einen Anspruch auf Versorgung mit sogenannten digitalen Gesundheitsanwendungen. Diese „Apps auf Rezept“ erleichtern die Kommunikation zwischen den einzelnen Akteuren des Gesundheitswesens und ermöglichen es der einzelnen Patientin oder dem einzelnen Patienten, die eigene Gesundheit besser zu steuern, etwa durch Apps, die Pulsfrequenz oder Schlafrhythmus messen, Symptome analysieren oder den Arztkontakt herstellen.

Digitale Gesundheitsanwendungen verbinden die Nutzerin und den Nutzer mit entsprechenden Services und fungieren als Kommunikations-Knotenpunkte. Ihre Basis sind die medizinischen Daten der versicherten Person, die mittels moderner Informations- und Kommunikationstechnologien zwischen Ärzten und Patienten, aber auch zwischen den einzelnen Leistungserbringern ausgetauscht werden können.

Die Gesundheitsanwendungen verarbeiten sensible und besonders schützenswerte persönliche Daten. Kann ein Angreifer Gesundheitsdaten eines Dritten manipulieren und damit deren Integrität verletzen, könnte das wesentlichen Einfluss auf Therapieentscheidungen und letztlich die Gesundheit der oder des Betroffenen haben.

Das BSI hat daher unabhängig von COVID-19 bereits 2019 eine Technische Richtlinie (TR) entwickelt und im April 2020 veröffentlicht, die bei Anwendung den Zugriff Unbefugter auf diese Daten erschwert. Die TR „Sicherheitsanforderungen an digitale Gesundheitsanwendungen“ (BSI TR-03161) kann grundsätzlich für alle mobilen Anwendungen, die sensible Daten verarbeiten und speichern, verwendet werden.

Die TR kann von Entwicklerinnen und Entwicklern mobiler Anwendungen im Gesundheitswesen als Leitfaden bei der Erstellung sicherer mobiler Applikationen genutzt werden. Sie wendet sich an Herstellerinnen und Hersteller von digitalen Gesundheitsanwendungen für mobile Endgeräte. Sie definiert den Stand der Technik und kann zukünftig beispielsweise im Rahmen einer Herstellererklärung oder als Grundlage für eine Zertifizierung genutzt werden.

DIE CORONA-WARN-APP

Auch die seit dem 16. Juni 2020 in den App-Stores von Apple und Google kostenlos zum Download verfügbare Corona-Warn-App des Bundes (CWA) ist vom Grundsatz her eine mobile Gesundheitsanwendung. Ihr großer Erfolg – bis Ende August 2020 haben mehr als 17 Millionen User die App heruntergeladen – setzt auch international Maßstäbe, wie selbst Großbritanniens Premier Boris Johnson anerkennen musste. Als er am 24. Juni 2020 im britischen Unterhaus vor der Opposition ausführte, kein Land der Welt habe eine funktionierende Tracing-App, wurde er von Oppositionsführer Keir Starmer korrigiert: Doch, Deutschland.

Nachdem eine zunächst geplante europäische Lösung mit zentraler Datenspeicherung von der Bundesregierung abgelehnt worden war, wurden die Deutsche Telekom und SAP beauftragt, eine App mit dezentraler Datenspeicherung zu entwickeln und zur Marktreife zu bringen. Die App sollte mit anderen europäischen Lösungen kompatibel sein. Nach Fertigstellung wurde die Corona-Warn-App vom Robert Koch-Institut (RKI) herausgegeben.

Die Corona-Warn-App nutzt Bluetooth, um den Abstand und die Begegnungsdauer zwischen Personen zu messen, die diese App installiert haben. Die Smartphones „merken“ sich Begegnungen, wenn die vom Robert Koch-Institut (RKI) festgelegten Kriterien zu Abstand und Zeit erfüllt sind. Dann tauschen die Geräte untereinander Zufallscodes aus. Werden Personen, die diese App nutzen, positiv auf COVID-19 getestet, können sie mithilfe der App freiwillig andere Nutzer darüber informieren.

Das BSI hat bei der Entwicklung der Corona-Warn-App und des zugehörigen umfassenden Sicherheitskonzeptes von Anfang an beratend zur Seite gestanden, um bei jedem Schritt ein Höchstmaß an IT-Sicherheit zu gewährleisten. Eine kurzfristig eingerichtete Taskforce arbeitete mit den Entwicklerinnen und Entwicklern der App bei SAP und Telekom ebenso wie mit der Fraunhofer-Gesellschaft, dem Helmholtz-Zentrum für Informationssicherheit CISPA und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) interdisziplinär zusammen. So unterstützte das BSI den Open-Source-Entwicklungsprozess etwa durch Code Reviews und Penetrationstests des zur Verfügung gestellten Codes von Frontend und Backend. Alle gefundenen Schwachstellen wurden und werden nach wie vor transparent gemacht und im engen Austausch mit der Bundesregierung, dem Robert Koch-Institut und den Entwicklerinnen und Entwicklern der App beseitigt. Kritische und schwerwiegende Schwachstellen wurden bereits vor dem Launch der App behoben.

Um die für eine breite Akzeptanz notwendige Transparenz herzustellen, wurden die Konzeption und der Programmcode (Quelltext) der App sowie die zugrundeliegende Server-Architektur und auch andere Dokumente zu den Funktionen der App auf der Entwicklungsplattform GitHub veröffentlicht (Open Source). Interessenten konnten so die Entwicklung und Programmierung der App nachvollziehen und an der Gestaltung mitwirken.

Die Expertinnen und Experten des BSI waren zudem maßgeblich an der Erarbeitung und Umsetzung des Sicherheitskonzepts beteiligt. Die Corona-Warn-App ist einfach zu bedienen, technisch auf dem neuesten Stand und datenschutzrechtlich unbedenklich. Sie zeigt aber auch, dass Informationssicherheit kein Hemmschuh bei Digitalisierungsprojekten ist. Im Gegenteil: Mit hohen Sicherheitsstandards kann man viele Anwenderinnen und Anwender erreichen und insbesondere die Akzeptanz entscheidend erhöhen. Nach einer Studie der Universität Oxford fängt eine Tracing-App zu wirken an, sobald 15 Prozent der Bevölkerung mitmachen (https://jme.bmj.com/content/46/7/427). Diesen Wert hat die CWA bereits nach wenigen Wochen erreicht. Das BSI wird die weitere Entwicklung der Corona-Warn-App hinsichtlich ihrer IT-Sicherheitseigenschaften auch im Produktiveinsatz eng begleiten.

DIGITALES GESUNDHEITSWESEN SICHER GESTALTEN

Das BSI beschäftigt sich kontinuierlich damit, in welchen Anwendungsfeldern der Digitalisierung Risiken entstehen könnten, und wie diese Risiken kalkulierbar und beherrschbar gemacht werden können. Ein Beispiel dafür ist die Weiterentwicklung der elektronischen Gesundheitskarte (eGK). Hier liegt der Fokus derzeit auf der Entwicklung und dem Einsatz von neuen Anwendungen wie zum Beispiel dem Notfalldatenmanagement (NFDM) und dem elektronischen Medikationsplan (eMP) im Zusammenhang mit der Arzneimitteltherapiesicherheit (AMTS) sowie der elektronischen Patientenakte (ePA) (siehe auch Artikel „Starker Aufwind für die Digitalisierung im Gesundheitswesen“ auf Seite 18).

Das BSI hat auch hier entsprechende Technische Richtlinien verfasst (TR 03154, TR 03155, TR 03157). Sie definieren den Stand der Technik und dienen der Überprüfung, ob die u. a. in Arztpraxen und Krankenhäusern im Einsatz befindlichen Konnektoren die mit dem BSI abgestimmten Anforderungen der gematik erfüllen.

So können zukünftig Daten für den medizinischen Notfall und elektronische Medikationspläne auf der eGK sicher gespeichert und im Notfall abgerufen werden. Im Fall des elektronischen Medikationsplans können bei neu zu verschreibenden Medikamenten durch die behandelnde Ärztin oder den behandelnden Arzt Wechselwirkungen mit bereits bestehenden Medikationen abgeglichen werden, und dadurch mögliche Risiken minimiert werden.

In einem weiteren Schritt steht gesetzlich Versicherten zusätzlich zu den bisherigen Funktionen eine elektronische Patientenakte (ePA) zur Verfügung, die sie freiwillig nutzen können. Gemäß dem am 14. März 2019 vom Bundestag beschlossen Terminservice- und Versorgungsgesetz (TSVG) sind alle gesetzlichen Krankenkassen verpflichtet, bis spätestens 2021 ihren Versicherten solche elektronischen Patientenakten anzubieten. Behandelnde Ärztinnen und Ärzte sowie Krankenhäuser können, nach Einverständnis und Freigabe durch die versicherte Person, auf die jeweilige Akte sicher zugreifen, um entsprechende medizinische Daten der Patientin oder des Patienten einzustellen oder einzusehen.

So können auch praxisübergreifende medizinische Behandlungen aufeinander abgestimmt werden, und für die Patientin oder den Patienten unter Umständen belastende Mehrfachuntersuchungen vermieden werden. Der Zugriff durch die Versicherten auf ihre individuelle Akte soll mittels eigener Geräte (PC, Smartphone oder Tablet) und einer Software ermöglicht werden. Zudem soll auch in öffentlich zugänglichen Geschäftsräumen der jeweiligen Krankenkassen die Möglichkeit geschaffen werden, mit einem gesicherten Gerät auf die eigene ePA zuzugreifen.

Ein weiterer Arbeitsschwerpunkt des BSI im Bereich Gesundheitsversorgung ist die IT-Sicherheit von Medizinprodukten. Das Projekt ManiMed - Manipulation von Medizinprodukten (siehe Artikel auf Seite 16) - startete Anfang 2019 und soll ein möglichst realistisches Abbild der Cyber-Sicherheitslage von vernetzten Medizinprodukten der folgenden Kategorien geben: Implantierbare Herzschrittmacher und Zubehör, Insulinpumpen, Beatmungsgeräte, Patientenmonitore und Infusionspumpen. Die Ergebnisse der sicherheitstechnischen Untersuchungen werden Ende 2020 veröffentlicht. Sie sollen langfristig in die Standardisierung und Normung einfließen und dem BSI bei der Erstellung technischer Richtlinien helfen.

BLAUPAUSE CORONA-WARN-APP

Wie die Corona-Warn-App leben auch viele andere Digitalisierungsprojekte des Bundes (nicht nur) im Gesundheitsbereich vom Vertrauen der Bürgerinnen und Bürger. Dieses Vertrauen entsteht durch Transparenz und bestmögliche Informationssicherheit. Das BSI bringt sich in die wesentlichen Digitalisierungsprojekte des Bundes gestalterisch ein, stellt dabei seine Expertise zur Verfügung und sorgt für ein Höchstmaß an Informationssicherheit.

Die Digitalisierung und Vernetzung im Gesundheitsbereich bringen Fortschritte, weil Patientinnen und Patienten umfassender betreut werden können, und die Kosten sinken. Aber sie bergen auch Gefahren, wenn IT-Sicherheit nicht vom ersten Schritt an mitgedacht und implementiert wird. Genau darum kümmert sich das BSI mit seiner über Jahrzehnte gewachsenen fachlichen Expertise, seiner Vernetzung mit allen Akteuren und seinem Engagement. ■

Gesucht:

Digitale Talente

(w/m/div.)

an den Standorten Bonn und Freital

Scannen und bewerben!

bsi.bund.de/jobs

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Sie begeistern sich für vielfältige, abwechslungsreiche und herausfordernde Aufgaben? Sie haben Spaß, Themen rund um die IT-Sicherheit im Team voranzubringen? Wir suchen Talente, deren Herz auf der digitalen Seite schlägt und die dazu beitragen wollen, dass die Menschen der digitalen Welt vertrauen können und die Digitalisierung eine Erfolgsstory wird.

Was Sie dafür mitbringen: Ein abgeschlossenes Studium in den Fachrichtungen Informatik, Wirtschafts- oder Verwaltungsinformatik, IT-Sicherheit oder IT-Management und Engagement für spannende Themen der Cyber-Sicherheit.

Besuchen Sie unsere Karriere-Seite auf **www.bsi.bund.de/karriere.**

Weitere Informationen: **bewerbung@bsi.bund.de** oder unter Tel.: 0228 99 9582 6388.

IT-Sicherheit und Schwachstellen in Medizinprodukten

Ergebnisse aus den BSI-Projekten eCare und ManiMed

von Dr. Dina Truxius, Referat Cyber-Sicherheit im Gesundheits- und Finanzwesen

Gehackte Medizinprodukte – eine befremdliche Vorstellung und ein Thema, das nicht nur Patientinnen und Patienten oder Ärztinnen und Ärzte, sondern auch die Menschen weltweit bewegt und betreffen kann. Die BSI-Projektarbeiten zeigen, wie es um die IT-Sicherheit von ausgewählten Produkten bestellt ist.

ECARE – DIGITALISIERUNG IN DER ALTENPFLEGE

Durch den Einzug von Digitalisierung und Vernetzung in das Gesundheitswesen werden vermehrt intelligente Systeme für den Alten- und Krankenpflegebereich produziert. All diese Produkte sollen Komfort und Entlastung für das Pflegepersonal bieten und den Patientinnen und Patienten idealerweise ein selbstbestimmteres und komfortableres Leben ermöglichen. Im Zuge des Projektes wurde zunächst eine Marktsichtung von Produkten erstellt, die in diesem Bereich in den letzten zwei Jahren angeboten wurden. Im Anschluss an die Marktsichtung wurden sechs Produkte aus verschiedenen Kategorien, wie z.B. Erinnerungsdienste oder Geräte zur Vitaldatenmessung, für das Pentesting ausgesucht (geringe Prüftiefe).

MANIMED – MANIPULATION VON MEDIZINPRODUKTEN

Die Sicherheit von Medizinprodukten bezieht sich in den meisten Fällen eher auf die Patientensicherheit als auf deren IT-Sicherheit. Der Trend zur Vernetzung betrifft jedoch zunehmend auch Medizinprodukte. Desgleichen haben die europäische und nationale Gesetzgebung das Thema im Fokus. Im Projekt ManiMed wurden je zwei vernetzte Medizinprodukte aus den folgenden fünf unterschiedlichen Geräteklassen sicherheitstechnisch untersucht (hohe Prüftiefe), da nicht alle auf dem Markt verfügbaren Produkte im Rahmen des Projektes getestet werden konnten:

- implantierbare Herzschrittmacher oder Defibrillatoren und deren Zubehör
- Insulinpumpen
- Beatmungsgeräte
- Patientenmonitore
- Infusionspumpen

Weitere Bedingungen der Marktsichtung waren, dass alle Produkte möglichst viele Schnittstellen aufweisen und nicht länger als fünf Jahre in Deutschland auf dem Markt sein sollten. Im Anschluss an die Marktsichtung wurden die Produkte entsprechend beschafft oder durch die Hersteller zur Verfügung gestellt und im Rahmen des Projektes getestet. Die Hersteller wurden über die Schwachstellenfunde und Gegenmaßnahmen informiert und ein koordinierter Prozess wurde gemeinsam durchgeführt.

FAZIT

Bei beiden Projekten wurden Schwachstellen unterschiedlicher Kritikalität für alle Produkte gefunden. In fast allen Fällen war die IT-Sicherheit und nicht die Patientensicherheit betroffen. Zu den kritischeren Schwachstellen gehörte beispielsweise die Offenlegung von sensiblen Geräte- oder Zugangsdaten. Die allermeisten Hersteller haben entsprechend reagiert, das Risiko bewertet, Updates bereitgestellt und die aktuellen Produkte und deren Nachfolgeprodukte hinsichtlich ihrer IT-Sicherheitseigenschaften verbessert.

Beide Projekte zeigten, dass der transparente und offene Umgang mit Schwachstellen und der entsprechende Kommunikationsaustausch notwendig sind, um langfristig Vertrauen aufzubauen, zu halten und zu stärken. Idealerweise fließen die Ergebnisse beider Projekte bereits in die Normung oder die standardisierten Vorgehensweisen ein und unterstützen das BSI bei der Erstellung technischer Richtlinien oder Empfehlungen. Auch im Anschluss an die Projektarbeiten sieht das BSI einen großen Bedarf an der Fortführung gemeinschaftlicher Arbeit zur Verbesserung von Cyber-Sicherheitseigenschaften. Projekte dieser Art gab es bisher weder auf nationaler noch auf internationaler Ebene. Daher sind die Ergebnisse wegweisend für das Vorgehen im Bereich der vernetzten Krankenpflege- und Medizinprodukte. ■

Starker Aufwind für die Digitalisierung im Gesundheitswesen

Aktuelle Entwicklungen in der Telematikinfrastruktur und Ausblick

von Alexandra Mayer, Referat Cyber-Sicherheit im Gesundheits- und Finanzwesen

In den letzten Jahren erhielt die Digitalisierung im Gesundheitswesen starken Aufwind. Um die verschiedensten Beteiligten in diesem Sektor zu vernetzen, wurde die Telematikinfrastruktur (TI) entwickelt. Das Kernstück der TI ist der Konnektor. Dieser sorgt für eine sichere Verbindung und ermöglicht somit die Vernetzung innerhalb des Gesundheitswesens. Der Konnektor ist für jede Arztpraxis, jede Apotheke, jedes Krankenhaus oder andere medizinische Einrichtungen der Anschluss zur TI.

Das Versichertenstammdatenmanagement (VSDM) ist eine der ersten Anwendungen der TI. Zur Aktualisierung der Versichertenstammdaten, die persönliche Daten und Angaben zur Krankenversicherung umfassen und auf der elektronischen Gesundheitskarte (eGK) der gesetzlich Krankenversicherten gespeichert sind, werden diese mit den Daten der Krankenkasse abgeglichen und aktualisiert. Hierfür wird die sichere Verbindung der TI genutzt.

AKTUELLE ENTWICKLUNGEN DER TI

Im Laufe des Sommers 2020 wurden für die Konnektoren Software-Updates bereitgestellt, die weitere Dienste der TI aktivieren: Das Notfalldatenmanagement (NFDM) ermöglicht jedem Versicherungsnehmer auf seiner eGK notfallrelevante medizinische Informationen zu speichern, die in einem Notfall für die behandelnde Ärztin oder den Arzt von größter Relevanz sein können. Neben Vorerkrankungen, Allergien und Medikation gibt es die Möglichkeit, im „Datensatz Persönliche Erklärung“ zu hinterlegen, ob medizinische Vollmachten, ein Organspendeausweis oder eine Patientenerklärung vorhanden sind, und wo diese zu finden sind. Diese Informationen können in einer Notfallsituation einen entscheidenden Unterschied für die Behandlung und somit den Versicherungsnehmer machen.

Neben dem NFDM wird der elektronische Medikationsplan (eMP) aktiviert und auf der eGK gespeichert. Der eMP soll alle verschreibungspflichtigen Arzneimittel enthalten, die eine Patientin oder ein Patient einnimmt, sowie die Selbstmedikation. Die Behandlung der versicherten Person soll erleichtert und verbessert werden, da verschiedene behandelnde Ärztinnen und Ärzte ihre Medikation besser aufeinander abstimmen und somit Wechselwirkungen vermeiden können.

Zusätzlich zu diesen beiden Diensten wird die Kommunikation zwischen verschiedenen Ärztinnen und Ärzten, Krankenhäusern, Apotheken, Kassenärztlichen Vereinigungen, Krankenkassen und anderen Einrichtungen durch Kommunikation im Medizinwesen (KIM) vereinfacht. Mit Hilfe von KIM kann die gesamte elektronische Kommunikation als sichere E-Mail verschickt werden. Dies können sowohl Arztbriefe und Befunde, als auch Arbeitsunfähigkeitsbescheinigungen sein. Die Authentizität der Dokumente ist durch die qualifizierte elektronische Signatur (QES), die mit einer Unterschrift gleichzusetzten ist, gewährleistet. KIM wird im Laufe der Zeit weiter ausgebaut, der Versand einer Arbeitsunfähigkeitsbescheinigung an die Krankenkassen ist beispielsweise für Anfang 2021 geplant.

DIE NAHE ZUKUNFT DER TI

Ab dem 1. Januar 2021 wird die elektronische Patientenakte (ePA) eingeführt. Die ePA soll die herkömmliche papiergebundene Patientenakte auf lange Sicht ablösen. Die versicherte Person hat dann nicht nur uneingeschränkten Zugriff auf ihre ePA und damit alle ihre medizinischen Daten, sondern kann frei entscheiden, welche Dokumente von wem angesehen und verändert werden dürfen. Protokolldaten können ebenfalls eingesehen werden, wodurch nachverfolgt werden kann, wer wann welche Daten geändert hat. Neben aktuellen Befunden und Behandlungen der versicherten Person wird auch die Möglichkeit geschaffen, Dokumente wie den Impfausweis zu speichern.

Zusätzlich hat die versicherte Person die Möglichkeit, über eine mobile Anwendung (App) und mit Hilfe eines persönlichen mobilen Endgerätes, auf die eigene ePA zuzugreifen. So können jederzeit von unterwegs die Patientendaten eingesehen werden. Auf diese Art wird die Informationshoheit der versicherten Person gewährleistet.

DIE FERNE ZUKUNFT DER TI

Ab dem 1. Juli 2021 wird das elektronische Rezept (E-Rezept) verfügbar sein. Rezepte werden von diesem Zeitpunkt an digital ausgestellt. Die Versicherten haben die Möglichkeit, Rezepte über eine App auf dem eigenen Smartphone zu verwalten. Das Rezept kann entweder direkt an die gewünschte Apotheke gesendet werden oder der entsprechende Token in der Apotheke vorgezeigt und gescannt werden. Die App ist selbstverständlich nicht verpflichtend, der Token kann vom verschreibenden Arzt ausgedruckt werden, so dass eine andere Art papiergebundenes Rezept vorliegt.

IT-SICHERHEIT DER ANWENDUNGEN

Die Anwendungen NFDM, eMP, ePA und E-Rezept werden alle auf freiwilliger Basis eingeführt. Medizinische Daten sind hoch sensible Daten und haben einen hohen Schutzbedarf. Um diesen Schutzbedarf erfüllen zu können, arbeiten BMG, gematik, BfDI und BSI gemeinsam an der Umsetzung des Projektes. Die Sicherheit der unterschiedlichen Anwendungen steht immer im Fokus der Entwicklung, wird fortwährend weiterentwickelt und auf dem aktuellen Stand der Technik gehalten. ■

Sicherheitslücke im Medizinprodukt entdeckt – was nun?

Der Coordinated-Vulnerability-Disclosure-Prozess hilft beim Umgang mit Schwachstellen

von Dr. Dina Truxius, Referat Cyber-Sicherheit im Gesundheits- und Finanzwesen

Schwachstellen in IT-Systemen können prinzipiell und zu jeder Zeit vorhanden sein. Selbst vor Medizinprodukten machen sie keinen Halt. Daher ist es wichtig, koordiniert vorzugehen und einem entsprechenden Prozess zu folgen, wenn Schwachstellen in (Medizin-) Produkten entdeckt werden.

Die Reife eines Unternehmens bezüglich der IT-Sicherheit wird einerseits daran gemessen, wie mit Schwachstellenmeldungen und Belangen der IT-Sicherheit umgegangen wird, aber auch daran, wie entsprechende Informationen kommuniziert und die daraus folgenden Handlungen koordiniert werden. Unternehmen, die in diesem Bereich Erfahrung haben, informieren ihre Kundinnen und Kunden und veröffentlichen Schwachstellen, sobald diese behoben sind. Dies geschieht auf internationaler Ebene in Form von Informationen an die entsprechenden Anwenderinnen und Anwender, durch ICS-Advisories, die vom CISA (Cybersecurity and Infrastructure Security Agency) in den USA erstellt und veröffentlicht werden sowie durch die Anmeldung von CVE (Common Vulnerabilities and Exposures). Das BSI unterstützt diese Transparenz, nutzt und integriert international etablierte Prozesse und steht daher in engem Austausch mit den amerikanischen Behörden, um kooperativ zu mehr koordinierter IT-Sicherheit beizutragen.

DER „RICHTIGE“ UMGANG MIT SCHWACHSTELLEN

Ein idealer Prozess hinsichtlich des Umgangs und der anschließenden Veröffentlichung von Sicherheitslücken ist gekennzeichnet durch ein hohes Maß an Gleichbehandlung, Kommunikation und Kooperation aller Beteiligten, unabhängig davon, ob es sich um ein vernetztes Medizinprodukt oder eine smarte Waschmaschine handelt. Die Beteiligten sind hierbei häufig Sicherheitsforscherinnen und -forscher, die eine Schwachstelle entdecken, oder die Hersteller des betroffenen Produkts. Je nach Produktkategorie und Verantwortungsbereich können gegebenenfalls auch die zuständige Behörde oder ein CERT (Computer Emergency Response Team) beteiligt sein.

Nach Erhalt der Information zu Schwachstellen bei einem Produkt ist wünschenswert, dass ein so genannter Coordinated-Vulnerability-Disclosure-Prozess (CVD) von allen Beteiligten durchgeführt wird. Dieser basiert auf vertrauensvollem Austausch und kontinuierlicher Zusammenarbeit. Während der gesamten Laufzeit des CVD erhält keine weitere Stelle, außer den Beteiligten, Kenntnis von den gefundenen Schwachstellen. Nach Abschluss des CVD soll transparent und offen über die Schwachstellen kommuniziert werden (Advisories etc.), um die IT-Sicherheit auf einem hohen Niveau zu halten und andere Hersteller über mögliche Schwachstellen zu informieren.

CVD-PROZESS AM BEISPIEL DES PROJEKTES MANIMED – MANIPULATION VON MEDIZINPRODUKTEN

Das Vorgehen im Projekt ManiMed (siehe Artikel auf S. 16) setzt auf die Gleichbehandlung der Hersteller und orientiert sich daher an einem CVD, bei dem die gefundenen IT-Sicherheitslücken vorerst nicht veröffentlicht werden (mind. 90 Tage). So hat der Hersteller Zeit, die Schwachstellen zu beheben und entsprechende Sicherheits-Updates zu entwickeln, diese zu überprüfen und auszurollen.

Im Projekt werden alle Produkte tiefgehenden IT-sicherheitstechnischen Prüfungen unterzogen. Die gefundenen Schwachstellen werden dem Hersteller in Form eines detaillierten Prüfberichts übermittelt, technisch beschrieben und ausführlich dargelegt. Im Prüfbericht werden bereits Mitigationsmaßnahmen vorgeschlagen, die einzelnen Schwachstellen werden nach CVSS V3 (Common Vulnerability Scoring System) klassifiziert und beziffert. Dieses System erlaubt eine Unterteilung der Schwachstellen in INFO, LOW, MEDIUM, HIGH und CRITICAL. Wobei kritische Schwachstellen umgehend behoben werden sollten. Alle Schwachstellen, die unter die Kategorie MEDIUM fallen, sind beim nächsten Update zu beheben. Sollten kritische Schwachstellen gefunden werden, die der Hersteller nicht beheben kann oder will, kann das BSI basierend auf seiner gesetzlichen Aufgabe nach § 7a BSIG den Hersteller zu einer Stellungnahme auffordern und gegebenenfalls gemäß § 7 BSIG verwarnen.

Der Hersteller erarbeitet dann aus dem vorliegenden Prüfbericht eine (Rest-) Risikoeinschätzung hinsichtlich “Safety and Security“ (Patienten- und IT-Sicherheit) sowie einen Zeitplan und leitet gegebenenfalls interne Prozesse ein. Sollte der Hersteller anhand der gefundenen Schwachstellen ein Patientenrisiko im Zuge seiner Risikoeinschätzung erkennen können, wird das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) als zuständige Aufsichtsbehörde in den Prozess einbezogen. Erst wenn die Schwachstellen behoben sind, sollen sie, in Absprache mit dem Hersteller, veröffentlicht und gegebenenfalls auf einschlägigen IT-Sicherheitskonferenzen vorgetragen werden. Der Hersteller darf sein getestetes Produkt im Anschluss an das Projekt weder als BSI-zertifiziert noch als BSI-geprüft bewerben, da weder Prüftiefe noch Umfang einer Zertifizierung entsprechen. Es gilt immer zu bedenken, dass selbst ein „frisch“ untersuchtes Produkt wieder mögliche Schwachstellen aufweisen kann. IT-Sicherheit ist ein kontinuierlicher Prozess, der während des gesamten Produktlebenszyklus beachtet werden sollte. ■

DAS BSI

Neuer IT-Studiengang „DACS“ an der Hochschule des Bundes

von Alessandra Krüger, Referat Personalentwicklung

Verschiedenste Cyber-Sicherheitsvorfälle der vergangenen Jahre, eine neue Qualiät an Cyber-Angriffen und die wachsende Digitalisierung von Staat, Wirtschaft und Gesellschaft zeigen, dass IT- und Cyber-Sicherheitsaspekte in der öffentlichen Verwaltung immer mehr an Bedeutung gewinnen. Die Ausbildung des passenden Nachwuchses für die IT-Sicherheit in der Bundesverwaltung leistet hierbei einen wertvollen Beitrag. Im Oktober 2020 ist daher der neue Studiengang „Digital Administration and Cyber Security“ (DACS) an der Hochschule des Bundes in Brühl gestartet. Neben anderen Behörden beteiligt sich auch das BSI mit ca. zehn Studienplätzen pro Jahr an den Auswahlverfahren sowie durch die Bereitstellung von Praktikumsplätzen. Ziel ist es, die Studierenden im Anschluss fest zu übernehmen. Der Schwerpunkt der BSI-Studierenden liegt dabei natürlich eher auf „Cyber-Security“ als auf „Digital Administration“.

VIELFÄLTIGE INHALTE

Vermittelt werden neben den Grundzügen von IT-Sicherheit, Forensik und Kryptographie auch Kenntnisse in IT-Projektmanagement und öffentlichem Recht – eine perfekte Ausrichtung auf die Bedarfe in den Behörden und damit auch auf die des BSI. Zwei halbjährige Praktika bei den Behörden vor Ort sorgen für eine Vertiefung des im Studium angeeigneten Wissens und unterstützen die Entscheidungsfindung der Studierenden für ein späteres Fachgebiet. Die Professorinnen und Professoren sind verwaltungserfahren und kennen die aktuellen Bedarfe und Standards der Bundesbehörden, welche sie den Studierenden praxisnah vermitteln.

DUAL STUDIEREN UND EIGENES GELD VERDIENEN

Die Studierenden befinden sich von Beginn ihres Studiums an in einem Beamtenverhältnis auf Zeit, verbunden mit einem Gehalt, das Stand 2020 etwas mehr als 1.500€ brutto beträgt. Im Gegensatz zu Hörsälen, die mit hunderten anderen Studierenden geteilt werden müssen, beträgt die Kursgröße nur 25 Personen. Im Rahmen freier Kapazitäten stehen Wohnheimplätze direkt an der Hochschule zur Verfügung, und den Studierenden bietet sich ein vielfältiges Sportangebot direkt auf dem Campus. Die Vorlesungszeiten von 08:00 Uhr bis 15:30 Uhr sind familienfreundlich. Das Studium wird mit einem Diplom-Verwaltungswirt abgeschlossen und ist praktisch mit einer Jobgarantie durch die jeweilige Praktikumsbehörde verbunden.

Die Bewerbung erfolgt über die Seite der Hochschule, weitere Infos sowie den Link zu der Ausschreibung finden Sie unter https://www.bsi.bund.de/karriere. ■

v.l. n.r.:
Thomas Seider, Dennis Brykin, Lukas Altmeier, Leonard Keding,
Gianluca Carcereri de Prati und Kay Kretschmar

Verstärkung der Cyber-Abwehrkräfte: Neuer BSI-Dienstsitz in Freital

Im Juli 2019 erfolgte der offizielle Startschuss für die Eröffnung des zweiten BSI-Standorts in Freital/Sachsen durch Bundesinnenminister Horst Seehofer und den sächsischen Innenminister Prof. Roland Wöller.

von Joachim Weber, Projektgruppe Aufbaustab Standort Sachsen

Das BSI ist eine tragende Säule der Sicherheitsarchitektur Deutschlands und damit zentraler Ansprechpartner für alle Angelegenheiten der Cyber-Sicherheit. Die Digitalisierung Deutschlands ist ohne die adäquate Berücksichtigung von Cyber-Sicherheit nicht denkbar, und daher ist eine entsprechende Einbindung des BSI in dieses wichtige Vorhaben unverzichtbar. Dem neuen Freitaler Dienstsitz des BSI mit seinen 200 Arbeitsplätzen kommt hierbei eine entscheidende Bedeutung zu. Die gegenwärtige Gestaltung der Digitalisierung wird geprägt von neuen Technologiebereichen wie z.B. den im Aufbau befindlichen 5G-Infrastrukturen oder auch dem digitalen Verbraucherschutz. Die Berücksichtigung der dabei anfallenden Cyber-Sicherheitsfragen und die Erarbeitung von praxisgerechten Lösungen zum Vorteil von Staat, Wirtschaft und Gesellschaft werden die Schwerpunktaufgaben der Freitaler BSI-Beschäftigten sein. Sie arbeiten hierbei sehr eng mit ihren BSI-Kolleginnen und -Kollegen in Bonn und Saarbrücken zusammen.

ZAHLREICHE FACHLICHE UND PROZESSUALE SCHNITTSTELLEN MIT ALLEN ABTEILUNGEN DES BSI

2019/20 hat das BSI eine tiefgreifende Umorganisation durchlaufen, die am 1. August 2020 offiziell in Kraft getreten ist. Das kennzeichnende Merkmal dieser Umorganisation ist die Schaffung einer integrierten BSI-Wertschöpfungskette, die Kompetenz- und Servicebereiche des BSI prozessorientiert und abteilungsübergreifend etabliert. Die am Standort Freital eingerichteten Organisationseinheiten zeichnen sich durch zahlreiche fachliche und prozessuale Schnittstellen mit allen Abteilungen des BSI aus. Während des Aufbaus des Standorts Freital werden diese internen Schnittstellen durch entsprechende Kontakte in Richtung Verwaltung, Wirtschaft und Gesellschaft ergänzt.

Die Organisation des Standorts Freital basiert ganz wesentlich auf der Einrichtung der beiden Fachbereiche SZ 3 und WG 3. Diese stehen für die Themenkomplexe „Cyber-Sicherheit in mobilen Infrastrukturen und Chiptechnologie“ sowie „Digitaler Verbraucherschutz, Cyber-Sicherheit für Gesellschaft und Bürger“. Die thematischen Schwerpunkte liegen zum einen in der Erarbeitung von technischen Grundlagen und Sicherheitsanforderungen mit Blick auf die neue 5G-Infrastruktur sowie der Durchführung regelmäßiger Audits, um die Einhaltung der einschlägigen BSI-Vorgaben sicherzustellen. Das BSI wird in diesem Zusammenhang z.B. entsprechende Netzwerkkomponenten zertifizieren und darüber hinaus die Bereitstellung chip-basierter eID-Technologien für mobile Anwendungsbereiche gewährleisten sowie ein entsprechendes IT-Sicherheitskennzeichen vergeben. Zum anderen wird der digitale Verbraucherschutz, soweit Fragen der Cyber-Sicherheit betroffen sind, durch den Aufbau von zwei spezialisierten Referaten mit zusätzlichen Organisationseinheiten für die Marktbeobachtung, einer Beratung sowie einem Service-Center für Cyber-Sicherheitsinformationen nachhaltig realisiert. Neben diesen beiden Fachbereichen, die in Freital durch insgesamt zehn Referate vertreten sind, gibt es darüber hinaus eine größere Anzahl weiterer BSI-Fachreferate, die mit ihren Bonner Abteilungen in enger Kooperation stehen und in Freital insbesondere regionale Bedarfslagen bedienen werden.

PERSONALGEWINNUNG UND SUCHE NACH NEUER LIEGENSCHAFT IN VOLLEM GANGE

Derzeit ist die Personalgewinnung für den Freitaler Dienstsitz in vollem Gange. Die ersten neuen Kolleginnen und Kollegen sind bereits eingestellt und werden am Hauptsitz des BSI in Bonn von den „Erfahreneren“ in ihre für sie in der Regel neuen Aufgaben intensiv eingearbeitet. Die individuell und mitarbeiterbezogen erstellten Einarbeitungskonzepte erleichtern dabei die Einarbeitungsphase, die nach ca. sechs Monaten abgeschlossen sein wird und anschließend zum Einsatz in Freital führt. Da die Freitaler BSI-Angehörigen nicht auf einmal eingestellt werden können, befindet sich eine größere Anzahl neu gewonnener Mitarbeiterinnen und Mitarbeiter über einen längeren Zeitraum in Bonn in der Einarbeitung. Für alle Beteiligten ist dies eine spannende wie auch herausfordernde Aufgabe.

Die zeit- und bedarfsgerechte Bereitstellung einer Liegenschaft für die neue Freitaler Außenstelle erweist sich ebenfalls als spannende Herausforderung, da die durch die Einstellungen ständig wachsende Anzahl an Mitarbeitenden unter Zeit- und Raumbedarfsgesichtspunkten synchronisiert werden muss. Hierzu arbeitet das BSI intensiv mit den örtlich zuständigen und sehr hilfreichen Stellen der Stadt Freital und der BImA (Bundesanstalt für Immobilienaufgaben) zusammen.

Die Eröffnung des zweiten BSI-Dienstsitzes in Freital bietet für den Bund wie auch für die Region Sachsen eine hervorragende Gelegenheit, in enger Kooperation mit allen Verantwortlichen die Cyber-Abwehrkräfte örtlich zu konzentrieren und zukunftsweisende Sicherheitsthemen mit wichtigen Impulsen von Behörden, Unternehmen und der Wissenschaft zu gestalten, zu bündeln und nachhaltig weiterzuentwickeln. ■

„Der Freistaat Sachsen möchte in der Cyber-Sicherheit eine führende Rolle übernehmen“

Ein Interview mit Staatssekretär Thomas Popp, der zugleich Beauftragter für Informationstechnologie (CIO) des Freistaates Sachsen ist.

■ **Lieber Herr Popp, Sie haben in Sachsen bis heute viele unterschiedliche Verwaltungsaufgaben übernommen. Was haben Sie aus diesem Erfahrungsschatz für sich und Ihre Arbeit als CIO des Freistaates mitgenommen?**

An den unterschiedlichen Stationen meiner beruflichen Laufbahn hatte ich immer mit Digitalisierung zu tun. Insbesondere in der Steuerverwaltung, die als Vorreiter der digitalen Revolution in der Verwaltung gilt, konnte ich mich umfassend in die Modernisierung und Digitalisierung der Verwaltungsprozesse einbringen. Dabei habe ich neben den fachlichen Erkenntnissen auch viel über Veränderungsprozesse insgesamt und wie Menschen in dieser Veränderung begleitet werden müssen, gelernt. Diese Erfahrungen helfen mir als Staatssekretär für Digitale Verwaltung und Verwaltungsmodernisierung natürlich auch bei der vor uns liegenden Aufgabe, die Verwaltung der Zukunft moderner und digitaler zu gestalten. In meiner über zwanzigjährigen Tätigkeit für den Freistaat habe ich viele interessante Menschen getroffen, die mir nützliche Impulse für meine Tätigkeit gegeben und mir auch oft eine neue Perspektive eröffnet haben. Gerade weil die anstehende digitale Transformation alle Bereiche betrifft und so grundlegende Veränderungen für alle mit sich bringt, ist es wichtig, einerseits zuzuhören, und sich andererseits auszutauschen.

■ **Als Bonner Bundesamt haben wir mittlerweile auch Wurzeln in Sachsen geschlagen. Was war für Sie der Grund zu sagen, wir bieten dem BSI im Freistaat eine zweite Heimat?**

Der Freistaat Sachsen möchte in der Cyber-Sicherheit eine führende Rolle übernehmen und in Zusammenarbeit mit Bund und Ländern sowie Wissenschaft und Wirtschaft zeigen, dass eine gebündelte Abwehr im Cyber-Raum effektiver ist, da Cyber-Bedrohungen nicht an Ländergrenzen Halt macht. Dafür steht die Landeshauptstadt und der Wirtschafts- und Innovationsstandort Dresden mit seiner Nähe zu Tschechien und Polen in besonderer Weise. Als größter Standort der Halbleiterindustrie in Europa bietet Dresden wichtige Anknüpfungspunkte für die Cyber-Sicherheit. Leipzig ist die Boomregion in Deutschland und verfestigt seinen Ruf als Technologiestandort. Aber auch abseits dieser beiden Metropolregionen stellt Sachsen durch seine Hochschullandschaft ein großes Potenzial an gut ausgebildeten Fachkräften zur Verfügung, gerade mit Blick auf die besonderen Qualifikationen in Bezug auf Cyber-Sicherheit. So ist es nur folgerichtig, das BSI hier in dieser Region stärker zu verorten und die Kooperation auch auf persönlicher Ebene zu festigen.

■ **Mit der Komm24 GmbH haben Sie eine eigene kommunale IT-Gesellschaft für den Freistaat gegründet, das Sächsische Verwaltungsnetz wurde jüngst vom BSI zertifiziert – zwei wichtige Meilensteine in Sachen Digitalisierung und IT-Sicherheit. Wie hilft das den Kommunen, der Wirtschaft und den Menschen vor Ort? Was unternimmt die Staatsregierung für die Informationssicherheit in Sachsen?**

Informationssicherheit ist einer der Grundpfeiler, auf denen die digitale Verwaltung aufbaut. Ohne umfassende Gewähr der Informationssicherheit wird uns ein erfolgreicher digitaler Transformationsprozess nicht gelingen. Nur wenn wir bspw. einfache digitale Zugänge zu Verwaltungsleistungen schaffen und gleichzeitig umfassende Informationssicherheit garantieren, werden diese Angebote durch Bürgerinnen und Bürger und Unternehmen auch genutzt. Das bedeutet ganz konkret, dass jedes digitale Verwaltungsangebot bereits in der Konzeptionsphase die Informationssicherheitsaspekte berücksichtigt, die dann in der Entwicklung und

technischen Implementierung umgesetzt werden. Zudem müssen Verwaltungsbedienstete sowie Nutzerinnen und Nutzer der Verfahren für Informationssicherheitsrisiken sensibilisiert werden, und zwar laufend. Für diese Aspekte mache ich mich in der aktuellen Legislaturperiode stark.

■ Das BSI wird in Freital vor allem die Sicherheit von Zukunftstechnologien weiterentwickeln. Aber auch der digitale Verbraucherschutz als neue BSI-Aufgabe wird von Sachsen aus vorangetrieben. Wo sehen Sie mögliche gemeinsame Handlungsfelder und Projekte von BSI und Einrichtungen in Sachsen?

Ich freue mich, dass es mit dem BSI einen kompetenten Akteur auf Bundesebene für den digitalen Verbraucherschutz gibt. Wie nötig das ist, zeigt eine von uns in Auftrag gegebene Umfrage zur Cyber-Sicherheit aus dem Jahr 2018: Die Bürger wünschen sich mehr Informationen und mehr Hilfsangebote. Sie wissen aber nicht, wen sie dazu befragen können. Ich erhoffe mir, dass das BSI diese Lücke füllen kann. Als Freistaat wollen wir dabei gern unterstützen. Vor den Einschränkungen im Zuge der COVID-19-Pandemie waren wir in Sachsen mit Sensibilisierungsveranstaltungen zur Cyber-Sicherheit unter dem Motto „Die Hacker kommen“ für Bürgerinnen und Bürger sehr aktiv. Allein im letzten Jahr haben wir 22 Veranstaltungen mit über 2.200 Teilnehmerinnen und Teilnehmern ausgerichtet. Im Fokus stand dabei auch der Europäische Aktionsmonat zur Cyber-Sicherheit, den das BSI in Deutschland koordiniert und an dem wir uns von Anfang an beteiligt haben.

■ Um ein Thema kommt man im Jahr 2020 nicht herum: Corona. Sie haben in einem Interview von einem neuen Drive im IT-Sicherheitsbereich im Zuge der Pandemie gesprochen. Was meinen Sie damit und wie haben Sie als Freistaat Sachsen diese schwierige Zeit gemeistert?

Ich denke, wie alle Verwaltungen standen wir vor der Herausforderung, arbeitsfähig zu bleiben. Corona hat uns in eine Art der digitalen Zusammenarbeit gezwungen, die Wochen vorher noch undenkbar erschien. Von einem auf den anderen Tag wurden Videokonferenzen und andere Kollaborationsplattformen eingerichtet und auch Dinge möglich, über die vorher ausschweifend diskutiert wurde. Die sächsische Staatsverwaltung blieb auch deshalb in schwierigen Zeiten arbeitsfähig, weil wir einerseits gute Vorarbeiten geleistet hatten, und andererseits, weil wir einen starken landeseigenen IT-Dienstleister und eine funktionierende Informationssicherheitsorganisation haben, die mit pragmatischen Ansätzen geholfen hat. Aber es bleibt aktuell die Erkenntnis, dass wir, wenn wir die Digitalisierung in diesem hohen Tempo weiterführen wollen, die Sicherheitsexperten mit ins Team holen müssen. Sie sind die Garanten dafür, dass Verwaltung nicht nur modern und digital ist, sondern auch hohe Sicherheitsanforderungen erfüllt. ■

Kurzprofil Thomas Popp

Thomas Popp wurde am 8. November 1961 in Schweinfurt geboren. Seine Laufbahn im öffentlichen Dienst begann der Volljurist im Jahr 1992 als Dozent an der Beamtenfachhochschule in Herrsching. Zwischen 1998 und 2004 verantwortete Thomas Popp als Projektkoordinator des Freistaates die Entwicklung des Leistungsvergleiches zwischen Finanzämtern in der Steuerverwaltung, war Sachgebietsleiter in verschiedenen Bereichen des Finanzamtes Freital und übernahm 2004 die Aufgabe des Vorstehers des Finanzamtes Freiberg.

Im Jahr 2005 folgte der Wechsel in das Sächsische Staatsministerium der Finanzen. 2010 wurde Thomas Popp mit der Leitung der Oberfinanzdirektion Chemnitz betraut und im Jahr 2011 zum Präsidenten des Landesamtes für Steuern und Finanzen ernannt.

Anfang 2015 wechselte er als Leiter der Zentralabteilung in die Sächsische Staatskanzlei. In dieser Funktion übernahm er den Vorsitz der Kommission zur umfassenden Evaluation der Aufgaben, Personal- und Sachausstattung des Freistaates Sachsen. Seit 10. April 2018 ist Thomas Popp Amtschef der Sächsischen Staatskanzlei und verantwortlich für die Stabsstelle „Landesweite Organisationsplanung, Personalstrategie und Verwaltungsmodernisierung“.

Mit Wirkung zum 1. August 2018 erfolgte darüber hinaus die Ernennung zum Beauftragten für Informationstechnologie (Chief Information Officer - CIO) des Freistaates Sachsen. Am 20. Dezember 2019 wurde Thomas Popp zum Staatssekretär und Mitglied der Sächsischen Staatsregierung ernannt.

Cyber-Sicherheit im Dialog mit allen Gesellschaftsgruppen

Arbeitsergebnisse des Projekts „Institutionalisierung des gesellschaftlichen Dialogs“ und Folgeprojekt „Dialog für Cyber-Sicherheit“

von Dr. Angelika Praus und Nora Lieberknecht, Projektgruppe Digitaler Verbraucherschutz

Die mit dem digitalen Wandel verbundenen Herausforderungen im Bereich Cyber-Sicherheit können nur im Dialog mit allen gesellschaftlichen Gruppen bewältigt werden. In diesem Bewusstsein intensiviert das BSI bereits seit 2016 den gesamtgesellschaftlichen Dialog zum Thema Cyber-Sicherheit im Rahmen eines partizipativen Multi-Stakeholder-Ansatzes. Das Projekt „Institutionalisierung des gesellschaftlichen Dialogs“ wurde 2019 abgeschlossen, das Nachfolgeprojekt ist im Oktober 2020 gestartet.

Herzstück des Dialogs ist die „Denkwerkstatt sichere Informationsgesellschaft“ als Dialogplattform für Akteure aus Staat, Wissenschaft, Wirtschaft, Kultur & Medien und Zivilgesellschaft. Beim Austausch unterschiedlicher Perspektiven auf Cyber-Sicherheit werden geschlossene Diskursgruppen aufgebrochen und dadurch die nachhaltige Entwicklung gemeinsamer Lösungsoptionen und Handlungsmöglichkeiten gefördert. Dabei ist das BSI bestrebt, insbesondere den Dialog mit der organisierten Zivilgesellschaft zu stärken und Impulse für die eigene Arbeit aufzunehmen. Der Dialog folgt außerdem dem Ansatz des „Open Government“ (vgl. Blogpost zur Denkwerkstatt 2018: opengovpartnership.de/open-government-praxis-denkwerkstatt-sichere-informationsgesellschaft).

ERGEBNISSE DES PROJEKTS „INSTITUTIONALISIERUNG DES GESELLSCHAFTLICHEN DIALOGS“

Ausgehend von der Denkwerkstatt arbeitete bis Ende 2019 eine Kerngruppe mit 15 Expertinnen und Experten aus den o. g. unterschiedlichen Bereichen im Rahmen des Projekts „Institutionalisierung des gesellschaftlichen Dialogs“ in verschiedenen Workshops und Arbeitstreffen an drei selbstgewählten Themen.

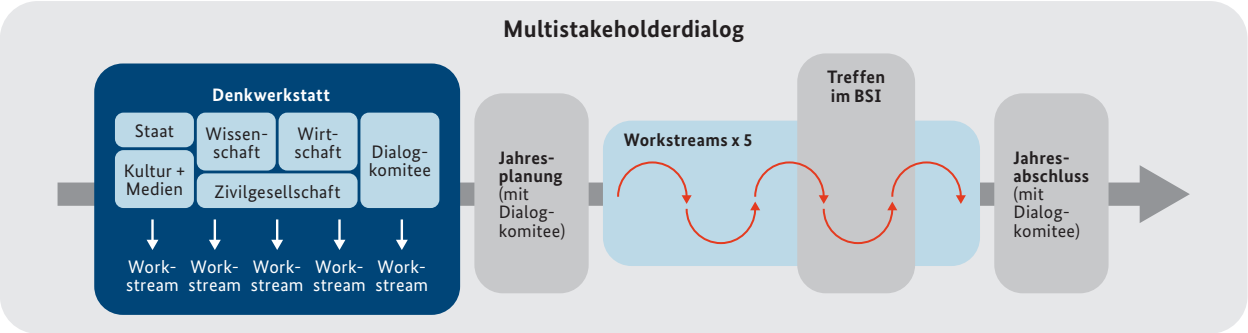


Abb 1: Vereinfachte Darstellung eines Jahreszyklus des Dialogprozesses

Ergebnis 1:
Mapping zivilgesellschaftlicher Akteure
Basierend auf Rechercheergebnissen und qualitativen Interviews beinhaltet der Bericht eine Zusammenstellung zivilgesellschaftlicher Akteure im Bereich Cyber-Sicherheit sowie ihrer wesentlichen Aktivitäten, Zielsetzungen und Vernetzungsstrukturen.

Ergebnis 2:
Vernetzungstag zum Thema
Eine Veranstaltung wurde konzipiert und am 9. September 2019 in Berlin durchgeführt, die zur Vernetzung der Akteure aus den Bereichen Wissensvermittlung und Cyber-Sicherheit beigetragen hat. So konnten die Akteure ihre Erfahrungen, insbesondere in Bezug auf effektive Aktivierung, Qualitätsmanagement sowie Zielgruppen und Formate, austauschen und entsprechende Synergien schaffen.

Ergebnis 3
Institutionalisierung des gesellschaftlichen Dialogs
Ein Modell wurde erarbeitet, wie der vom BSI initiierte Multi-Stakeholder-Dialog künftig vertieft und verstetigt werden kann (s. Abb. 1).

FORTFÜHRUNG DES „DIALOGS FÜR CYBER-SICHERHEIT“

Der Multi-Stakeholder-Dialog wird seit Oktober 2020 im Anschlussprojekt „Dialog für Cyber-Sicherheit“ fortgeführt. Das von den Stakeholdern selbst entworfene Partizipations-bzw. Multi-Stakeholder-Modell wird dabei über einen längeren Zeitraum (bis zu fünf Jahre) implementiert und verstetigt.

Das Modell ermöglicht Akteuren aller gesellschaftlichen Gruppen eine verstärkt ergebnisorientierte Arbeit an partizipativ festgelegten Themen der Cyber-Sicherheit. Dazu dienen neben der Denkwerkstatt insbesondere agile Arbeitsgruppen, sog. „Workstreams“, in denen die Stakeholder gemeinsam über drei bis neun Monate an den selbstgewählten Themen und Ergebnissen arbeiten. Unter Einbeziehung der Expertinnen und Experten des BSI soll dabei kontinuierlich ein fachlicher Austausch ermöglicht werden.

> „Die Entwicklung eines Rahmens für die Auseinandersetzung mit kritischen Perspektiven der Zivilgesellschaft durch Stakeholder der Denkwerkstatt Sichere Informationsgesellschaft war ein bedeutender Schritt und birgt Potenzial für eine stärkere Berücksichtigung gesellschaftlicher Belange in der Sicherheitsarchitektur.“
>
> *Daniel Guagnin, Teilnehmer des Dialogs und Mitentwickler des Dialogmodells*

Das BSI als Cyber-Sicherheitsbehörde des Bundes möchte so in der Gesellschaft einen größeren Rückhalt für das Thema IT-Sicherheit erreichen, neue Themen und Bedarfe der unterschiedlichen gesellschaftlichen Gruppen im Bereich Cyber-Sicherheit frühzeitig identifizieren und Impulse aus dem Dialogprozess in die eigene Arbeit einfließen lassen. Insbesondere in den jährlich stattfindenden Denkwerkstätten soll der Dialog mit zivilgesellschaftlichen, wirtschaftlichen und staatlichen Akteuren in einer vertrauensvollen und kooperativen Atmosphäre etabliert werden, um so gemeinsam die neuen Herausforderungen im Bereich Cyber-Sicherheit der nächsten Jahre anzugehen und eine sichere Informationsgesellschaft zu gestalten. ■

Weitere Informationen zum Projekt und den Ergebnissen unter:

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

Cyber-Sicherheit im Zeichen von Emotet und Corona

Erkenntnisse aus dem Bericht zur Lage der IT-Sicherheit in Deutschland 2020

In seinem Bericht „Die Lage der IT-Sicherheit in Deutschland“ berichtet das BSI einmal im Jahr über Cyber-Bedrohungen sowie Entwicklungen im Bereich IT-Sicherheit. Die aktuelle Ausgabe steht jedoch nicht nur im Zeichen von Gefahren wie Emotet oder kritischen Schwachstellen. Auch die COVID-19-Pandemie hatte einen Einfluss auf die IT-Sicherheitslage in Deutschland. Die Lage bleibt also angespannt, mit insgesamt mehr als einer Milliarde bekannter Schadprogramm-Varianten.

Wie das BSI beobachten konnte, nutzten Angreifer im Berichtszeitraum Juni 2019 bis Mai 2020 Schadprogramme für cyber-kriminelle Massenangriffe auf Privatpersonen, Unternehmen, Behörden und andere Institutionen, aber auch für gezielte Angriffe auf ausgewählte Opfer. Zugleich hat die Bedrohung durch Daten-Leaks mit der Offenlegung von Millionen von Patientendatensätzen im Internet eine neue Qualität erreicht. Zudem traten mehrere, teils kritische Schwachstellen in Software-Produkten auf, die Angreifer für Schadprogrammangriffe oder Datendiebstahl ausnutzen konnten. Dabei verwendeten die Angreifer auch verstärkt den Faktor „Mensch“ als Einfallstor für Angriffe, die mit Social-Engineering-Methoden arbeiten und gleichzeitig als Türöffner für weitere Angriffe dienen.

NEUE SCHADPROGRAMMWELLE IM HERBST UND WINTER: EMOTET DOMINIERT DIE LAGE

Dominiert wurde die Lage durch das Schadprogramm Emotet, das sich schon im vergangenen Berichtszeitraum als besonders gefährlich erwiesen hatte. Es ermöglicht eine Kaskade weiterer Schadsoftware-Angriffe bis hin zu gezielten Ransomware-Angriffen auf ausgewählte, zahlungskräftige Opfer. Insgesamt war das Aufkommen neuer Schadprogrammvarianten im Herbst und Winter überdurchschnittlich hoch (der Tageszuwachs lag zeitweise bei knapp 470.000 Varianten).

MILLIONEN PATIENTENDATEN IM INTERNET ÖFFENTLICH ZUGÄNGLICH

Meldungen zu Diebstählen von Kundendaten wurden im Berichtszeitraum erneut regelmäßig beobachtet. Aber nicht nur Diebstahl führte zum Datenabfluss. Im Berichtszeitraum wurden auch Datenbanken mit hochsensiblen medizinischen Daten frei zugänglich im Internet entdeckt. Anders als bei Datendiebstählen war hier also kein technisch aufwändiger Angriff notwendig, sondern unzureichend gesicherte oder falsch konfigurierte Datenbanken waren Ursache für den Datenabfluss.

KRITISCHE SCHWACHSTELLEN IN REMOTE-ZUGÄNGEN

Im Berichtszeitraum sind mehrere kritische Schwachstellen aufgetreten. Die neuen Schwachstellen BlueKeep und DejaBlue im Remote Desktop Protocol von Windows machten viele Windows-Systeme bis hin zu Windows 10 angreifbar. Durch die Schwachstellen können Angreifer einen beliebigen Code – auch Schadprogramm – auf den angreifbaren Systemen ausführen. Die Schwachstellen ermöglichen Schadprogrammen außerdem, sich automatisiert weiterzuverbreiten, und werden daher auch als „wurmfähig" bezeichnet. Microsoft hat Sicherheits-Updates für alle betroffenen Systeme bereitgestellt.

SOCIAL-ENGINEERING-ANGRIFFE UNTER AUSNUTZUNG DER COVID-19-PANDEMIE

Cyber-Kriminelle, die sich auf Betrug im Internet spezialisiert haben, reagieren in der Regel schnell auf gesellschaftlich relevante Themen und Trends, um diese für Angriffe auszunutzen. Im Zuge der COVID-19-Pandemie wurden beispielsweise, Phishing-Kampagnen, CEO-Fraud und Betrugsversuche mit IT-Mitteln beobachtet. So gelang es Betrügern beispielsweise Soforthilfe-Maßnahmen zu missbrauchen, indem sie die Antragswebseiten amtlicher Stellen täuschend echt nachahmten. Die unternehmensbezogenen Daten, die Antragstellerinnen und Antragsteller auf den gefälschten Seiten eingegeben hatten, nutzten die Cyber-Kriminellen anschließend, um sich als Antragstellerin bzw. Antragsteller auszugeben und Hilfsgelder missbräuchlich zu beantragen. ■

IT-SICHERHEIT IM KRITIS-GESUNDHEITSSEKTOR: STATUS QUO UND HANDLUNGSEMPFEHLUNGEN

Labore und Krankenhäuser in Deutschland sind gut vor Cyber-Angriffen und Ausfällen ihrer kritischen Dienstleistungen geschützt. Das ist das Ergebnis zweier durch das BSI in Auftrag gegebenen Studien. Die Studien für den KRITIS-Sektor Gesundheit wurden mit dem Ziel erarbeitet, die relevanten Prozesse der kritischen Dienstleistungen zu identifizieren und den Status Quo der Informationssicherheit in Krankenhäusern bzw. Laboren in Deutschland zu untersuchen. Darüber hinaus enthalten die Studien Handlungsempfehlungen zur Erhöhung des Schutzniveaus und einen Ausblick auf die Zukunft der Digitalisierung innerhalb der beiden Branchen. Sie sind verfügbar unter:

Weitere Informationen:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KRITIS/Studie_Informationssicherheit_stationaere_med_Versorgung.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KRITIS/Studie_Informationssicherheit_in_Laboren.html

Cyber-Sicherheitslage für Deutschland 2020

Auf einen Blick: Zahlen aus dem Lagebericht zu IT-Sicherheit in Deutschland 2020

117,4 MIO.
neue Schadprogramm-Varianten

2019: 114 MIO.

durchschnittlich **322.000** neue **Schadprogramm-Varianten** pro Tag in Spitzenwerten **470.000**

76 %
ist der Anteil unerwünschter **SPAM-MAILS** an allen in den Netzen des Bundes eingegangenen Mails

▶ 2019: 69 % ◀

24,3 MIO.
Patientendatensätze
waren Schätzungen zufolge international frei im Internet zugänglich

419
KRITIS-Meldungen

▶ 2019: 252

▶ 2018: 145

52.000
WEBSEITEN
wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt

35.000
Mails mit Schadprogrammen
wurden durchschnittlich pro Monat in deutschen Regierungsnetzen abgefangen

109.000
Abonnenten Bürger-CERT
- 2019: 105.000
- 2018: 100.000

rund **100**
Produkte und Standorte
hat das BSI im Bereich Common Criteria zertifiziert

mehr als **4.400**
Mitglieder der Allianz für Cyber-Sicherheit
- 2019: 3.700
- 2018: 2.700

rund **1.700**
registrierte **KRITIS-Anlagen**

knapp **7 MIO.**
Meldungen zu Schadprogramm-INFEKTIONEN
übermittelte das BSI an deutsche Netzbetreiber

Ein Blick zurück – ein Schritt nach vorn

30 Jahre BSI: Jubiläum und 17. IT-Sicherheitskongress

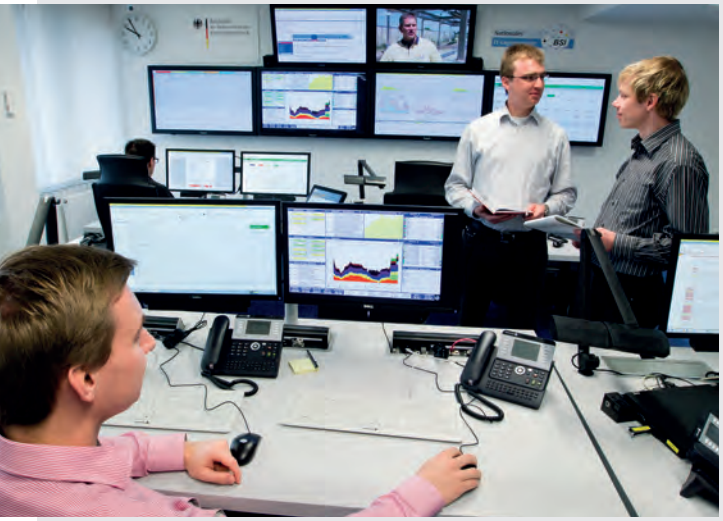
Mit dreißig Jahren ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) noch eine junge Behörde. Und auch sein Aufgabengebiet – die Gestaltung der Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft – kann dieses Attribut mit Fug und Recht für sich in Anspruch nehmen. Aber Grund genug, einmal zurückzublicken, sind dreißig Jahre schon.

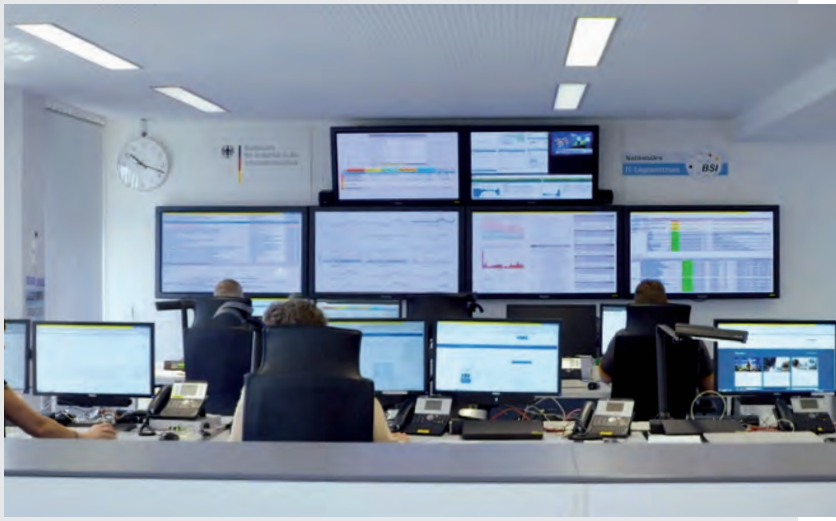
GRÜNDUNG ALS BERATUNGSBEHÖRDE

Als das BSI am 1. Januar 1991 seine Arbeit aufnimmt (auf Basis des BSI-Errichtungsgesetzes vom 17. Dezember 1990), erhält die IT-Sicherheit nicht nur eine gesetzliche Grundlage, sondern auch eine neue Ausrichtung. Dem Gesetz zugrunde liegen eine neue Definition von Sicherheit sowie ein neues Verständnis von Prävention und Informationspolitik – erstmals formuliert im Zukunftskonzept IT der Bundesregierung vom Juli 1989: Alle Betroffenen und Interessierten sollten über Risiken der Informationstechnik und mögliche Schutzmaßnahmen unterrichtet werden.

Der Kerngedanke, dass ein Bundesamt für die IT-Sicherheit aller gesellschaftlichen Gruppen beratend und unterstützend tätig sein sollte, war damals noch nicht selbstverständlich. Doch spätestens mit Beginn der breiten kostenlosen Nutzung des Internets ab 1993 wurde deutlich, wie zukunftsweisend dieser Ansatz war. IT-Sicherheit wird nun zu einer vorrangigen staatlichen Aufgabe. Um sie zu schaffen und zu fördern, um ihre Bedrohung zu bekämpfen und zu mindern, muss der Staat immer stärkere Rahmenbedingungen schaffen, Standards setzen und aktiv Hilfestellung geben.

Nicht zuletzt daraus erwuchsen in den kommenden Jahren immer neue Aufgaben, trat neben die Beratung und Unterstützung zunehmend auch die eigene operative Umsetzung. Gegründet als der zentrale IT-Sicherheitsdienstleister des Bundes, sind der Schutz der Regierungsnetze und die Sicherung zentraler Netzübergänge seit jeher die vornehmsten Aufgaben des BSI.





Das Nationale IT-Lagezentrum im BSI.

BSI für Bürger-Broschüren
*Das BSI bietet auf seiner Bürger-Webseite insgesamt fünf Broschüren zu zentralen Themen für Privatanwender*innen an, darunter u.a. zum sicheren Umgang mit mobilen Geräten, zu wichtigen Tipps in der Nutzung von Cloud-Diensten sowie zu Informationen über das Internet der Dinge.*

Seit 1994 betreibt das BSI zudem ein Computer Emergency Response Team (CERT), das Informationen über Sicherheitslücken und neue Angriffsmuster sammelt, auswertet und Informationen und Warnungen an die betroffenen Stellen weitergibt: Eine operative Umsetzung der Erkenntnis, dass nicht nur die Abwehr von Schadprogrammen und der Hinweis auf Schwachstellen, sondern auch die Reaktion auf IT-Sicherheitsvorfälle wichtig sind.

SOLIDER GESETZLICHER RAHMEN

Mit dem 2009 durch das Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes novellierten BSI-Gesetz konnte das BSI für die Bundesbehörden verbindliche Sicherheitsstandards für die Beschaffung und den Einsatz von IT entwickeln. Es wurde zur zentralen Meldestelle für IT-Sicherheit innerhalb der Bundesverwaltung, um insbesondere bei IT-Krisen nationaler Bedeutung durch aufbereitete Informationen und kompetente Analysen die Entscheidungs- und Handlungsfähigkeit der Bundesregierung sicherzustellen. Und es etablierte ein IT-Krisenmanagement für die Bundesverwaltung als eine Art Frühwarnsystem, das die Erstellung von Lagebildern ermöglicht, Krisenreaktionsprozesse definiert und mit Übungen unterlegt.

Noch einmal – und entscheidend – erweitert wurden die Aufgaben und Befugnisse des BSI durch das im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz. Mit verbindlichen Mindestanforderungen an die IT-Sicherheit, flankiert durch eine Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle, will das Gesetz vor allem den Schutz der Kritischen Infrastrukturen (KRITIS) verbessern und die Netzsicherheit in den Bereichen erhöhen, deren Ausfall oder deren Beeinträchtigung der Versorgungsdienstleistungen dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland hätte. KRITIS-Betreiber müssen darum die Einhaltung von IT-Sicherheit nach dem Stand der Technik regelmäßig gegenüber dem BSI nachweisen (§ 8a BSIG). Sofern Sicherheitsmängel aufgedeckt werden, darf das BSI im Einvernehmen mit den Aufsichtsbehörden deren Beseitigung anordnen.

Das BSI ist auch die zentrale Meldestelle für die IT-Sicherheit Kritischer Infrastrukturen (nach § 8b BSIG). Diese müssen dem BSI erhebliche Störungen ihrer IT melden, sofern sie Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben können. Das BSI bewertet und analysiert diese Meldungen und setzt sie mit weiteren Meldungen und Erkenntnissen aus anderen Quellen in Beziehung.

Daraus entsteht ein Lagebild, auf dessen Basis beispielsweise kurzfristige Warn- und Alarmierungsmeldungen sowie Handlungsempfehlungen für Betroffene erstellt werden können. Umgekehrt sammelt und bewertet das BSI sämtliche für die Abwehr von Angriffen auf

29. Cyber-Sicherheits-Tag der Allianz für Cyber-Sicherheit
Mit einem neuen Veranstaltungskonzept lockten die Allianz für Cyber-Sicherheit (ACS) und der Deutsche Industrie- und Handelskammertag (DIHK) am 26. September 2019 zahlreiche Interessierte zum 29. Cyber-Sicherheits-Tag nach Berlin. Denn im Bereich der Cyber-Sicherheit lässt sich zwar vieles individuell lösen. Einfacher und besser funktioniert es aber, wenn man von Erfahrungen und Erkenntnissen anderer lernen kann.

die IT-Sicherheit Kritischer Infrastrukturen relevanten Informationen und leitet diese an die Betreiber sowie die zuständigen (Aufsichts-)Behörden weiter. Die Betreiber erhalten somit Informationen und Know-how und können von der Auswertung der Meldungen aller Betreiber sowie vieler anderer Quellen durch das BSI profitieren.

In zwei Rechtsverordnungen zur Umsetzung des IT-Sicherheitsgesetzes wurde en détail geregelt, welche Unternehmen aus den KRITIS-Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Finanz- und Versicherungswesen sowie Wasser und Ernährung unter das IT-Sicherheitsgesetz fallen.

So solide dieser Rechtsrahmen damit auch ist, die Entwicklung der Digitalisierung erlaubt kein Innehalten. Aus der Umsetzung des IT-Sicherheitsgesetzes und vor dem Hintergrund der aktuellen Bedrohungslage ist der gegenwärtige Referentenentwurf eines IT-Sicherheitsgesetzes 2.0 entstanden. Er sieht neue Pflichten für die Betreiber Kritischer Infrastrukturen, aber auch neue Aufgaben des BSI, wie den digitalen Verbraucherschutz und ein Kennzeichen für die Sicherheit von IT-Produkten, vor. Beides soll die Sensibilisierung für Cyber-Sicherheit stärken und das Sicherheitsniveau deutlich erhöhen.

KOOPERATIVE GESTALTUNG DER CYBER-SICHERHEIT

Eine sichere Gestaltung der Digitalisierung und Erhöhung des Informationssicherheitsniveaus ist eine gesamtgesellschaftliche Aufgabe, die eine intensive Kooperation unterschiedlicher Akteure erfordert. Als die nationale Cyber-Sicherheitsbehörde des Bundes, gestaltet das BSI zum Schutz von Staat, Politik, Gesellschaft und Wirtschaft die Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion mit einem ausgeprägten kooperativen Ansatz. Es setzt auf ein enges und gleichberechtigtes Zusammenarbeiten aller Akteure und stellt seinen umfassenden, unabhängigen und neutralen Sachverstand zur Verfügung.

Auf diese Weise verfügt Deutschland über eine funktionierende Cyber-Abwehr aus einer Hand. Dies zeigt sich vor allem dort, wo das BSI im Rahmen seiner sich erweiternden Zuständigkeiten über seine ursprüngliche Aufgabe hinaus neue Zielgruppen erschließen und neue Informations- und Unterstützungsangebote machen konnte:

16. IT-Sicherheitskongress
Das BSI brachte 2019 rund 700 IT-Sicherheitsexperten zusammen.

Im KRITIS-Bereich kooperiert das BSI über seine Aufgaben aus dem IT-Sicherheitsgesetz hinaus im Rahmen der öffentlich-privaten Partnerschaft UP KRITIS mit den KRITIS-Betreibern, deren Verbänden und den zuständigen staatlichen Stellen. Der Umsetzungsplan (UP) adressiert acht der neun Sektoren Kritischer Infrastrukturen. Den Sektor Staat und Verwaltung adressiert auf Bundesebene der UP BUND. Die notwendigen Regelungen für Länder und Kommunen treffen die Länder.

Mit der Allianz für Cyber-Sicherheit, die 2012 mit dem ITK-Branchenverband Bitkom initiiert wurde, soll die Widerstandsfähigkeit insbesondere der kleinen und mittelständischen Unternehmen gegenüber Cyber-Angriffen gestärkt werden. Dies erfolgt unter anderem durch die Bereitstellung praktikabler IT-Sicherheitsempfehlungen für KMU durch das BSI und durch Partner der Allianz. Der Allianz gehören inzwischen über 4.400 Institutionen an, davon mehr als 140 Partner-Unternehmen und knapp 100 Multiplikatoren.

Mit der Website www.bsi-fuer-buerger.de und dem kostenlosen Warn- und Informationsdienst „Bürger-CERT“ stellt das BSI seine Erkenntnisse zur Cyber-Sicherheitslage auch Privatanwendern zum Schutz ihrer IT-Systeme und Daten zur Verfügung. Mit der Facebook-Seite www.facebook.com/bsi.fuer.buerger und dem Twitter-Kanal www.twitter.com/BSI_Presse ist das BSI auch in den sozialen Netzwerken vertreten.

Das BSI verfügt schon heute auf der Basis seiner technisch tiefgehenden Expertise über eine integrierte Wertschöpfungskette, von der Beratung über die Entwicklung sicherheitstechnischer Lösungen, der Abwehr von Angriffen auf die Cyber-Sicherheit bis hin zur Standardisierung und Zertifizierung.

Aber es gilt auch: Analog zu einer immer größeren Bedeutung von Cyber-Sicherheit in einer hochgradig vernetzten Gesellschaft sind die zukünftigen Herausforderungen des BSI bestimmt nicht geringer als die bei seiner Gründung. ■

17. DEUTSCHER IT-SICHERHEITSKONGRESS
Am 2. und 3. Februar 2021 veranstaltet das BSI zum 17. Mal den alle zwei Jahre stattfindenden Deutschen IT-Sicherheitskongress. Erstmalig findet der IT-Sicherheitskongress in hybrider Form statt: Die Moderation und Speaker-Vorträge erfolgen live vor Ort, die Kongress-Teilnehmerinnen und Teilnehmer nehmen virtuell teil. Zwei Tage lang werden sich Teilnehmerinnen und Teilnehmer aus Verwaltung, Wirtschaft und Wissenschaft über aktuelle Trends und Perspektiven in der IT-Sicherheit austauschen. Der Kongress ist eine feste Größe im Veranstaltungskalender der IT-Sicherheitsbranche und darüber hinaus. Sein Ziel ist es, das Thema IT-Sicherheit aus unterschiedlichen Blickwinkeln zu beleuchten, Lösungsansätze vorzustellen und weiterzuentwickeln. Es wird wieder eine Vielzahl von kreativen, praxisnahen und verständlichen Beiträgen geben, aus denen ein Veranstaltungsprogramm komponiert wird, das das Spektrum der Cyber-Sicherheit in Gänze abdeckt. Der Parlamentarische Staatssekretär Prof. Dr. Krings (Bundesinnenministerium) konnte bereits als Speaker für den Kongress gewonnen werden. Aus Anlass des 30-jährigen Bestehens des BSI bindet der Kongress im kommenden Jahr das Jubiläum in den ersten Kongresstag mit ein.

BSI und VDA: Gemeinsam für mehr Cyber-Sicherheit im Auto
Das BSI und der Verband der Automobilindustrie (VDA) arbeiten zukünftig in Fragen der Cyber-Sicherheit eng zusammen. Eine entsprechende gemeinsame Absichtserklärung unterzeichneten VDA-Präsidentin Hildegard Müller und BSI-Präsident Arne Schönbohm in Berlin.

Sicherheitsanforderungen für Telekommunikationsnetze veröffentlicht
Die Bundesnetzagentur hat heute den aktuellen Entwurf des Kataloges von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten veröffentlicht. Der Katalog wurde im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt.

Das Jahr 2020 für das BSI

Rückblick

Bedrohungsabwehr rückt weiter in den Vordergrund: Ressortübergreifende Kooperation zwischen Kommando CIR und BSI
Mitarbeiter des BSI verstärken das Blue-Team bei der Cyber-Abwehr-Übung Locked Shields.

Mehr Cyber-Sicherheit in der Luftfahrt:
BSI und EASA vereinbaren strategische Zusammenarbeit
Moderne Flugzeuge sind digital vernetzte, fliegende Hochleistungsrechner. Für einen reibungslosen Flug muss daher neben der klassischen Flugsicherheit auch die Cyber-Sicherheit betrachtet werden. Gemeinsames Ziel des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Agentur der Europäischen Union für Flugsicherheit ist es, die Cyber-Sicherheit in der internationalen Luftfahrt nachhaltig zu steigern.

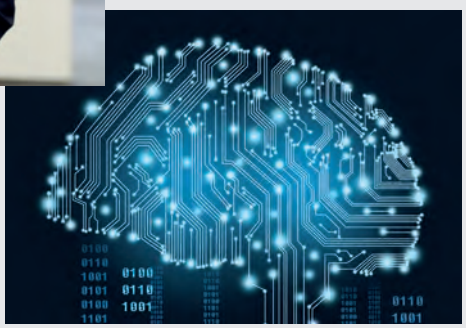
#CyberConference2020
BSI und BMI richten die Cyber-Sicherheitskonferenz anlässlich der deutschen EU-Ratspräsidentschaft aus.

BSI und Verbraucherzentrale stärken digitalen Verbraucherschutz
Gemeinsam für eine sichere digitale Welt – auf dieses Ziel haben sich der Verbraucherzentrale Bundesverband e.V. (vzbv) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) verständigt. Der vzbv-Vorstandsvorsitzende Klaus Müller und BSI-Präsident Arne Schönbohm unterzeichneten dazu am 4. Juni eine entsprechende gemeinsame Grundsatzvereinbarung (Memorandum of Understanding).

Informationsangebote und -services für Bürgerinnen und Bürger
Die Cyberfibel ist ein Kooperationsprojekt des Bundesamts für Sicherheit in der Informationstechnik (BSI) und Deutschland sicher im Netz e. V..

Das BSI als (Mit-)Gestalter in der digitalen Gesundheitsvorsorge.
Ein Thema beim Besuch von Gesundheitsminister Jens Spahn: Wieviel sollten Krankenhäuser in ihre Informationssicherheit investieren? Die Antwort findet sich nun im Krankenhaus-Zukunftsgesetz, das vorsieht, mindestens 15 Prozent der beantragten Fördermittel für Maßnahmen zur Verbesserung der Informationssicherheit einzusetzen.

BSI veröffentlicht Studie zur Sicherheit von Blockchain-Anwendungen
Das BSI hat im Rahmen einer Marktanalyse rund 300 Blockchain-Anwendungen bewerten lassen. Auftragnehmer der Studie war das Forschungszentrum Informatik (FZI) in Karlsruhe.



BSI-Team räumt bei CHES-Challenge alle Preise ab
*Das BSI hat mit einem Team aus acht Mitarbeiterinnen und Mitarbeiter*innen auch 2020 wieder am Seitenkanalwettbewerb teilgenommen und dabei alle Preise gewonnen, die schlussendlich vergeben wurden.*

IT-SICHERHEIT IN DER PRAXIS

Wie sicher ist der Dienstwagen?

Neuer IT-Grundschutz-Baustein „Allgemeines Fahrzeug“ beleuchtet Informationssicherheit bei Fahrzeugen

von Daniel Gilles, Referat BSI-Standards und IT-Grundschutz

Digitale Assistenz- oder Infotainmentsysteme sind zu einem festen Bestandteil moderner Fahrzeuge geworden, wie z.B. herkömmlicher Pkw, Lkw, Schiffe oder Flugzeuge. Daraus ergeben sich neue Risiken für die Informationssicherheit der Fahrzeuge, die das BSI im neuen IT-Grundschutz-Baustein „Allgemeines Fahrzeug“ aufgreift.

Das BSI bietet mit dem IT-Grundschutz seit über 25 Jahren eine bewährte Methodik an, um sich effizient mit dem Thema Informationssicherheit zu befassen. Im Zentrum der praktischen Arbeit steht hierbei das IT-Grundschutz-Kompendium, das als „lebendes Werkzeug“ kontinuierlich weiterentwickelt wird. Rund 100 Fachtexte thematisieren in zehn sogenannten IT-Grundschutz-Bausteinen unterschiedliche Aspekte und Facetten der Informationssicherheit. Sie beschreiben Gefährdungen und Anforderungen, benennen die Verantwortlichen in Unternehmen sowie Behörden und ermöglichen somit fundierte Sicherheitsbetrachtungen. Außerdem geben sie Antworten auf Fragen wie: Welche Anforderungen an die Informationssicherheit sind wichtig? Welche Regelungen müssen definiert werden?

Der IT-Grundschutz wird kontinuierlich weiterentwickelt, Trends werden bewertet und Themen ergänzt. Ein Ergebnis dieser Aktualisierung ist der neue IT-Grundschutz-Baustein „Allgemeines Fahrzeug“, der die Informationssicherheit von Fahrzeugen betrachtet und damit der rasanten Weiterentwicklung im Bereich der Fahrzeug-IT Rechnung trägt.

DAS MOBILE BÜRO IM FAHRZEUG ABSICHERN

Für alle Fahrzeuge – ob an Land, im Wasser oder in der Luft – gilt, dass neben Aspekten zur herkömmlichen Fahrzeugsicherheit („Safety“), die Informationssicherheit („Security“) frühzeitig beim Einsatz neuer Geräte mitbedacht werden muss. Ein Spediteur hat heutzutage in den eingesetzten Lkw Informationen über die Kunden wie Kontaktdaten oder Lieferumfang. Ein Vertriebsmitarbeiter verfügt in seinem Pkw über ein mobiles Büro mit Laptop und Smartphone, das sich mit der IT des Fahrzeuges verbindet. Fahrzeuge, die beruflich genutzt werden und mit einer beachtlichen IT-Ausstattung aus dem Werk kommen, sind besonderen Risiken ausgesetzt. Abbildung 1 gibt einen Überblick über mögliche Gefährdungen.

Abbildung 1: Risiken für die Informationssicherheit in PKWs

EIN THEMA – VIELE SYNERGIEN

Spezialisten aus dem Kommando Cyber- und Informationsraum der Bundeswehr, aus der Bundes- und Landespolizei sowie dem Feuerwehrwesen haben sich mit denselben Fragestellungen zu sicherer Fahrzeug-IT auseinandergesetzt. Das BSI hat gemeinsam mit diesen Expertinnen und Experten eine interdisziplinäre Arbeitsgruppe gegründet, um den neuen Baustein „Allgemeines Fahrzeug“ zu erarbeiten. Dieser Baustein ist für alle Fahrzeugarten mit Motor und Fahrzeugkabine, die sich in der Regel auf Land-, Luft-, Wasser- und Seestraßen fortbewegen, anwendbar. Der Baustein zeigt auf, wie ein Fahrzeug als sichere mobile Arbeitsumgebung eingesetzt und die im Fahrzeug integrierte IT abgesichert werden kann. Hierzu werden insbesondere organisatorische Anforderungen an den Fahrzeugeinsatz sowie Fahrzeugauswahl und -beschaffung gestellt, da eine technische Absicherung der im Fahrzeug integrierten IT-Komponenten meist nur eingeschränkt möglich ist. Ein passendes Beispiel hierfür sind die Schließsysteme der Fahrzeuge. Bereits bei der Auswahl der Fahrzeuge sollte darauf geachtet werden, dass die Fahrzeuge über angemessen sichere Schließsysteme verfügen. Werden Fahrzeuge im Bestand eingesetzt, die über unsichere Schließsysteme verfügen, kann in vielen Fällen die Sicherheit durch organisatorische Maßnahmen gewährleistet werden. Ein Beispiel hierfür sind Fahrzeuge mit schlüssellosen Schließsystemen, die durch Relay-Angriffe umgangen werden können. Hier genügt in den meisten Fällen, die Keyless-Funktion des Schließsystems zu deaktivieren, um Relay-Angriffe zu verhindern.

VOM DRAFT INS IT-GRUNDSCHUTZ-KOMPENDIUM 2021

Der neue IT-Grundschutz-Baustein bildet die erste Ausgangsbasis für das breite Themenfeld der Informationssicherheit von Fahrzeugen. Aufgrund der zunehmenden Verbreitung von IT in Fahrzeugen aller Art ist es vorstellbar, den ersten IT-Grundschutz-Baustein perspektivisch um Bausteine zu weiteren Themen zu ergänzen. In der Vergangenheit hat es sich bewährt, dass Anwenderinnen und Anwender sowie Expertinnen und Experten für spezifische Anwendungsszenarien, wie z.B. spezielle Fahrzeuge, zunächst einen benutzerdefinierten Baustein erstellen. Dieser wird für die fachliche Diskussion und Weiterentwicklung auf der BSI-Webseite veröffentlicht. Durch dieses Vorgehen wird das IT-Grundschutz-Kompendium stetig um weitere aktuelle Themen erweitert.

Feedback zu dem neuen IT-Grundschutz-Baustein und weitere Anregungen zu dem Thema Informationssicherheit von Fahrzeugen nimmt das BSI unter grundschutz@bsi.bund.de gerne entgegen. ■

Weitere Informationen:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Intelligente autonome Fahrzeuge, aber sicher

Arbeitsgruppe von BSI und VdTÜV zu Anforderungen an Künstlich Intelligente (KI-) Systeme im Mobilitätsbereich

von Dr. Arndt von Twickel, Matthias Neu, Dr. Christian Berghoff und Prof. Markus Ullmann, Referat Bewertungsverfahren für eID-Technologien in der Digitalisierung

Das BSI und der Verband der deutschen TÜV-Häuser entwickeln gemeinsam Anforderungen an Künstliche Intelligenz (KI)-Systeme im Mobilitätsbereich. Am Beispiel der Verkehrsschilderkennung wird der gesamte Lebenszyklus eines KI-Systems mit Schwerpunkt auf die IT-Sicherheit analysiert. Ziel ist die Vorbereitung von anwendungsspezifischen Prüfkriterien für KI-Systeme, die auf tiefen neuronalen Netzen basieren.

EINSATZ VON KI IN FAHRZEUGEN: GROSSE CHANCEN, GROSSE HERAUSFORDERUNGEN

Der massive Einsatz von Sensorik, Rechenleistung und KI-Algorithmen verspricht, dass Autos „intelligenter" werden und langfristig sogar komplett autonom agieren können. Um den erhofften Gewinn an Verkehrssicherheit und Komfort zu realisieren, müssen jedoch große Herausforderungen gelöst werden. Autonome Fahrzeuge müssen in Echtzeit mit hochkomplexen, teils unbekannten Fahrsituationen umgehen können. Fehler, z.B. durch die Fehlinterpretation eines Stoppschildes als Tempo-100-Schild, können dabei im schlimmsten Fall Menschenleben kosten.

DER GESAMTE LEBENSZYKLUS EINES KI-SYSTEMS MUSS BETRACHTET WERDEN

Der Lebenszyklus von KI-Systemen unterscheidet sich in wesentlichen Punkten von dem klassischer IT-Systeme: Während die Struktur und die Parameter von klassischen IT-Systemen von deren Entwicklern vorgegeben werden, müssen die Parameter von neuronalen Netzen für eine korrekte Funktion mittels maschinellen Lernens anhand von großen Datensätzen, z.B. tausenden Bildern von Verkehrsschildern für die Verkehrsschilderkennung, trainiert werden. Hochqualitative, ausgewogene und umfangreiche Datensätze sind wesentlich, um ein gutes Trainingsergebnis zu erzielen. Datensätze müssen durch geeignete Maßnahmen vor absichtlich manipulierten oder versehentlich falschen Daten geschützt werden, da diese zu sehr schwer detektierbaren Fehlfunktionen führen können.

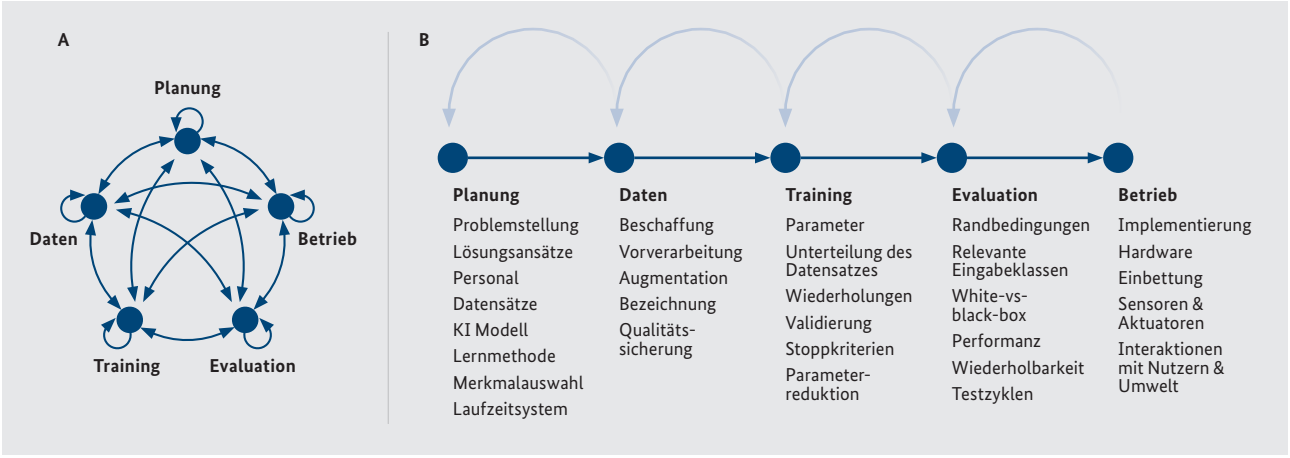
DIE PRÜFUNG VON KI-SYSTEMEN ERFORDERT NEUE METHODEN UND WERKZEUGE

In vielen Anwendungsgebieten, wie z.B. der Bildverarbeitung, sind neuronale Netze hochperformant und anderen Lösungen überlegen. Andererseits ist ihre systematische Prüfung aufgrund ihrer schlechten Interpretierbarkeit und ihres riesigen Eingaberaums stark erschwert. Dies gilt insbesondere für gezielte Angriffe, die auf qualitativ neue Verwundbarkeiten von neuronalen Netzen abzielen, z.B. manipulierte Trainingsdaten oder adversariale Angriffe. Bei letzteren suchen Angreifer gezielt nach Änderungen der Sensoreingänge, die gewünschte Falschentscheidungen auslösen. Beispielsweise können Angreifer unauffällige Aufkleber auf Verkehrsschildern anbringen, die zu deren gezielter Fehlklassifikation führen. Solche Manipulationen sind sehr schwer detektierbar und nach aktuellem Forschungsstand gibt es keine neuronalen Netze, die gegen alle bekannten Angriffe immun sind.

Neben den klassischen Methoden der IT-Sicherheit werden somit ergänzende, neue Konzepte, Methoden und Werkzeuge zur Absicherung und Prüfung der Robustheit und IT-Sicherheit von KI-Systemen entlang des gesamten Lebenszyklus benötigt, z.B. zur Qualitätskontrolle der Trainingsdaten oder zur Prüfung von Verwundbarkeiten. Deren Entwicklung ist Gegenstand der aktuellen Forschung, an der sich das BSI in Form von Projekten und studentischen Arbeiten aktiv beteiligt.

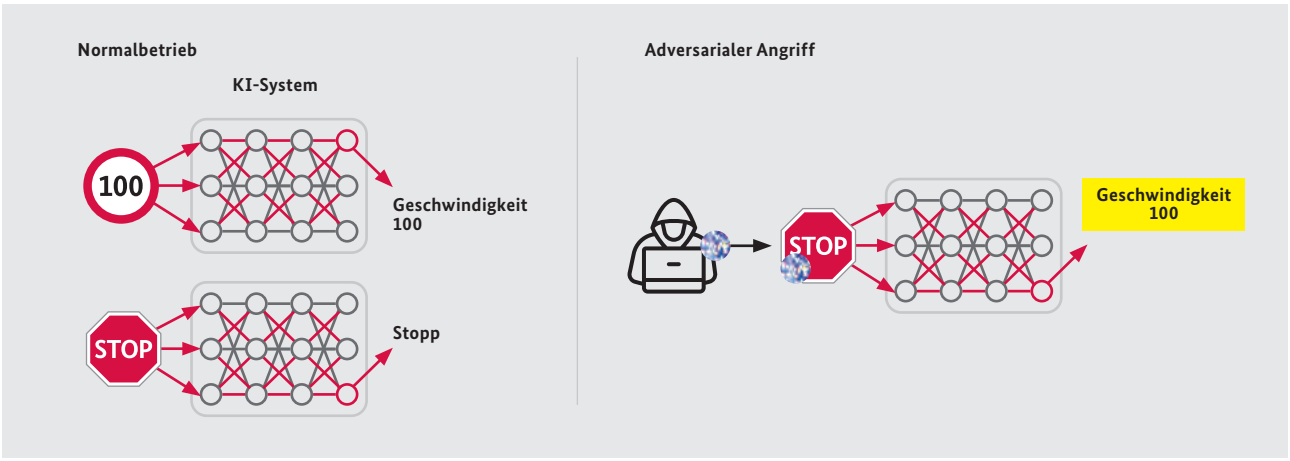
FORMULIERUNG VON ANFORDERUNGEN AN KI-SYSTEME ERFORDERT BETRACHTUNG KONKRETER ANWENDUNGEN

Entlang des Lebenszyklus von KI-Systemen hat die KI-Arbeitsgruppe von BSI und VdTÜV zunächst generalisierte Anforderungen, u. a. hinsichtlich der Datenqualität und geeigneter Netzwerkmodelle, erarbeitet und hierbei unterschiedliche Sichtweisen, wie z.B. Robustheit, IT-Sicherheit und Interpretierbarkeit, berücksichtigt. Anschließend wurden die Anforderungen für ein möglichst einfaches und gleichzeitig praxisrelevantes KI-System, die Verkehrsschilderkennung, angepasst. Hierbei wurde festgestellt, dass sich die generalisierten Anforderungen entweder direkt oder mit nur geringen Anpassungen übernehmen lassen. In den nächsten Schritten werden erstens die Anforderungen an Verkehrsschilderkennungssysteme in praxisnahen Projekten überprüft; zweitens das generalisierte Modell an weitere, qualitativ unterschiedliche KI-Systeme angepasst, um zu testen, ob dies ähnlich problemlos funktioniert; drittens Interaktionseffekte im Zusammenspiel mehrerer (KI-)Systeme in Fahrzeugen untersucht und viertens Prüfkriterien erarbeitet, die den Nachweis erbringen sollen, dass die definierten Anforderungen auch eingehalten werden. Die Erkenntnisse der KI-Arbeitsgruppe von BSI und VdTüv werden mit Expertinnen und Experten aus Wissenschaft und Wirtschaft diskutiert und in nationale und internationale Standardisierungsgremien wie DIN und ETSI eingebracht. Langfristiges Ziel muss sein, die Prüfung von autonomen Fahrzeugen, inkl. aller Subsysteme, als Grundlage für deren sicheren Einsatz im Straßenverkehr zu ermöglichen. ■



Lebenszyklus eines KI-Systems

Der Lebenszyklus eines KI-Systems kann in die Phasen Planung, Daten, Training, Evaluation und Betrieb unterteilt werden. (A) In der Realität ist die Entwicklung eines KI-Systems nicht linear, d. h. sie springt zwischen den Phasen hin und her. Oft ist sie auch von der Intuition und der Erfahrung des Entwicklers abhängig. Der Entwickler versucht, den schnellsten Weg zu einem einsetzbaren KI-System mit den gewünschten Eigenschaften zu finden. (B) Für die Analyse des Lebenszyklus und für die Entwicklung von Anforderungen ist eine sequenzielle Darstellung hilfreich. Für jede Phase werden hier wichtige funktionale Komponenten genannt. Weitere wichtige Komponenten, u. a. aus den Perspektiven Robustheit, Datenschutz und Benutzerakzeptanz, werden hier nicht genannt.

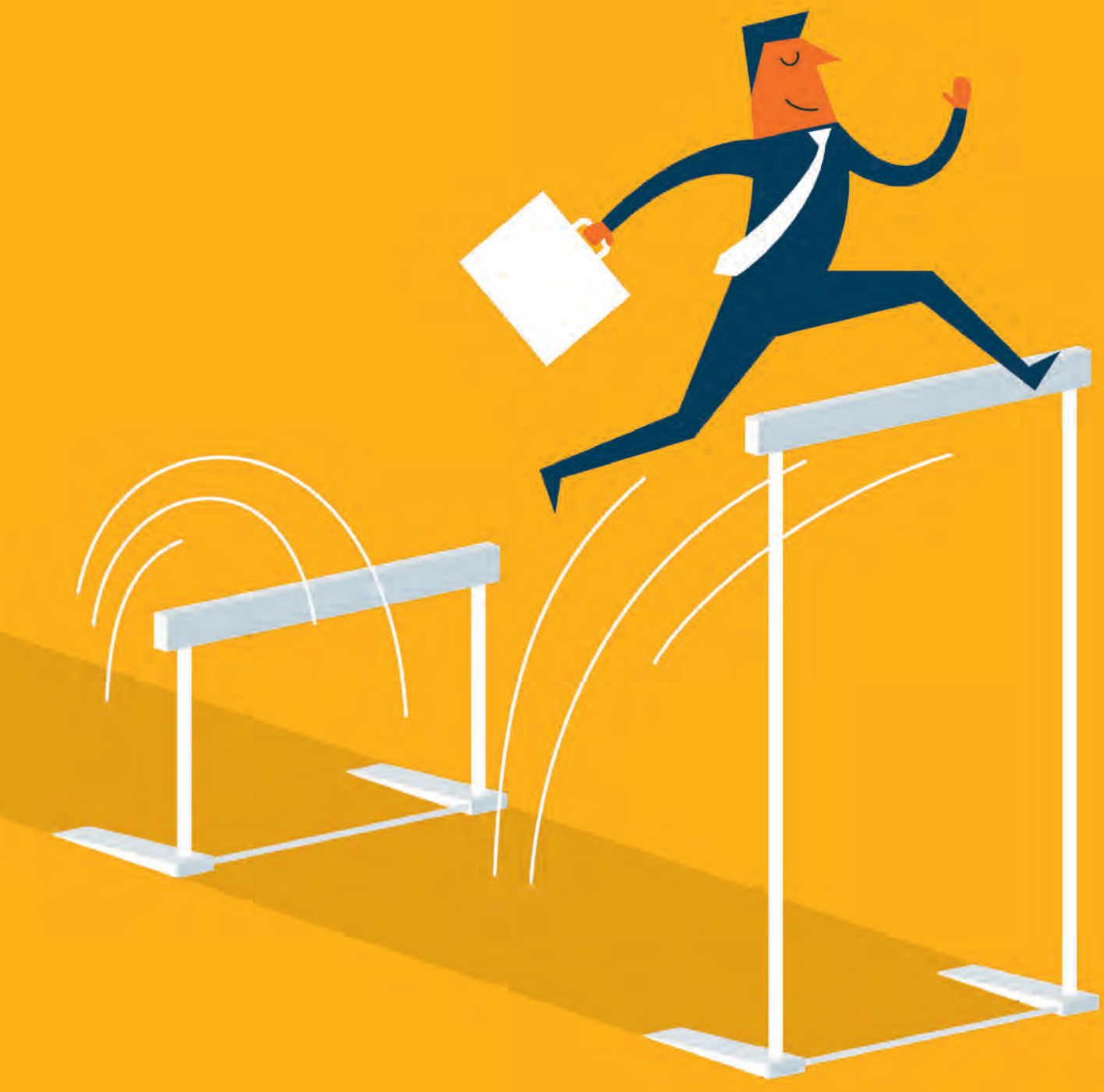


Adversarialer Angriff auf Verkehrsschilderkennung

Für Eingabedaten, die gut im Trainingsdatensatz repräsentiert wurden, trifft ein KI-System i. d. R. sehr robust die gewünschten Entscheidungen, wie hier links schematisch für die Verkehrsschilder „Stop“ und „100“ gezeigt. Angreifer machen sich bei adversarialen Angriffen allerdings den riesigen Eingaberaum von KI-Systemen zunutze, der unmöglich vollständig durch die Trainingsdaten repräsentiert werden kann, und suchen gezielt nach Eingaben, die zu einer gezielten Fehlentscheidung führen. Im schematischen Beispiel rechts hat ein Angreifer ein Muster für einen Aufkleber berechnet, welches zur Falscherkennung eines Stoppschildes als Geschwindigkeit-100-Schild führt.

COVID-19-Pandemie: Eine Feuertaufe für die neuen Regierungsnetze

von Dr. Lothar Eßer, Leiter des Referats Sicherheit in Regierungsnetzen: IT-Notfallmanagement und Anwendungen



Die aktuelle Pandemielage aufgrund von COVID-19 hat auch Auswirkungen auf informationstechnische Anwendungen und Infrastrukturen des Bundes, von denen die Netze des Bundes (NdB) besonders hervorzuheben sind.

Die Netze des Bundes haben als ressortübergreifende, zentrale Infrastruktur am 1. Juli 2019 den Informationsverbund Berlin-Bonn (IVBB) abgelöst, der zuvor 20 Jahre lang erfolgreich die Kommunikation zwischen den Bundesministerien, ihren nachgeordneten Bereichen, dem Deutschen Bundestag und den Bundesgerichten sichergestellt hat. Auch die NdB verfügen über besonders abgesicherte Übergänge in externe Netze, um den Mitarbeitenden in den genannten Behörden eine sichere Kommunikation, wie z.B. Telefonie oder Internetrecherche und natürlich auch die sichere Kommunikation mit den Kolleginnen und Kollegen in den Ländern, zu ermöglichen.

Die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) ist dabei für den Betrieb verantwortlich, und das Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Sicherheit in den NdB. Betreiber ist derzeit die Deutsche Telekom Business Solutions GmbH (DTBS). Alle drei Stellen arbeiten eng und konstruktiv zusammen und sorgen gemeinsam für einen schnellen und transparenten Informationsfluss, um die Stabilität und die Sicherheit der Regierungsnetze jederzeit auf einem hohen Niveau zu halten.

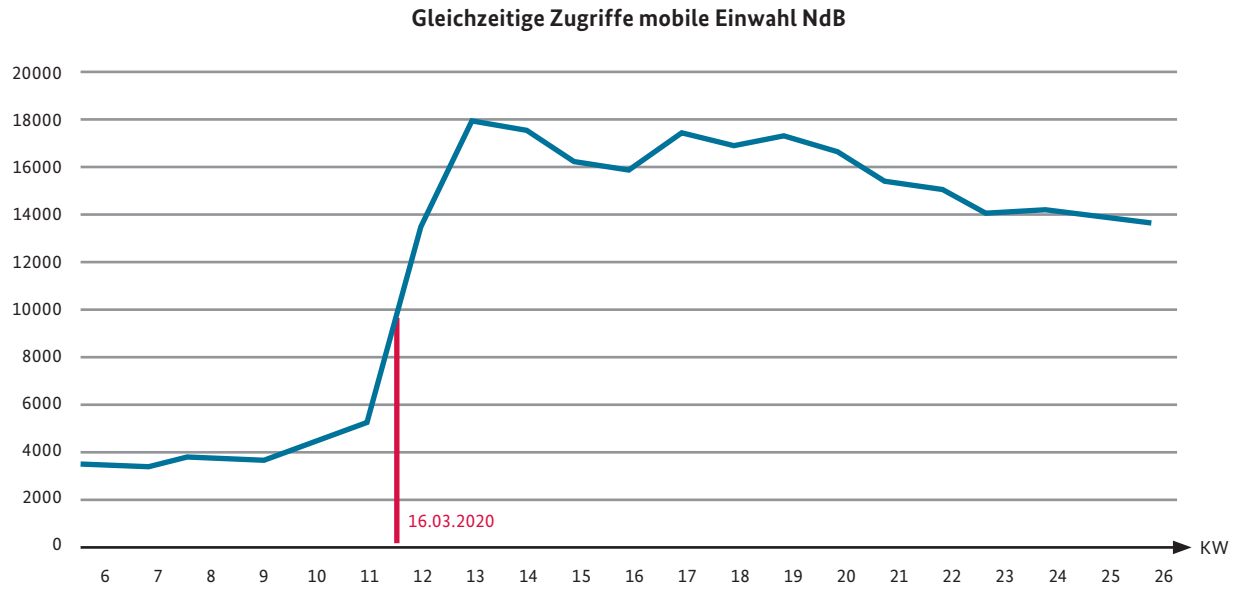
Die NdB bedienen deutschlandweit ca. 650 verschiedene Liegenschaften mit Schwerpunkt Bonn und Berlin. Die weit über 100.000 Mitarbeiterinnen und Mitarbeiter, die vor der Pandemie überwiegend ihre Arbeit in den Liegenschaften ihrer jeweiligen Behörde wahrnahmen, führen in der Regel am Tag durchschnittlich 100.000 behördenübergreifende Telefonanrufe über die zentrale Infrastruktur. An den zentralen Internetzugängen fallen in beiden Richtungen zwischen zwei und fünf Gbit/s an, und mehr als 1.000.000 E-Mails durchlaufen täglich das zentrale E-Mail-System.

Als Anfang des Jahres erste Berichte über die Verbreitung des COVID-19-Virus in China und den damit verbundenen Auswirkungen die Welt beunruhigten, wurde die Situation durch die drei für die NdB zuständigen Institutionen (BDBOS, BSI und DTBS) sehr aufmerksam beobachtet. Zunächst schien die Lage noch unter Kontrolle, und die WHO verhielt sich zurückhaltend gegenüber der Gefahr einer weltweiten Pandemie. Dennoch begann die DTBS präventiv bereits mit den ersten Vorsorgemaßnahmen. So wurden die Betriebsteams in Gruppen unterteilt, um einzelne, persönliche Kontakte außerhalb dieser Gruppen zu minimieren. In allen Gruppen war zudem ausreichend Expertenwissen vorhanden. U. a. dadurch konnte bis heute verhindert werden, dass Betriebspersonal in größerer Anzahl wegen einer Infektion mit dem Virus oder aufgrund einer Quarantäne ausfielen. Die weitere Ausbreitung in Italien und die Verbreitung des Virus im Kreis Heinsberg alarmierte alle drei Beteiligten. BDBOS und BSI analysierten daraufhin in enger Zusammenarbeit die technische Situation in der zentralen Infrastruktur unter der Annahme, dass eine größere Anzahl an Beschäftigten, z.B. wegen angeordneter Quarantäne, ihre Arbeit im Home Office erledigen muss.

Die Analyse führte zu folgendem Ergebnis:
Die eingesetzte Technik in der zentralen Infrastruktur ist, unter Beachtung der Wirtschaftlichkeit, so dimensioniert und durch Redundanzmaßnahmen so abgesichert, dass genügend Reserven für die hauptsächlich in den Behörden erzeugte Kommunikationslast zur Verfügung stehen.
Die Analyse zeigte aber auch, dass sich, unter der Annahme einer Verlagerung der Büroarbeit ins Home Office, Engpässe in den Bereichen mobile Zugänge, Telefon- und Videokonferenzen sowie bei der Telefonie ins öffentliche Netz ergeben würden. Um diesen Engpässen entgegen zu wirken, initiierten BDBOS und BSI umgehend, bereits vor Bekanntwerden der Schulschließungen, mit der DTBS die ersten technischen Maßnahmen und stießen die dafür notwendigen Beschaffungen an, um absehbaren Lieferengpässen entgegen zu wirken.

Mitte März überschlugen sich plötzlich und unerwartet, insbesondere mit einer bis dato nicht gekannten Heftigkeit, die Ereignisse mit bundesweiten Schulschließungen und weiteren von Bund und Ländern beschlossenen Vorsorgemaßnahmen gegen die Verbreitung des COVID-19-Virus. Tatsächlich wechselten viele Behördenmitarbeiterinnen und -mitarbeiter in der Folge ins Home Office und nahmen ihre Dienstgeschäfte von dort aus wahr.

In Abbildung 1 ist erkennbar, dass sich die gleichzeitige Nutzung eines der wichtigsten mobilen Dienste am 16. März 2020, dem ersten Tag der Schulschließungen, von etwa 4.000 schlagartig auf über 9.000 erhöhte. In den folgenden Tagen und Wochen stieg die gleichzeitige Nutzung weiter auf über 16.000.



Zum Zeitpunkt der Schulschließungen waren noch nicht alle zuvor initiierten Maßnahmen vollständig umgesetzt. Daher kam es in den ersten ein bis zwei Wochen nach dem 16. März 2020 zu Einschränkungen, insbesondere bei der Telefonie ins öffentliche Netz und bei den Telefonkonferenzen. Alle Beteiligten verstärkten ihre Anstrengungen weiter, um die Einschränkungen schnellstmöglich zu beseitigen.

Insgesamt wurde in kurzer Zeit u. a. der wichtigste mobile Dienst in seiner Kapazität vervierfacht. Die Anschlüsse an das öffentliche Telefonnetz wurden mehr als verdoppelt. Die Anzahl der gleichzeitigen Teilnehmerinnen und Teilnehmer an Telefonkonferenzen wurde um den Faktor 22 erhöht. Die Redundanz des Internetzugangs wurde verbessert, und die Bandbreite an einem Standort um sechs Gbit/s erhöht. Die Möglichkeiten des mobilen Zugriffs per Smartphone wurden ebenfalls um etwa 50 Prozent ausgebaut. Daneben stehen demnächst weitere neue mobile Dienste zur Verfügung.

Als größte Herausforderung erwies sich die Erhöhung der Kapazitäten im Bereich der Videokonferenzlösungen. Die Verlagerung einer großen Anzahl an Arbeitsplätzen ins Home Office erhöhte schlagartig die Notwendigkeit, direkt vom Arbeitsplatz aus Videokonferenzen mit den Kolleginnen und Kollegen oder externen Partnern durchzuführen. Dabei ist zu beachten, dass Videokonferenzen innerhalb der NdB verschlusssachentauglich sein müssen.

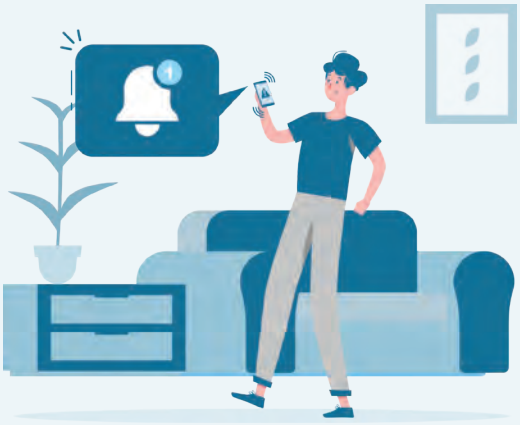
Die meisten Behörden betreiben ihre an den NdB angeschlossenen Hausnetze eigenständig. Sie gehören damit, genau wie früher beim IVBB, nicht zur zentralen Infrastruktur. Die Behörden stehen daher genauso vor der Herausforderung, ihren Mitarbeiterinnen und Mitarbeitern entsprechende Videokonferenzlösungen zur Verfügung zu stellen. Aufgrund des hohen Bedarfs und gleichzeitig fehlender Kapazitäten, werden in manchen Behörden eigene Lösungen umgesetzt oder Lösungen von Cloudanbietern verwendet.

In den NdB verstärkte die BDBOS ihre Anstrengungen, das bestehende Angebot an sicheren Videokonferenzlösungen aus eigener Hand mit Unterstützung des BSI deutlich auszubauen. Verbesserungen an der Technik der verschlusssachenkonformen Lösungen sowie der Aufbau eines Systems für den normalen Schutzbedarf für bis zu 1.000 gleichzeitige Teilnehmerinnen und Teilnehmer sind bereits zu vermelden.

FAZIT

Knapp ein halbes Jahr nach dem Start der Netze des Bundes haben die neuen Regierungsnetze bereits die erste Feuertaufe überstanden. Dazu mussten zahlreiche Erweiterungen in kürzester Zeit umgesetzt werden. Diese waren aufgrund eines sich über Nacht stark veränderten Nutzungsverhaltens in der COVID-19-Pandemie notwendig geworden. Dazu haben alle Beteiligten eng und konstruktiv zusammengearbeitet und können die in den letzten Wochen gewonnenen Erkenntnisse und Erfahrungen in die nun zu erwartenden neuen Herausforderungen einbringen. Denn weder die COVID-19-Pandemie noch die damit verbundenen Maßnahmen in den NdB sind abgeschlossen. Zusätzlich müssen die zentrale Firewall sowie die Netz- und Behördenanschlusskapazitäten mit ihren Sicherheitsmaßnahmen angepasst werden, um für jeden Arbeitsplatz, ob im Büro oder im Home Office, auch Anwendungen mit hoher Datenrate, wie Videokonferenzlösungen, sicher zu ermöglichen. ■

DIGITALE GESELLSCHAFT



BSI-Basistipp

Heute schon geupdatet?

Update, Patch, Aktualisierung oder Bugfix – warum regelmäßige Updates so wichtig sind

Die Aufforderung ein Update durchzuführen, also Software zu aktualisieren, taucht gefühlt meist dann auf, während man wichtige Arbeiten am Computer oder am Smartphone erledigt. Doch so lästig diese Aufforderungen manchmal sind: Updates schützen. Betriebssysteme für PC und Laptop, Apps von Smart-TVs, Software von Smartphones oder auch das Virenschutzprogramm – sie alle bieten nur dann Computerschädlingen möglichst wenig Angriffsfläche, wenn sie auf dem aktuellsten Stand sind. Umso bedenklicher ist, dass nur ein Viertel (25 Prozent) der Internetnutzer und -nutzerinnen in Deutschland die automatische Installation von Updates aktiviert. Das ergab die Umfrage „Digitalbarometer 2020“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK). 57 Prozent der Befragten verlassen sich auf Maßnahmen wie Virenschutzprogramme oder Firewalls. Regelmäßige Updates bieten jedoch eine Schutzwirkung, die nicht zu unterschätzen ist, und stellen so eine wichtige präventive Maßnahme dar. Sie schließen Sicherheitslücken, beseitigen Bugs im Betriebssystem oder fügen neue Funktionen hinzu. So verhindern Updates, dass ein Antivirenprogramm beispielsweise bereits eingeschleuste Schadprogramme aufspüren und blockieren bzw. entfernen muss.

Das Ignorieren von Updates kann unangenehme Folgen haben. Betrüger können so bekannte Sicherheitslücken ausnutzen, um Schadprogramme zu installieren. Die Folgen können erheblich sein: Schadprogramme kann Daten stehlen, löschen oder verschlüsseln sowie Programme manipulieren, was bis zum vollständigen Verlust von Daten oder dem Missbrauch so abgegriffener Passwörter und Bankdaten führen kann.

Prominentes Beispiel: Im April 2017 infizierte die Malware WannaCry Zehntausende Computer auf der ganzen Welt und verschlüsselte Dateien, die sich auf ihnen befanden. Dies war möglich, weil die Windows-Betriebssysteme nicht auf die neueste Version aktualisiert worden waren. Und selbst heute sind Systeme ohne dieses Update nach wie vor durch WannaCry gefährdet. Aktualisierte Systeme waren und sind für diese Malware hingegen unangreifbar.

SO BEHALTEN SIE DEN ÜBERBLICK ÜBER WICHTIGE SOFTWARE-UPDATES

1. Verschaffen Sie sich einen Überblick über die von Ihnen eingesetzten Programme auf dem PC, Laptop, Tablet oder Smartphone! Prüfen Sie, zu welchen Produkten Sie automatische Update-Services einrichten können und bevorzugen Sie immer automatische Updates.
2. Machen Sie es sich zur Regel, Hinweise auf Updates zu beachten und nicht wegzuklicken!
3. Erstellen Sie eine Übersicht darüber, für welche Programme Sie eigenständig auf Updates achten müssen! Informieren Sie sich regelmäßig über Updates – etwa durch den Newsletter „Sicher ° Informiert“ des BSI.
4. Installieren Sie Updates möglichst sofort, sobald diese verfügbar sind!

Weitere Informationen:

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

9-Punkte-Plan für ein digitales Deutschland

Ein Interview mit Dr. Markus Richter, Staatssekretär im Bundesministerium des Innern, für Bau und Heimat und Beauftragter der Bundesregierung für Informationstechnik

■ **Herr Staatssekretär Dr. Richter, Sie haben bereits kurz nach Ihrem Amtsantritt einen „9-Punkte-Plan für ein digitales Deutschland" veröffentlicht, mit dem Sie die Digitalisierung in Deutschland voranbringen wollen. Was sind die Kernpunkte dieses Plans?**

Wir möchten in den kommenden Monaten spürbare Fortschritte bei der Digitalisierung erzielen. Dazu haben wir die aus unserer Sicht neun wichtigsten Punkte in einem Schwerpunkteplan zusammengestellt, der auf den drei Säulen der Digitalisierung im BMI fußt: Digitale Gesellschaft, Digitale Verwaltung sowie Cyber- und Informationssicherheit. Ich bin davon überzeugt, dass wir mit der Umsetzung des Plans die Digitalisierung in Deutschland ein bedeutendes Stück voranbringen werden.

Unser Ziel ist es auch, die Menschen vom Mehrwert der Digitalisierung zu überzeugen. Das gelingt nur, wenn wir ihre Vorteile möglichst schnell greifbar machen.

Wir priorisieren daher Projekte, die konkrete Ergebnisse produzieren: Dicke Bretter wie die Umsetzung des Onlinezugangsgesetzes, aber auch ganz konkrete Meilensteine wie der Aufbau einer Digitalakademie zur Qualifizierung der Verwaltungsmitarbeitenden, Optimierungen beim Online-Ausweis, die flächendeckende Einführung von E-Rechnung und E-Akte und die Evaluierung und Fortschreibung der Cyber-Sicherheitsstrategie aus dem Jahr 2016 werden uns in den kommenden Monaten stark beschäftigen.

■ **Wo sehen Sie im Bereich Cyber-Sicherheit die Herausforderungen?**

Für die Cyber-Sicherheit ergeben sich die Herausforderungen insbesondere aufgrund der zunehmenden Digitalisierung aller Lebensbereiche und generell dem stetigen Technologiefortschritt.

Wir machen deutliche Fortschritte bei der Stärkung der Cyber- und Informationssicherheit, stehen aber immer wieder einer Vielzahl neuer Entwicklungen gegenüber, die naturgemäß auch Risiken mit sich bringen. Neue Technologien wie Wearables, d. h. intelligente elektronische Geräte, die am Körper getragen werden, durchdringen unseren Alltag, allen voran die Smart Watch. Durch die ständige Internetanbindung sowie das GPS-Tracking dieser Geräte werden neue Möglichkeiten für kriminelle Absichten eröffnet, wie z.B. die Verletzung der Privatsphäre von Nutzerinnen und Nutzern.

Wir müssen außerdem feststellen, dass Schadprogramme immer ausgefeilter und Cyber-Angriffe gezielter ausgeführt werden. Das seit längerer Zeit bekannte Schadprogramm Emotet beispielsweise wird durch Angreifer fortlaufend angepasst und mit neuen Fähigkeiten ausgestattet. Emotet wird über Spam-Kampagnen verteilt und stellt eine akute Bedrohung für den Anwender dar.

Das Schadprogramm liest u. a. die Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern infizierter Systeme aus. Diese Informationen nutzen die Täter dann zur weiteren Verbreitung des Programms. Ist ein System erst einmal infiziert, lädt Emotet weitere Schadsoftware nach. Für Privatanwender kann eine Infektion den Verlust von wichtigen Daten bedeuten.

Eine weitere große Herausforderung sehe ich auch im Erhalt und in der Stärkung der digitalen Souveränität Deutschlands und Europas. Aktuell bestehen für die Öffentliche Verwaltung große Abhängigkeiten von einzelnen IT-Anbietern. Dies kann auch zu Risiken wie eingeschränkter Informations- und Datensicherheit führen. Es ist daher notwendig, die Digitale Souveränität und somit die eigene Handlungsfähigkeit im digitalen Raum weiter zu stärken, und dies gehen wir an.

„Eine große Herausforderung sehe ich im Erhalt und in der Stärkung der digitalen Souveränität Deutschlands und Europas.“

■ Wie kann Ihnen das BSI in seiner Rolle als Gestalter der Informationssicherheit in der Digitalisierung bei der Umsetzung Ihres 9-Punkte-Plans helfen?

Als Cyber-Sicherheitsbehörde des Bundes ist es Aufgabe des BSI, Deutschland digital sicher zu machen. Seit nun fast schon 30 Jahren ist das BSI inzwischen an unserer Seite. Sie unterstützen vielseitig, um ein Höchstmaß an IT-Sicherheit für die Bevölkerung zu gewährleisten. Hierfür möchte ich Ihnen zunächst danken.

Unser Ziel ist es, den Menschen den sicheren Zugang zu digitalen Lebensräumen zu erleichtern. Die Bürgerinnen und Bürger, aber auch Unternehmen, müssen sich sicher fühlen, wenn sie bspw. die im Rahmen des Onlinezugangsgesetz digitalisierten Verwaltungsleistungen in Anspruch nehmen. Und hierfür brauchen wir das BSI, mit Blick auf das Onlinezugangsgesetz denke ich da insbesondere an Ihr Angebot zur Sicherheitsberatung.

In unserem 9-Punkte-Plan haben wir eine Vielzahl von Themen verankert, die direkt durch das BSI umgesetzt werden müssen. Nehmen wir nur das Thema digitaler Verbraucherschutz, das mit dem IT-Sicherheitsgesetz 2.0 Aufgabe des BSI werden soll.

In diesem Zusammenhang planen wir die Einführung eines einheitlichen und freiwilligen IT-Sicherheitskennzeichens. Dieses Kennzeichen macht die IT-Sicherheit von Produkten im Verbrauchersegment erstmals für Bürgerinnen und Bürger transparent und nachvollziehbar. Grundlage hierfür bilden zunächst Technische Richtlinien des BSI. Die erste Technische Richtlinie wurde durch das BSI bereits für Breitband-Router erstellt. Ziel ist, dass sich die Bürgerinnen und Bürger mit diesem „digitalen Beipackzettel“ über die IT-Sicherheit der von ihnen erworbenen Produkte informieren können. ■

Kurzprofil Dr. Markus Richter

Dr. Markus Richter ist Staatssekretär im Bundesministerium des Innern, für Bau und Heimat und Beauftragter der Bundesregierung für Informationstechnik. Der Jurist war unter anderem Referatsgruppenleiter IT im Bundesverwaltungsamt, Abteilungsleiter für Infrastruktur und IT und CIO im Bundesamt für Migration und Flüchtlinge und Vizepräsident im Bundesamt für Migration und Flüchtlinge. Dr. Markus Richter wurde 1976 in Münster/Westfalen geboren. Er hat zwei Kinder.

Wie sicher ist kontaktloses Bezahlen per Near Field Communication?

Das BSI unterzog Bezahlkarten und Bezahlterminals umfassenden Tests

von Sabine Mull und Rainer Schönen, Referat Cyber-Sicherheit im Gesundheits- und Finanzwesen

Die Angst, dass kontaktlose Bankkarten nicht nur an dem entsprechenden Kassenterminal, sondern quasi immer und überall ausgelesen werden können, treibt viele Nutzerinnen und Nutzer von Giro- und Kreditkarten um, die mit einem entsprechenden NFC-Chip ausgestattet sind. Immer wieder gibt es in unterschiedlichen Medien Berichte darüber, dass die Funktion zum kontaktlosen Bezahlen in Girocards und Kreditkarten ein Sicherheitsrisiko darstellt. So wird in Videobeiträgen gezeigt, wie mit einem kleinen mobilen Zahlterminal Geldbeträge bis zu 50€ unberechtigt von den Konten ahnungsloser Passanten abgebucht werden. Dazu wird nur das Terminal an die Hosentasche oder die Handtasche gehalten und schon ist der Diebstahl erfolgt.

WIE REAL IST DIESE GEFAHR WIRKLICH?

Zunächst ist zu bedenken, dass Kriminelle ein Konto mit dem Zahlterminal verknüpfen müssen, damit überhaupt Geld abgebucht werden kann. Um ein Konto zu öffnen, müssen sich Kriminelle nach den Standards des Geldwäschegesetzes identifizieren, so dass hier eine erste Hürde existiert.

Daneben gibt es technische Aspekte zu beachten. Die Reichweite von „Near Field Communication", dem Funkstandard NFC, der die kontaktlose Kommunikation zwischen Karte und Terminal ermöglicht, beträgt lediglich wenige Zentimeter. Das führt dazu, dass Kriminelle schon sehr nah in die Komfortzone des Opfers eindringen müssen. Zusätzlich kann die Signalstärke durch unterschiedliche Materialien gedämpft werden.

AD-HOC-UNTERSUCHUNGEN

Zur Überprüfung der angesprochenen Berichte hat das BSI Szenen aus diesen Videos nachgestellt und untersucht, ob kontaktlose Zahlungen unbemerkt ausgelöst werden können, vor allem wenn gleichzeitig mehrere NFC-fähige Karten präsentiert werden.

Dazu wurden verschiedene Karten (Girocards, Kreditkarten, Jahreskarten des ÖPNV und Personalausweise), die über einen NFC-Chip verfügen, in den unterschiedlichsten Kombinationen in das Lesefeld eines Bezahlterminals geführt. Die Ergebnisse waren jedoch weder eindeutig noch vollständig nachvollziehbar: In manchen Fällen wurde keine der Karten ausgelesen, in anderen wurde eine Karte ausgelesen, aber nicht die, die dem Lesegerät am nächsten war. Bei weiteren Versuchen mit unterschiedlichen Karten wurde stets eine bestimmte Karte ausgelesen, unabhängig von ihrer Position zum Lesegerät. Es gab definitiv keine konsequente nachvollziehbare Störung durch eine weitere oder generell mehre Karten, die verhindert hätte, dass eine Zahlung ausgelöst wird.

Es hat sich jedoch gezeigt, dass Abbuchungen nicht so einfach im Vorbeigehen ausgelöst werden können. Dies gelang weder bei einem Portemonnaie in der Gesäßtasche noch bei einer Geldbörse in der Handtasche zuverlässig, unabhängig davon, wie viele NFC-fähige Karten in den Geldbeuteln aufbewahrt wurden.

SYSTEMATISCHE UNTERSUCHUNGEN IN EINER DEFINIERTEN LABORUMGEBUNG

Diese Vorabuntersuchungen wurden in einem unabhängigen Prüflabor weiter vertieft. Für die Tests wurden sowohl verschiedene Kartentypen aus den unterschiedlichsten Einsatzbereichen wie Kreditkarten, Debitkarten, Prepaidkarten, VDV-Karten und eID-Dokumente ausgewählt als auch verschiedene Lesegeräte wie Zahlungsterminals, Mobiltelefone und spezifizierte Referenzgeräte verwendet.

Bei Lesegeräten bzw. Terminals, die auf Grundlage des Standards „EMVCo Contactless" (Karten mit Bezahlfunktion) entwickelt wurden, soll bei der gleichzeitigen Präsentation von mehreren Karten tatsächlich keine ausgewählt werden. Bei auf der ISO/IEC 14443 und NFC-Forum basierenden Terminals ist dies nicht so. Hier ist sogar gewollt, dass aus mehreren Karten auf jeden Fall eine ausgewählt wird.

Dies kann das unterschiedliche Verhalten mehrerer Karten in einem Lesefeld erklären. So sollen beispielsweise ÖPNV-Jahreskarten immer noch erkannt werden, auch wenn eine Kreditkarte im gleichen Feld funkt. Mehrere Zahlkarten hingegen sollten sich gegenseitig stören.

ERGEBNISSE

Auch bei den Tests, die mit dem Prüflabor durchgeführt wurden, stellte sich heraus, dass von EMVCo-Lesegeräten selbst dann eine Zahlkarte ausgewählt werden kann, wenn diese mit anderen Zahlkarten in das Lesefeld gehalten wird. Der Antikollisionsmechanismus des Lesegeräts greift also nicht immer zuverlässig.

FAZIT

Untersuchungen mit unterschiedlichen Bezahlterminals haben ergeben, dass das gleichzeitige Vorhandensein von mehreren kontaktlosen Karten keine Garantie dafür ist, dass ein ungewolltes Auslesen einer dieser Karten zuverlässig verhindert wird. Die einzig wirkungsvolle Schutzmaßnahme ist die Verwendung von geeigneten Schutzhüllen, in denen kontaktlose Karten aufbewahrt werden sollten. Nur so kann sichergestellt werden, dass eine ungewollte Kommunikation zwischen einem beliebigen Lesegerät und einer oder mehreren kontaktlosen Karten verhindert wird.

Grundsätzlich stellt sich allerdings die Frage, wie wahrscheinlich es ist, dass Angreifer die Karte in Hosentaschen oder Handtaschen lokalisieren können, ohne dass die persönliche Komfortzone des Opfers verletzt wird. ■

Sichere elektronische (Fern-) Identifizierung und Know Your Customer (KYC)-Prozesse

Voraussetzungen und einheitliche Regelungen für Europa zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung

von Stephan Kohzer, Referat Cyber-Sicherheit im Gesundheits- und Finanzwesen

Im Frühjahr 2018 konstituierte die Europäische Kommission eine Expertengruppe zu den Themen „Electronic Identification (eID) and Remote Know-Your-Customer (KYC) Processes“. Das Ziel: europaweit sichere elektronische (Fern-) Identifizierungen und einheitliche Know-Your-Customer-Prozesse. Das BSI beteiligt sich aktiv an der Gestaltung eines europäischen digitalen Binnenmarkts mit gemeinsamen Standards.

UNGEWÖHNLICHE AKTIVITÄTEN FRÜHZEITIG AUFDECKEN

Mit dem übergeordneten Ziel, Wirtschaftskriminalität, Geldwäsche und Terrorismusfinanzierung zu bekämpfen, haben die Mitgliedsstaaten der EU schon lange staatliche Regelungen aufgestellt. In Deutschland ist hier insbesondere das Geldwäschegesetz relevant, das vergleichsweise hohe Vorgaben an die Identifizierung von Kunden der Geldwäscheverpflichteten – insbesondere Banken oder Versicherungen – stellt.

Neben der Identifizierung sind regelmäßig weitere Kriterien zu prüfen und Risikobewertungen vorzunehmen: Was ist der Zweck der Geschäftsbeziehung?

Finden ungewöhnliche Geldströme statt? Gibt es Verbindungen zu sogenannten Risikostaaten? Ist der Kunde bereits auffällig geworden oder bekleidet er ein Amt, das anfällig für illegale Geldströme ist? Die eindeutige Identifizierung, die Risikobetrachtungen und erweiterten Sorgfaltspflichten sind Teile der sogenannten „Know Your Customer"- (KYC-) Prozesse und sollen sicherstellen, dass ungewöhnliche Aktivitäten frühzeitig aufgedeckt werden.

FERNIDENTIFIZIERUNG IM AUFSCHWUNG

Jeder kennt die Identifizierung mittels des Personalausweises oder des Reisepasses bei der Kontoeröffnung in einer Bankfiliale vor Ort. Hierbei wird der physische Ausweis von geschultem Personal auf Echtheit überprüft, und ein Abgleich mit der Person vor Ort durchgeführt.

Daneben wurden im Laufe der Zeit weitere Verfahren entwickelt, die eine Präsenzüberprüfung vor Ort verzichtbar machen. So ermöglichen z.B. Online-Anträge mit Identifizierung in einer Postfiliale (sog. PostIdent-Verfahren) oder übergangsweise via Videointerview eine Identifizierung von nicht anwesenden Kundinnen und Kunden. Im Gegensatz zu PostIdent und Videointerview, die nicht durchgehend digital und medienbruchfrei sind, sind Online-Anträge mit Nutzung der Online-Ausweisfunktion/eID des Personalausweises vollständig digital und medienbruchfrei. Zur Verwirklichung des digitalen Binnenmarktes in der EU, zur Stärkung des Wettbewerbs und zur Nutzung der digitalen Angebote unabhängig von Nationalität und Wohnsitz werden solche Verfahren für die Fernidentifizierung zukünftig unabdingbar sein, vorzugsweise in ihren digitalen und medienbruchfreien Varianten.

Wie kann ich als Kunde in einem anderen europäischen Mitgliedsstaat online ein Konto eröffnen und mich aus der Ferne eindeutig identifizieren? Welche Standards sind notwendig, um hier von Seiten der Anbieter eine ausreichende Überprüfung der elektronischen Daten und eine zweifelsfreie Zuordnung zum Antragssteller vornehmen zu können? Wie können die unterschiedlichen staatlichen, privatwirtschaftlichen und länderspezifischen Lösungen hinsichtlich ihrer Sicherheit und Vertrauenswürdigkeit eingestuft und miteinander verglichen werden?

Die von der EU-Kommission ins Leben gerufene Expertengruppe (EG) hat genau solche Fragen diskutiert und sich insbesondere auf zwei Themenschwerpunkte fokussiert:

1. Eine Bestandsaufnahme der aktuell eingesetzten elektronischen Verfahren wurde durchgeführt. Gleichzeitig wurde analysiert, wie die Kundendaten zu den Anbietern gelangten. Die Sicherheit und Vertrauenswürdigkeit der erhobenen Daten aus den jeweiligen Verfahren wurden eingeschätzt.

2. Unabhängig von bestehenden Verfahren sollte auf Grundlage der eIDAS-Identifizierungs- und Authentifizierungsmittel ein Rahmenwerk entwickelt werden, das zukünftig die Basis für europaweite Identifizierungen und Nutzbarkeit/Übertragbarkeit der erhobenen KYC-Daten darstellt. Insbesondere Fragestellungen zu den Themen Mindestdatensatz, notwendige und einheitliche Vertrauensniveaus, sichere Datenquellen und Übertragungswege wurden hier aufgegriffen.

Die Ergebnisse der beiden Themenschwerpunkte veröffentlichte die EU-Kommission in zwei Berichten Ende März 2020.

HOHE ANFORDERUNGEN FÜR EUROPAWEITE VORGABEN UND STANDARDS

Aus Sicht des BSI sind für die europaweite elektronische Identifizierung und KYC-Prozesse folgende Punkte von besonderer Relevanz:

Mit der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (kurz: eIDAS-Verordnung) existiert ein Standard, an dem sich zukünftige – auch privatwirtschaftliche – Verfahren orientieren sollten. Zukünftige – auch privatwirtschaftliche – Verfahren sollten sich an diesem Standard orientieren.

Zudem ist wichtig, dass einheitliche Vorgaben und Standards innerhalb der EU gefestigt werden. Ansonsten würden unterschiedliche Lösungen mit nicht vergleichbaren Sicherheitsniveaus Arbitragemöglichkeiten bieten. Die vermehrte Nutzung des Verfahrens mit den geringsten Anforderungen würde dazu führen, dass alternative sicherere Verfahren aus dem Markt verdrängt werden und das Sicherheitsniveau grundsätzlich verschlechtert wird.

Das BSI wird die Aktivitäten der Kommission und der Mitgliedsstaaten weiterhin verfolgen, um das Ziel IT-Sicherheit voranzubringen und damit auch die Bekämpfung von Wirtschaftskriminalität, Geldwäsche und Terrorismusfinanzierung IT-technisch zu unterstützen. ■

Weitere Informationen:

https://ec.europa.eu/digital-single-market/en/news/reports-expert-group-eid-and-kyc-processes

Gemeinsam für eine sichere digitale Welt

Der vzbv und das BSI kooperieren, um den digitalen Verbraucherschutz in Deutschland voranzubringen

von Dr. Angelika Praus, Projektgruppe Digitaler Verbraucherschutz

Cyber-Sicherheit ist eine Gemeinschaftsaufgabe. Ein wirksamer Verbraucherschutz in der digitalen Welt kann daher nur im Rahmen eines kooperativen Ansatzes gelingen. Der Verbraucherzentrale Bundesverband e.V. (vzbv) als etablierter Akteur des Verbraucherschutzes hat eine starke Stimme in der Öffentlichkeit und ist für das BSI ein wichtiger Partner.

In einer gemeinsamen Grundsatzvereinbarung („Memorandum of Understanding", kurz MoU) haben sich der vzbv und das BSI für zunächst drei Jahre zu einer partnerschaftlichen Zusammenarbeit bekannt. Zum Schutz der Verbraucherinnen und Verbraucher in der digitalen Welt ermöglicht diese Kooperation eine Kombination aus technischer Expertise, verbraucherrechtlichen Befugnissen und Wirksamkeit in der Fläche. Mit ihr sollen Synergien geschaffen werden, die direkt bei den Verbraucherinnen und Verbrauchern ankommen.

Konkret werden mit der Partnerschaft diese Ziele verfolgt:

- Einsatz für sichere vernetzte IT-Systeme und Online-Dienste
- Information und Aufklärung der Verbraucherinnen und Verbraucher über Reaktionsmöglichkeiten im Schadensfall
- Sensibilisierung der Bevölkerung für Schutzmöglichkeiten im Zusammenhang mit digitalen Anwendungen
- Gemeinsame Aktivitäten – sofern rechtlich möglich – um präventiv gegen mögliche Verstöße gegen den bestehenden Rechtsrahmen im Bereich des Verbraucherschutzes vorzugehen

Diese Zielsetzung soll dazu beitragen, dass seitens der Wirtschaft die Sicherheit der Produkte und Anwendungen erhöht wird und bei Verbraucherinnen und Verbrauchern eine angemessene Resilienz gegenüber Bedrohungen und Gefahren für die Informationssicherheit erzeugt wird.

Ein erstes gemeinsames Projekt von vzbv und BSI befasst sich mit dem Thema „Zwei-Faktor-Authentisierung". Aus einem systematischen Marktüberblick und einer technischen Bewertung der eingesetzten Verfahren sollen Empfehlungen für unterschiedliche Zielgruppen abgeleitet werden. Um Interessen von Verbraucherinnen und Verbrauchern im Bereich Informationssicherheit durchzusetzen, beabsichtigen vzbv und BSI außerdem, bestehende Befugnisse (Klagebefugnis durch den vzbv) und Kompetenzen (technische Expertise durch das BSI) im Rahmen der Rechtsdurchsetzung zu verbinden.

Das Memorandum of Understanding zwischen vzbv und BSI ist abrufbar unter:

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

DREI FRAGEN AN KLAUS MÜLLER (VORSTAND DES VERBRAUCHERZENTRALE-BUNDESVERBANDS)

■ Wie können Verbraucherinnen und Verbraucher in der digitalen Welt gestärkt werden?

Digitale Produkte und Systeme werden immer komplexer, so dass sie für viele Menschen kaum noch zu verstehen sind. Die Verantwortung für IT-Sicherheit darf also nicht auf die Verbraucherinnen und Verbraucher abgewälzt werden. Wir fordern daher eine sichere und datenschutzfreundliche Technikgestaltung durch die Hersteller. Produkte und Dienste müssen von Anfang an ein hohes Maß an IT-Sicherheit nach dem Stand der Technik erfüllen – Stichwort: „Security by Design" – und mit sicheren Voreinstellungen ausgestattet sein – Stichwort: „Security by Default". Verbraucherinnen und Verbraucher müssen darauf vertrauen können, dass Produkte und Dienste bereits bei ihrer Entwicklung und Implementierung ein hohes Maß an IT-Sicherheit erfüllen und auch während ihrer Lebensdauer mit Sicherheits-Updates versorgt werden. Die Datenskandale der vergangenen Jahre zeigen, dass dafür klare gesetzliche Regelungen notwendig sind.

■ Welchen Mehrwert bietet die Zusammenarbeit von vzbv und BSI für Verbraucherinnen und Verbraucher?

Der vzbv widmet sich verstärkt dem Thema IT-Sicherheit. Mit der Zusammenarbeit von vzbv und BSI bündeln wir unsere Kompetenzen und erzeugen Synergieeffekte. Der vzbv bringt seine Erfahrung in der Rechtsdurchsetzung, der politischen Arbeit und der Marktbeobachtung ein. Das ergänzt sich ideal mit der herausragenden technischen Expertise des BSI im Bereich der Cyber-Sicherheit. Davon profitieren die Verbraucherinnen und Verbraucher.

■ Welche konkreten Themen haben für Sie im Bereich des digitalen Verbraucherschutzes in den nächsten drei Jahren besondere Relevanz?

Mit zunehmender Vernetzung wird die IT-Sicherheit immer wichtiger. Wir brauchen einen starken Datenschutz. Die Wahrung der Privatsphäre hat hohe Priorität. Auch die Spielregeln für den Einsatz von Künstlicher Intelligenz gewinnen immer größere Relevanz für den Verbraucherschutz. Deshalb arbeitet der vzbv daran, diese mitzugestalten.

„Mit der Kooperation sollen Synergien geschaffen werden, die direkt bei den Verbraucherinnen und Verbrauchern ankommen."

Kurzprofil Klaus Müller

Klaus Müller, Jahrgang 1971, ist seit Mai 2014 Vorstand des Verbraucherzentrale-Bundesverbands (vzbv). Der vzbv ist der Dachverband der 16 Verbraucherzentralen und 26 weiterer verbraucherpolitisch orientierter Verbände. Von 2006 bis 2014 leitete Klaus Müller die Verbraucherzentrale Nordrhein-Westfalen. Zuvor war der Volkswirt in der Politik tätig: Vom Jahr 2000 bis 2005 war er Umweltminister in Schleswig-Holstein, bis 2006 Mitglied des Schleswig-Holsteinischen Landtags. Von 1998 bis 2000 war Klaus Müller Abgeordneter des Deutschen Bundestages.

Arbeiten im BSI: Das New Normal aktiv gestalten

von Bettina Jäkel-Schmidt, Referat Personalentwicklung

Noch gut erinnern wir uns alle an den Lockdown im März 2020, als plötzliche Veränderungen in unserem Arbeitsalltag auftraten. Auch das BSI hatte viele Herausforderungen zu bewältigen: Schlagartig befanden sich die Mitarbeitenden überwiegend im Home-Office, trafen sich in digitalen Meetings, und der „kleine Dienstweg" zur Klärung von Anliegen in der Kaffeeküche war nicht mehr möglich. Diese Erfahrung, die das Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO) als „großartige Leistung" und „Gemeinschaftserlebnis" bezeichnet, wurde auch am BSI so erlebt: Alle waren stolz, dass die Herausforderung so gut bewältigt werden konnte.

SCHNELLE ANPASSUNG AN DIE NEUEN BEDINGUNGEN

Das BSI erlangte in der Pandemie sehr schnell eine neue Normalität: Eine hohe Quote an mobilem Arbeiten, der schnelle Umstieg auf Videokonferenzen und auch die Digitalisierung der Facharbeit, wie z.B. der Umstieg auf virtuelle Vorstellungsgespräche, kennzeichneten diese Phase.
Dabei waren die Erfahrungen mit der veränderten Arbeitssituation individuell unterschiedlich: Obwohl viele das Home-Office als konzentrierteres Arbeiten schätzten, vermissten sie gleichzeitig die Begegnung und die persönliche Abstimmung vor Ort.

VERÄNDERTE FÜHRUNG

Das BSI hat bereits 2019 einen Prozess zur Weiterentwicklung der Führungskultur gestartet. Kern dieses Prozesses ist die Fokussierung auf einen wirkungsorientierten Führungsstil. Die Corona-Krise und die Auseinandersetzung mit einer Arbeitskultur im New Normal haben als Katalysator fungiert: Durch das überwiegend mobile Arbeiten sind Führungskräfte stärker denn je gefordert, ihren Führungsstil über Ziele und Ergebnisse zu definieren. Anwesenheit als Leistungsmerkmal ist im New Normal keine Option mehr.

Seit Beginn der Pandemie wurden Führungskräfte daher verstärkt mit einem gezielten Kanon aus wirkungs- und mitarbeiterorientierten Führungsskills in (Online-) Schulungsformaten in ihrem Führungsalltag unterstützt.

EIN BILD FÜR DIE ZUKUNFT

Schon während der ersten Wochen unter veränderten Arbeitsbedingungen in der Krise wurde damit begonnen, die gemachten Erfahrungen als „Lessons Learned" zu dokumentieren. Bereits vor der allgemeinen Diskussion zum New Normal in der Öffentlichkeit erteilte die BSI-Leitung den Auftrag, ein Zielbild zur neuen Normalität zu entwickeln. Motto: „Positive Aspekte der vergangenen Monate mitnehmen, negative Aspekte vermeiden".

In drei Online-Workshops wurde ein erstes Zielbild des New Normal mit Beteiligung aller Abteilungen, der Gremien und der Gleichstellungsbeauftragten skizziert. Der Prozess erfolgte komplett digital, wurde parallel in einem Wiki dokumentiert und war bereits Teil des New Normal.

Im ersten Workshop analysierte die Gruppe die tatsächliche Veränderung: Wie war es vor Corona? Wie ist es jetzt? Dabei wurden insgesamt 43 Themen in den vier Handlungsfeldern identifiziert. Im zweiten Workshop wurden die Veränderung beschrieben und erste Leitsätze für das Zielbild entwickelt. Schließlich wurde im dritten Workshop erarbeitet, welche kritischen Erfolgsfaktoren

und Lösungsansätze noch berücksichtigt werden müssen. Durch die Dokumentation aller Workshop-Ergebnisse im internen Wiki entstand eine Sammlung, die sogenannte „Schatzkiste“, auf die bei der weiteren Gestaltung des New Normal zurückgegriffen werden kann.

VERSCHIEDENE PERSPEKTIVEN FORMEN EIN BILD

Das von der Personalentwicklung gestaltete Format und die Zusammenarbeit in der Gruppe waren bereits Teil einer neuen virtuellen Normalität. Diese Arbeitsweise in den Workshops war höchst effizient und brachte viele Aspekte und Perspektiven in das Zielbild ein. Nur diese Betrachtung machte es möglich, ein ganzheitliches Zielbild zu entwickeln.

Im Nachgang zu den Workshops wurden die Ergebnisse in einem zweiseitigen Papier zum New Normal zusammengefasst und durch die Behördenleitung abgestimmt. Es beschreibt die Ziele einer zukunftsfähigen Arbeitskultur am BSI, die der veränderten Arbeits- und Lebenswelt während und nach der Corona-Pandemie dauerhaft Rechnung tragen soll.

Es ist immer noch zu früh, um alle Veränderungen und ihre Auswirkungen zu erfassen. Daher soll am BSI kontinuierlich an den gesammelten Erfahrungen weiter gelernt werden.

Das Leitbild soll bei der zukünftigen Ausgestaltung und Weiterentwicklung in allen Bereichen des BSI Berücksichtigung finden.

Mit der Umsetzung des Leitbilds werden zukunftsfähige Rahmenbedingungen geschaffen, um nicht nur die Ziele des BSI zu erreichen, sondern auch eine effiziente abteilungs- und hierarchieübergreifende Zusammenarbeit zu etablieren und die Zufriedenheit der Mitarbeitenden durch eine bessere Vereinbarkeit von Beruf, Familie und Leben zu fördern.

Das BSI setzt mit seinem Zielbild des New Normal seinen Weg als zukunftsfähiges Bundesamt, attraktiver Arbeitgeber und als Partner in Staat, Wirtschaft und Gesellschaft weiter fort: New Normal ist für uns ein Katalysator zur Digitalisierung des BSI. Wir möchten Vorreiter für eine moderne Behörde mit digitalen Verwaltungsprozessen sein. Mit verstärkt digitalem Arbeiten leisten wir einen Beitrag zur nachhaltigen Gesellschaft und dem schonendem Umgang mit Ressourcen (bspw. weniger Dienstreisen, Pendelverkehr, Papierverbrauch). ■

Zu den folgenden vier Handlungsfeldern wurden Leitsätze in Wir-Form erarbeitet, um den Zielzustand des New Normal zu beschreiben:

1. **Arbeitsorganisation (Wie arbeiten wir?):** z.B. hybrides Arbeiten; Flexibilisierung von Ort und Zeit
2. **Arbeitsmittel (Womit arbeiten wir?):** z.B. an die Herausforderungen angepasste Hard- und Software; ergonomische Ausstattung
3. **Führung und Kooperation (Wie führen wir?):** z.B. Führen und Arbeiten auf Distanz; ist eine individuellere Führung notwendig?
4. **Kompetenzen (Was müssen wir wissen und können?):** z.B. digitale Kompetenzen; Erhöhung der Kommunikationskompetenz; Wissensmanagement

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 personenbezogenen 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. die 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 | www.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:	November 2020
Texte und Redaktion:	Nora Basting und Mark Schulz, Bundesamt für Sicherheit in der Informationstechnik (BSI); FAKTOR 3 AG
Konzept und Gestaltung:	FAKTOR 3 AG Kattunbleiche 35 22041 Hamburg www.faktor3.de
Druck:	Appel und Klinger Druck & Medien GmbH Bahnhofstraße 3 96277 Schneckenlohe Internet: www.ak-druck-medien.de
Artikelnummer:	BSI-Mag 20/712-1
Bildnachweise:	Titel: GettyImages © shapecharge; S. 4, BSI, GettyImages © Dong Wenjie; S. 10, FAKTOR 3 AG - Composing; S. 12, Screenshot-Composing BSI/FAKTOR 3 AG; S. 14, Bundesregierung Corona Warn App/FAKTOR 3 AG - Composing; S. 18, Shutterstock © Fit Ztudio; S. 21, © PopTika; S. 22, Shutterstock © Prokopeva Irina; S. 25, Hochschule des Bundes für Öffentliche Verwaltung; S. 26, BSI; S. 29, Thomas Popp © Matthias Rietschel; S. 30, GettyImages © Henrik Sorensen; S. 32, BSI, FAKTOR 3 AG - Composing; S. 36, BSI, FAKTOR 3 AG - Composing; S. 38-39, BSI; S. 40-41, BSI, Bundesministerium des Innern, für Bau und Heimat, Pexels © Errin Casano, Pexels © Pixabay, Pexels © worldspectrum, Pexels © alphatradezone, GettyImages © Dong Wenjie, Bundes-Verbraucherzentrale, Pexels © sarayut; S. 42, GettyImages © Kathleen Finlay; S. 43, GettyImages © Busakorn Pongparnit; S. 44, GettyImages © Artur Debat; S. 46, GettyImages © sorbetto; S. 49, Freepik © Stories; S. 52, GettyImages © Vectorios2016; S. 54, GettyImages © Westend61; S. 57, Gert Baumbach - vzbv.; S. 58, GettyImages © Hugo Donabella Mattos / EyeEm; S. 60, GettyImages © Gandee Vasan;

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