Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

BSI-Magazin 2021/02

Mit Sicherheit

Im Blickpunkt: **Online-Wahlen**

Cyber-Sicherheit

Zertifiziert in die Quanten-zukunft: Für sichere Quantum Key Distribution

IT-Sicherheit in der Praxis

Das IT-Sicherheitskennzeichen: Transparenz für alle schaffen

Digitale Gesellschaft

Crashtest für Cyber-Sicherheit: Wie IT-Sicherheit die Mobilitätswende voranbringt

EDITORIAL

Erste Wahl: IT-Sicherheit

Das zweite Halbjahr 2021 stand weiterhin im Zeichen der Corona-Pandemie, die trotz Fortschritten bei ihrer Bekämpfung den Alltag vieler Menschen geprägt hat. Wir haben an Events virtuell statt vor Ort teilgenommen, uns zeitweise im Homeoffice und im virtuellen Schulunterricht eingerichtet, Videokonferenzen und digitale Familientreffen abgehalten.

Mit Blick auf die Informationssicherheit lassen sich die letzten Monate vor diesem Hintergrund kurz zusammenfassen: Nie war Digitalisierung präsenter. Und sie wird weiter voranschreiten – in Staat, Wirtschaft und Gesellschaft. Mit all ihren Vorzügen und den damit verbundenen großen und wachsenden Aufgaben für die Cyber-Sicherheit.

Deshalb war die Verabschiedung des IT-Sicherheitsgesetzes 2.0 ein wichtiger Meilenstein, nicht nur für das BSI, sondern für die Cyber– und Informationssicherheit in Deutschland insgesamt. Denn der Gesetzgeber hat mit diesem wichtigen Upgrade entscheidende Voraussetzungen für eine sichere Digitalisierung geschaffen. Diese kann nur gelingen, wenn Informationssicherheit von Anfang an mitgedacht wird. Sie darf nicht länger als Bremsklotz missverstanden werden, sondern ist vielmehr eine Investition in die Zukunft. Uns allen muss klar sein, dass Informationssicherheit die Voraussetzung für eine erfolgreiche Digitalisierung ist.

Dies zeigt sich auch bei Wahlen und Abstimmungsprozessen. Durch die Einschränkungen der Corona-Pandemie ist der Bedarf an digitalen Lösungen rasant gestiegen. Präsenzveranstaltungen wie Vereins- oder Aktionärsversammlungen, Meetings von Unternehmen oder Plenar- und Gremiensitzungen von Parlamenten oder Parteien konnten über Monate hinweg nicht oder nur sehr eingeschränkt stattfinden. Im Sonderteil „Online-Wahlen“ beleuchten wir unterschiedliche Aspekte und Handlungsempfehlungen für eine sichere Durchführung von Abstimmungsprozessen im digitalen Raum.

Darüber hinaus informieren wir Sie in dieser Ausgabe unter anderem über Sicherheitsanforderungen im Post-Quanten-Zeitalter, das neue IT-Sicherheitskennzeichen und die Bedeutung von IT-Sicherheit für die Automobilbranche.

Ich wünsche Ihnen Gesundheit und eine interessante Lektüre.
Ihr

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik

INHALT

AKTUELLES

Verbraucherschutz wird digital

Neues Gremium: Der Beirat Digitaler Verbraucherschutz

Um die Cyber-Sicherheit im digitalen Alltag von Verbraucherinnen und Verbrauchern zielgruppenorientiert und praxistauglich durch Entwicklung und Umsetzung geeigneter Maßnahmen zu erhöhen, wird das BSI seit Juni 2021 durch ein unabhängiges Expertengremium, den Beirat Digitaler Verbraucherschutz, unterstützt. Dafür wählt dieser sich jährlich ein Fokusthema, zu dem Handlungsempfehlungen erarbeitet werden. Der Beirat setzt sich aus zehn Mitgliedern zusammen, welche die Verbraucherperspektive [illegible] der Zivilgesellschaft, der Verbraucherwissenschaften, der Informatik und der Wirtschaft einbringen. Zur Sprecherin des Beirats wurde Prof. Dr. Martina Angela Sasse (Lehrstuhl für Human-Centred Security, Ruhr-Universität Bochum) gewählt. Weitere Informationen zum neuen Gremium, dessen Mitgliedern und Aufgabenstellungen unter www.bsi.bund.de und bei der Geschäftsstelle des Beirats: beiratdigitalerverbraucherschutz@bsi.bund.de

Informationssicherheit im Wandel

Migration zu Post-Quanten-Kryptografie

Das BSI hat einen wichtigen Schritt in Richtung „Migration zu Post-Quanten Kryptografie“ gemacht. Der SINA Communicator H ist das erste GEHEIM-zugelassene VS-IT-Produkt in Deutschland, in dem erfolgreich eine quantencomputerresistente Schlüsseleinigung implementiert wurde. Die Einsatzfähigkeit des Geräts wurde durch eine Telefonkonferenz auf Leitungsebene zwischen den Ressorts BMI, AA, BMVg, BKAmt und dem BSI erfolgreich demonstriert.

Der SINA Communicator H ermöglicht sowohl GEHEIM- als auch VS-NfD-zugelassene Telefonate und Telefonkonferenzen. Er wird sich gleichzeitig in VS-NfD-Netzwerke unterschiedlicher Mandantinnen und Mandanten einbinden können und diese Netzwerke sicher voneinander trennen. Neben der Unterstützung von IPsec für Gespräche und zur Einbindung in bestehende SINA-Infrastrukturen können GEHEIM-Gespräche bereits mittels SCIP-Protokoll auch Ende-zu-Ende gesichert werden. Zukünftig wird das Gerät z.B. als 64kbit/s SATCOM Telefon, als Videotelefon oder als Thin-Client-Arbeitsplatz mit Monitor, Maus und Tastatur vielfältige Nutzungsszenarien unterstützen. Die ersten Geräte wurden Anfang September an die Bundesverwaltung ausgeliefert.

Als weiteres VS-IT-Produkt mit quantencomputerresistenter Kryptografie wird zukünftig das R&S®ELCRODAT 7-FN der Firma Rohde & Schwarz SIT erwartet.

Weitere Informationen:

https://www.bsi.bund.de/PQ-Migration

Ein starker Partner

Bundesweit erste Kooperationsvereinbarung: Niedersachsen und BSI

Am 17. November 2021 haben Präsident des BSI, Arne Schönbohm, und der Minister für Inneres und Sport Niedersachsen, Boris Pistorius, in Hannover die erste Kooperationsvereinbarung zwischen einem Bundesland und dem BSI im Einsatz gegen Cyber-Kriminalität unterschrieben.

„Das Informationssicherheitsniveau in Deutschland zu stärken und auf dem höchst möglichen Niveau zu halten, um Cyber-Bedrohung frühestmöglich zu erkennen und abzuwehren, kann nur im Team gelingen. Das Land Niedersachsen ist hier von Beginn an ein starker Partner“, so Arne Schönbohm.

Siebzehn Kooperationsfelder regeln nun die seit 2018 bestehende Zusammenarbeit verbindlich. Neben der gegenseitigen Unterstützung bei herausgehobenen Cyber-Sicherheitsvorfällen zählen dazu Hospitationen und die gemeinsame Arbeit bei Standards in der Informationssicherheit.

Minister Boris Pistorius unterstrich die Bedeutung dieser Vereinbarung aus Sicht Niedersachsens: „Bedrohungen aus dem Cyber-Raum machen weder an Landes- noch an internationalen Grenzen halt. Mit dieser Vereinbarung werden wir mit dem BSI noch enger zusammenrücken, uns stetig besser vernetzen und mehr voneinander lernen!“

Läuft beim BSI

Drei-Standorte und die ganze Welt!

Corona war und ist für alle herausfordernd – sowohl um in Bewegung als auch als Kolleginnen und Kollegen beieinander zu bleiben. Aus diesem Grund starteten im Sommer 2021 – unter der Schirmherrschaft und der aktiven Beteiligung des Abteilungsleiters Jörg Pieper – 35 Teams in eine ehrgeizige Challenge. Bei BSI@walk – der Drei-Standorte-Challenge, fanden sich Kolleginnen und Kollegen abteilungsübergreifend zusammen, um den jeweils anderen BSI-Standorten einen Besuch abzustatten. Natürlich aufgrund der Pandemie nicht persönlich, aber mit genügend Schritten, so dass Bonn, Saarbrücken und Freital erlaufen wurden. Gut 1300 Kilometer bzw. rund 2 Millionen Schritte legte jedes Team zurück. Motivation gab es zusätzlich per Chat.

Einem fitten Frauenteam gelang es schließlich, als erstes wieder am Ausgangsort anzukommen. Aber natürlich ist das Gewinnen nicht alles – der Spaß an der Bewegung stand im Vordergrund! Und gemeinsam geht noch mehr: Insgesamt haben die Mitarbeitenden in acht Wochen 43.388 Kilometer zurückgelegt und sind damit sogar einmal um den Äquator gelaufen!

Bei der Siegerehrung waren sich die Teilnehmerinnen und Teilnehmer einig: Auch in Zeiten der Pandemie haben wir es geschafft, in Bewegung und beieinander zu bleiben.

CYBER-SICHERHEIT

Die Beschleunigte Sicherheitszertifizierung (BSZ)

Für mehr Vertrauen in IT-Produkte

von Dr. Helge Kreutzmann, Referat Anerkennung und Zertifizierung von Stellen und Personen und Dr. Kai Redeker, Referat Zertifizierung von Netzwerkkomponenten und Beschleunigte Sicherheitszertifizierung

Bei Produkten, die Informationstechnik verwenden, zeichnen sich in den letzten Jahren zwei zentrale Trends ab: Zum einen wird das Tempo der durch die Digitalisierung bedingten Veränderungen verschiedenster Lebensbereiche immer höher, zum anderen haben aber immer neue Schwachstellen immer massivere Auswirkungen auf unser Leben und unsere Wirtschaftsgüter, da die Produkte immer tiefer in unser (Geschäfts-) Leben integriert und gleichzeitig weltweit vernetzt sind.

Um Aussagen über die Vertrauenswürdigkeit von IT-Produkten zu erlangen, bietet das BSI schon seit mehr als 30 Jahren die Zertifizierung von Produkten an. Zusammen mit der französischen Partnerbehörde ANSSI (Agence nationale de la sécurité des systèmes d'information) ist das BSI mittlerweile inoffizieller Weltmeister bei der Zertifizierung von Produkten für staatliche Anwendungen oder sehr hohe Sicherheitsanforderungen. Was aber in dieser Zeit klar fehlte, war ein Angebot für breitere Marktsegmente, die durch die bisher ausschließlich hierfür genutzten Common Criteria nicht erreicht wurden.

Aufwand für den Hersteller reduzieren

Inspiriert von Ideen der französischen CSPN-Zertifizierung (Certification de Sécurité de Premier Niveau) hat sich das BSI daher die Frage gestellt,

wie breitere Herstellerkreise zur Zertifizierung von Produkten für z.B. einsatzkritische Bereiche bewegt werden können. Klar war, dass das Zertifikat weiterhin die vom BSI bekannte hohe (Sicherheits-)Aussage treffen können muss. Eine zentrale Zielstellung war jedoch auch, die Anforderungen an den Hersteller zu reduzieren und sich bei der Prüfung auf die Aspekte zu fokussieren, die den größten Anteil zur Sicherheitsaussage beitragen. Gleichzeitig muss aber auch der dynamischen Weiterentwicklung und dem Bekanntwerden neuer Schwachstellen (und den zugehörigen Patches) in der Informationstechnik Rechnung getragen werden. So entstand die BSZ.

Um den Aufwand der Hersteller (einschließlich des finanziellen) zu reduzieren, werden keine umfangreichen spezialisierten oder formalen Informationen zum Design verlangt, wie dies bei der Common Criteria-Zertifizierung regelmäßig der Fall ist. Stattdessen erfolgt eine Prüfung über die Schnittstellen mit nur minimalen Informationen über den inneren Aufbau des Produktes. Gleichzeitig wird das Vertrauen in das Produkt nicht mehr über abstrakte Stufen definiert, sondern es wird von einem erfahrenen Angreifenden mit begrenztem Zeitbudget ausgegangen. Dazu wird mit einem am Verfahrensanfang ermittelten und dann festgelegten Zeitumfang geprüft, der insgesamt im Bereich von 15 bis maximal 60 (in der Regel 35) Personentagen liegt. Damit sind zudem Durchlaufzeiten von drei Monaten von der Eröffnung des Verfahrens bis zur Zertifikatsvergabe realistisch, was für das Time-to-Market sehr hilfreich ist.

Gleichzeitig wird die dynamische Entwicklung nicht vergessen. Erfahrungsgemäß werden Sicherheitsaktualisierungen (Updates) benötigt. Daher müssen BSZ-zertifizierte Produkte einen Aktualisierungsmechanismus bereitstellen. Dieser ist Teil der Prüfung. Zudem werden Hersteller für die Laufzeit des Zertifikats verpflichtet, über diesen Mechanismus bei Bedarf Updates auszuliefern. Und falls vom Unternehmen gewünscht, können solche gezielten Updates auch mit geringem Zeitaufwand geprüft und zertifiziert werden.

Erster Geltungsbereich: Netzwerkkomponenten

Nach einer Machbarkeitsstudie und mehreren Pilotverfahren ist das BSZ-Programm im Oktober mit dem ersten Geltungsbereich Netzwerkkomponenten (z. B. Router und industrielle Steuerungssysteme), gestartet. In der Zukunft werden sukzessive weitere Geltungsbereiche erschlossen.

Der Ablauf eines BSZ-Verfahrens ist wie folgt: Zunächst bereitet der Antragsteller, normalerweise ein Hersteller oder Vertreiber eines Produkts, die wenigen benötigten Dokumente vor. Zentral sind hier die Sicherheitsvorgaben, ein relativ kurzes Dokument von ca. zehn Seiten, in dem Einsatzumgebung und Sicherheitsfunktionen des Produkts beschrieben werden. Außerdem muss der Antragsteller eine vom BSI anerkannte Prüfstelle beauftragen, das Produkt im Verfahren zu prüfen. Nun können der Antrag und alle zugehörigen Dokumente bei der Zertifizierungsstelle des BSI eingereicht werden.

Im nächsten Schritt prüfen sowohl die Zertifizierungsstelle als auch die Prüfstelle die Dokumente, um festzustellen, ob diese und das Produkt die Voraussetzungen für ein BSZ-Verfahren erfüllen und eine Evaluation möglich ist. Ist dies der Fall, wird eine Auftaktbesprechung vereinbart. Hier wird die Prüfung des Produkts diskutiert, der Prüfaufwand inklusive fixer Zeitplanung festgelegt und es werden alle offenen Punkte geklärt. Nun beginnt die Prüfung und es sind keine Änderungen an Produkt oder Dokumentation mehr möglich. Die Prüfstelle dokumentiert die durchgeführten Tests, Ergebnisse sowie Bewertungen und präsentiert diese im Abschlussinterview der Zertifizierungsstelle. Basierend darauf fällt die Zertifizierungsstelle die Entscheidung, ob das Zertifikat erteilt wird.

Erst dann wird der Antragsteller über die Prüfungsergebnisse und die Entscheidung informiert. Im Falle einer positiven Entscheidung erhält der Antragsteller das Zertifikat zur Verwendung. Ein BSZ-Zertifikat ist in der Regel zwei Jahre lang gültig. Bei negativem Ausgang ist ein neues, ggf. verkürztes Verfahren möglich. Gleichzeitig hat der Antragssteller eine gute Übersicht über die gefundenen Probleme. ■

Weitere Informationen:

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

Zertifiziert in die Quantenzukunft

Für sichere Quantum Key Distribution

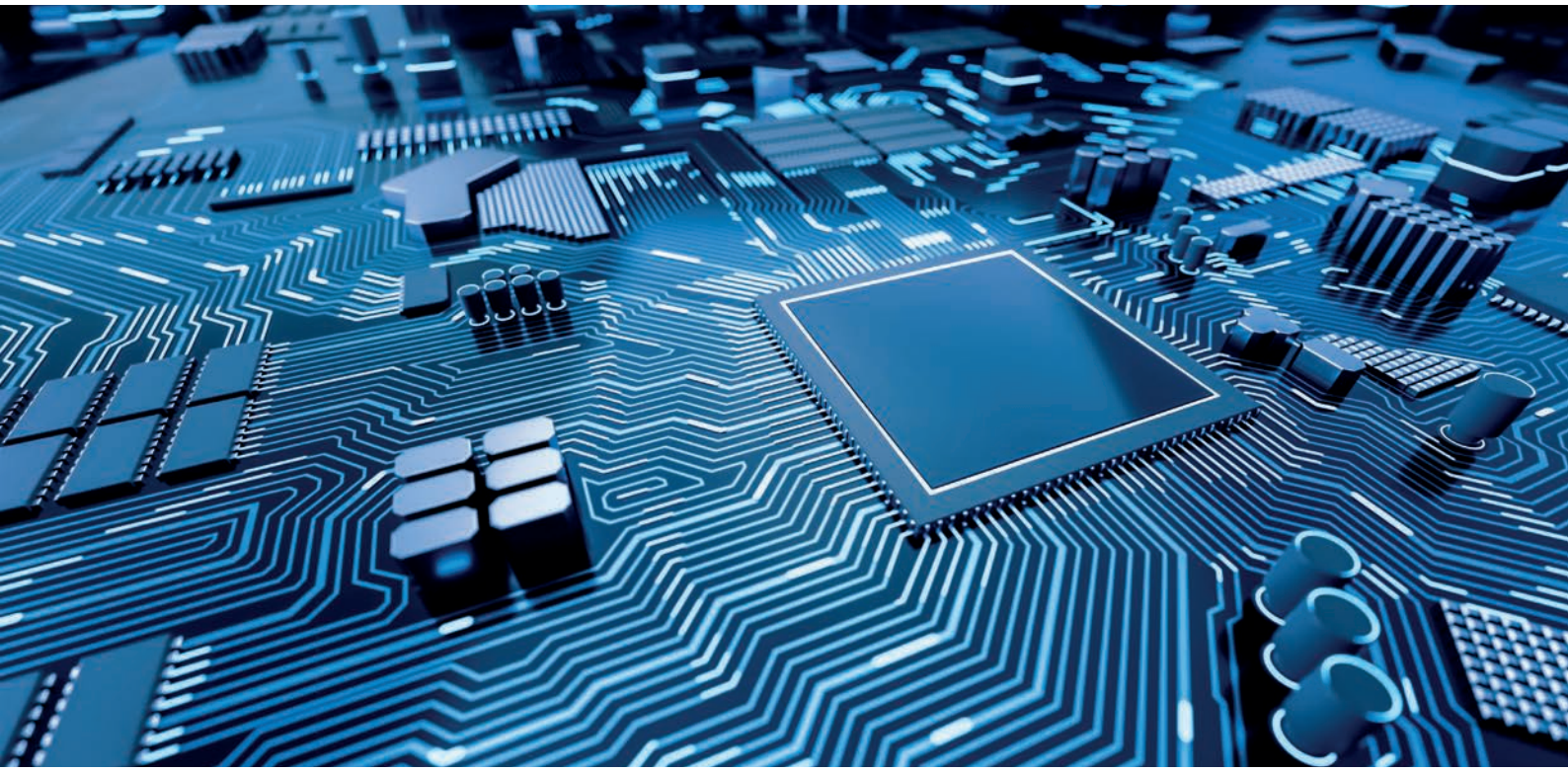
von Dr. Tobias Hemmert, Dr. Manfred Lochter, Stephanie Reinhardt, Referat Vorgaben an und Entwicklung von Kryptoverfahren und Dirk Fischer, Referat Zertifizierung Hardware

Weltweit wird intensiv an Quantencomputern geforscht, die die heute verwendete Public-Key-Kryptografie gefährden würden. Als Lösungen für quantencomputerresistente Schlüsseleinigungsverfahren werden die Post-Quanten-Kryptografie und die Quantum Key Distribution (QKD) vorgeschlagen. Um einer sicheren Nutzung von QKD den Weg zu ebnen, hat das BSI ein erstes Protection Profile (PP) für QKD-Geräte in Auftrag gegeben.

Die heute eingesetzte Public Key-Kryptografie ist von der fortschreitenden Entwicklung von Quantencomputern bedroht. Die Verwirklichung skalierbarer Quantencomputer ist zurzeit Gegenstand intensiver Forschung; nicht nur von großen Unternehmen wie IBM und Google, sondern auch in Deutschland, wo die Bundesregierung immense Mittel bereitstellt. Deshalb ist es wichtig, bereits vorausschauend zu kryptografischen Verfahren zu migrieren, die auch gegen Angriffe mit Hilfe von Quantencomputern resistent sind. Das BSI arbeitet für den Bereich der Hochsicherheit unter der Arbeitshypothese, dass es Anfang der 2030er Jahre Quantencomputer geben wird, die die heute verwendete Public-Key-Kryptografie gefährden. Diese Aussage ist nicht als Prognose zur Verfügbarkeit von Quantencomputern zu verstehen, sondern stellt einen Richtwert für die Risikobewertung dar.

Für Schlüsseleinigungsverfahren haben sich zwei grundsätzlich verschiedene Ansätze herausgebildet: zum einen die Post-Quanten-Kryptografie und zum anderen die Quantum Key Distribution (QKD). Die Sicherheit der Post-Quanten-Kryptografie beruht auf der angenommenen Schwierigkeit bestimmter mathematischer Probleme, dagegen basiert die Sicherheit von QKD auf rein quantenmechanischen – und somit physikalischen – Prinzipien. Zur Nutzung der geeigneten quantenmechanischen Effekte wird spezialisierte Hardware eingesetzt, wie beispielsweise Photonenquellen und -detektoren. Das BSI hat bereits den Wechsel zur Post-Quanten-Kryptografie eingeleitet und betrachtet QKD als mögliche zukünftige Ergänzung zu Post-Quanten-Schlüsseleinigungsverfahren. Dies betrifft momentan allerdings eher spezielle Anwendungsfelder, da die technischen Voraussetzungen für QKD noch stark limitierend sind und noch keine zertifizierten Produkte zur Verfügung stehen.

Es gibt weltweit bereits eine Vielzahl an Aktivitäten zur Einführung von QKD, zum Beispiel die europäische Initiative EuroQCI (The European Quantum Communication Infrastructure). Diese verfolgt das Ziel, innerhalb der nächsten Jahre eine europäische Quantenkommunikationsinfrastruktur aufzubauen. Im Juli 2021 ist Irland als der letzte Mitgliedsstaat der EU EuroQCI beigetreten. Das so entstehende Netzwerk soll mittels QKD vereinbarte Schlüssel bereitstellen, die insbesondere für hochsichere Anwendungen verwendet werden können. Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekt QuNET (vgl. Kasten zum Demonstrator) ist gewissermaßen der deutsche Anteil an EuroQCI. Neben diesen beiden Projekten, EuroQCI und QuNET, gibt es noch zahlreiche weitere deutsche Initiativen. Angesichts der großen Investitionen in QKD und internationalen, weitreichenden Plänen zum Aufbau von QKD-Netzen beschäftigt sich auch das BSI bereits jetzt vorausschauend mit der Sicherheitsbewertung von QKD. Das Ziel: „Security by Design“.



Das Projekt: Protection Profile für Quantum Key Distribution

Mit der Einführung einer neuen Technologie wie QKD stellt sich natürlich die Frage nach der Sicherheitsbewertung der entsprechenden IT-Sicherheitsprodukte. Ein international anerkannter Standard zur Sicherheitsevaluierung sind die Common Criteria (CC). Als ersten Schritt zur Entwicklung von Evaluierungskriterien hat das BSI die Prüfstelle der Telekom Security 2020 mit der Erstellung eines Protection Profiles (PP) für QKD beauftragt. Ein solches PP stellt in gewisser Weise eine Blaupause dar, die Herstellern, die ein bestimmtes Sicherheitsniveau anstreben, dabei hilft, ein produktspezifisches Security Target zu erstellen. Das beauftragte PP beschränkt sich zunächst auf sogenannte Prepare & Measure-Protokolle und Punkt-zu-Punkt-Verbindungen. Netzwerkaspekte werden also nicht berücksichtigt. Um möglichst frühzeitig die wissenschaftliche Community und Hersteller einzubinden sowie ein international anerkanntes PP zu erstellen, erfolgt die Erarbeitung des PPs in Zusammenarbeit mit einer Fachuntergruppe des European Telecommunications Standards Institute (ETSI) und soll schließlich zu einem ETSI-Standard führen. Eine abschließende Zertifizierung des PPs ist als nächster Schritt geplant. Ein zertifiziertes PP kann dann – mit geeigneten Ergänzungen – auch als Basis eines VS-Zulassungsverfahrens verwendet werden. Bei Zulassungen können insbesondere Anforderungen an die Herkunft von Produkten hinzukommen.

Ebenso soll durch das PP die Entwicklung von Produkten erleichtert werden, die dem Ziel der EU einer „certified secure end-to-end quantum communication infrastructure (QCI) composed of space-based and terrestrial-based solutions, enabling information and data to be transmitted and stored ultra-securely“ (EU19) entsprechen. Daher ist angestrebt, das Protection Profile auf dem Sicherheitsniveau EAL4+ (augmentiert um AVA_VAN.5 und ALC_DVS.2) zu verankern.

Das PP soll so offen gestaltet werden, dass national regulierte oder definierte Aspekte auch weiterhin der Entscheidung der jeweiligen Länder obliegen können. In Deutschland wären dies etwa Aspekte der Kryptografie und der Zufallszahlenerzeugung (TR-02102 und AIS 20/31).

Ausblick

Mit der anstehenden Finalisierung des BSI/ETSI-Protection Profiles ist der Weg zu einer umfassenden QKD-Infrastruktur jedoch noch nicht zu Ende beschritten. Perspektivisch hinzukommen werden verschiedene andere QKD-Varianten, zum Beispiel verschränkungsbasierte QKD-Protokolle. Diese Protokolle sollen insbesondere bei der Satellitenkommunikation eingesetzt werden. Daneben sind Quantennetzwerke und die Einbindung traditioneller Kryptografie wichtig. Mit fortschreitender Entwicklung der Technologie ist durchaus auch denkbar, weitere PPs zu entwickeln.

Neben dem Ausblick auf weitere Versionen des Protection Profiles wird durch die Tätigkeiten des BSI auch der Grundstein zur Schaffung eines erforderlichen europäischen Zertifizierungsökosystems gelegt. Im europäischen Rahmen wünschenswert ist die Bildung einer Technical Domain für QKD, in welcher die für eine

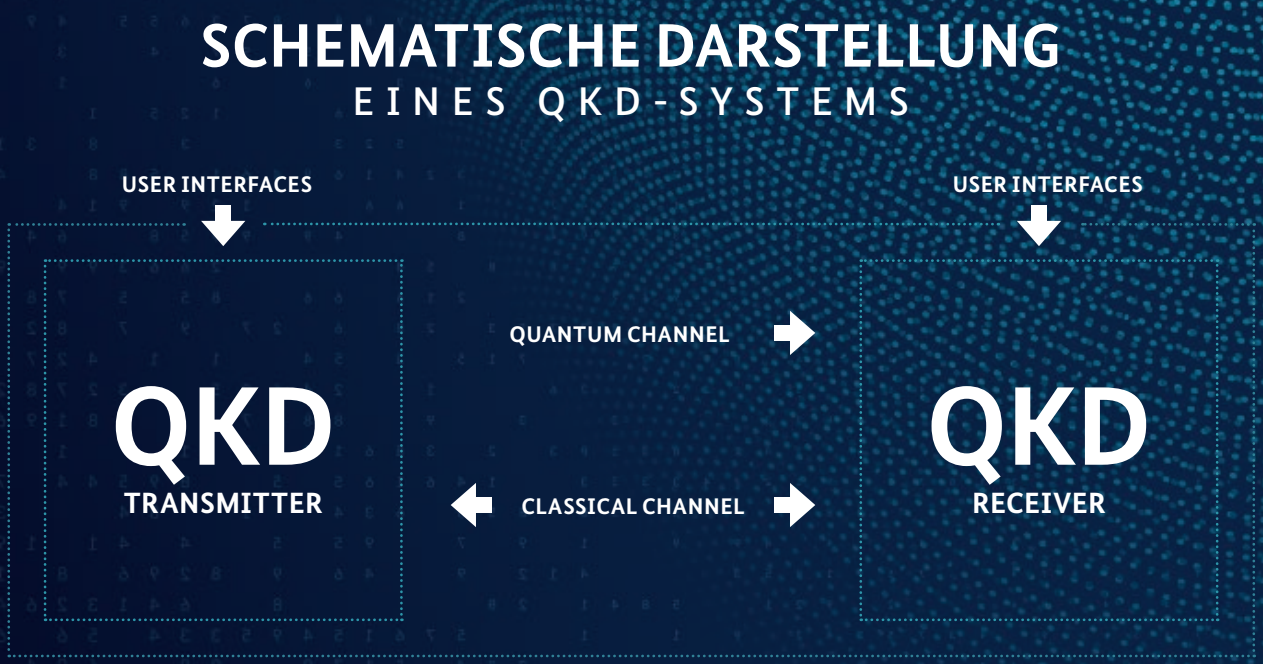


Abbildung: Schematische Darstellung eines QKD-Systems

schnelle und erfolgreiche Zertifizierung erforderlichen und international harmonisierten Begleitdokumente zielgerichtet erstellt werden können. Eine Technical Domain kann aus gemeinsamen Arbeitsgruppen von Zertifizierungsbehörden, Prüfstellen und Industrie bestehen – also allen an einem Produktzertifizierungsverfahren beteiligten Akteuren. Die noch zu erstellenden Begleitdokumente umfassen beispielsweise die Ausdefinition von Prüfmethodologien, einheitliche Rahmen zur Schwachstellenbewertung, technische und fachliche Vorgaben zur Expertise von Prüfstellen und intensive Beschäftigung mit technologiespezifischen Angriffsmethoden, wie beispielsweise Seitenkanälen.

Die Standardisierung von QKD-Protokollen ist ebenfalls noch ein aktives Feld. Idealerweise gehört zu einem QKD-Standard auch ein Sicherheitsbeweis mit einer quantitativen Sicherheitsaussage. Als Cyber-Sicherheitsbehörde des Bundes arbeitet das BSI daher auch in diesem Themengebiet gestaltend mit, um eine sichere Implementierung von QKD zu gewährleisten. ■

Weitere Informationen:

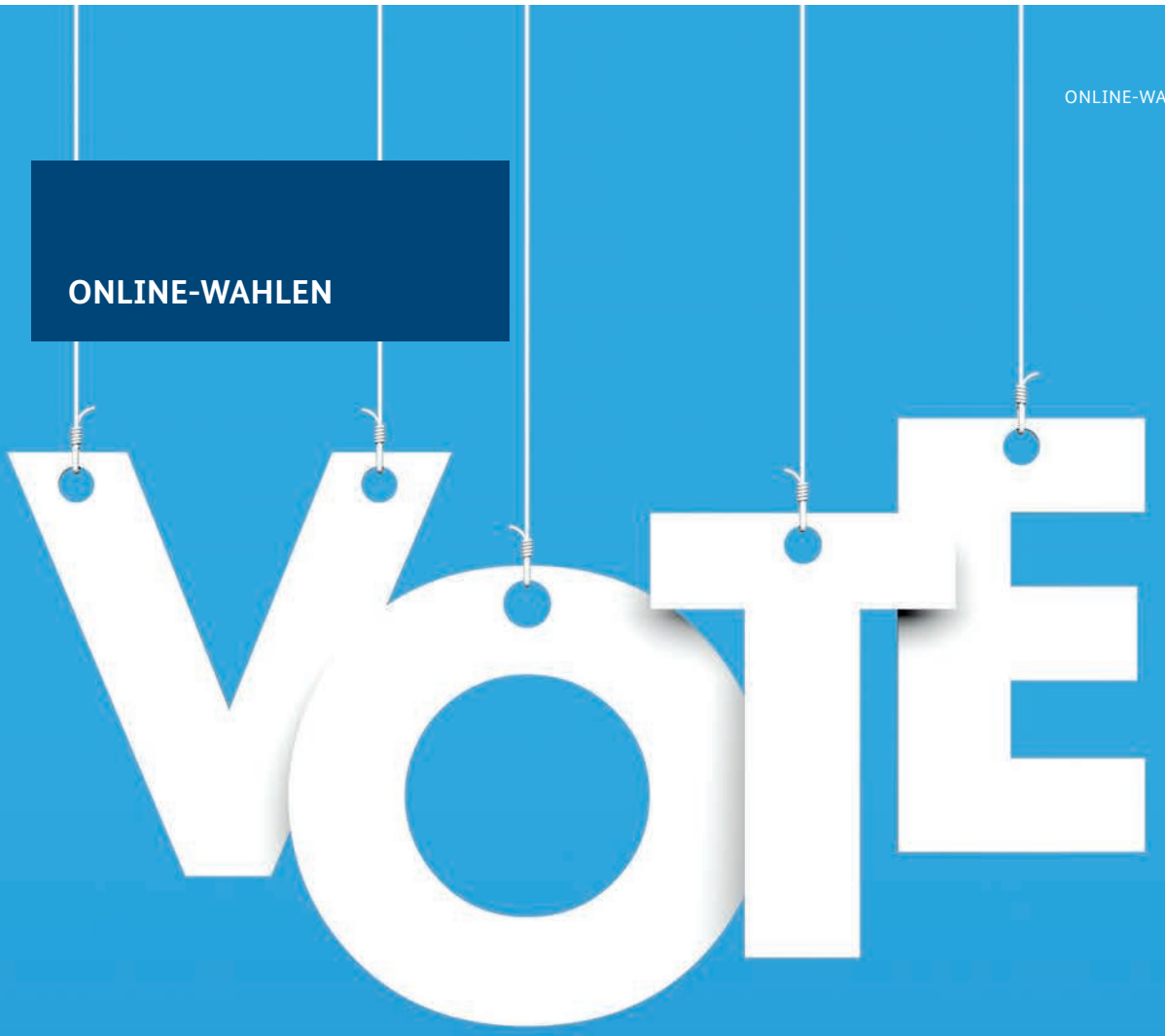
https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

www.bsi.bund.de/Quanten

Dr. Martin Schell, Leiter des Fraunhofer HHI

QuNET-Demonstrator
Am 10. August 2021 startete Frau Ministerin Karliczek die erste quantengesicherte Videokonferenz zwischen zwei Bundesbehörden, dem BMBF und dem BSI. Der Demonstrator entstand im Rahmen der vor zwei Jahren gestarteten QuNET-Initiative, in der die Fraunhofer-Gesellschaft, die Max-Planck-Gesellschaft und das Deutsche Zentrum für Luft- und Raumfahrt (DLR) an der Basis für ein Pilotnetz für die Quantenkommunikation forschen. Das BSI ist im Beirat von QuNET vertreten und berät insbsondere zu Sicherheitsfragen. Bei der Demonstration teilten alle Beteiligten das Ziel eines Quanten-Ökosystems, in dem zertifizierte und zugelassene Produkte vertrauenswürdige Kommunikation sicherstellen.

ONLINE-WAHLEN



Sonderteil Online-Wahlen

Die Corona-Pandemie hat dazu geführt, dass Veranstaltungen wie Vereins- oder Aktionärsversammlungen, Meetings von Unternehmen oder Plenar- und Gremiensitzungen von Parlamenten und Parteien über Monate hinweg nicht oder nur sehr eingeschränkt stattfinden konnten. Ein rasanter Anstieg beim Bedarf an digitalen Lösungen für virtuelle Versammlungen, Wahlen und Abstimmungen war die Folge.

Der Sonderteil „Online-Wahlen“ beleuchtet, wie solche Formate vor dem Hintergrund der wachsenden Bedrohungslage im Cyber-Raum möglichst sicher durchgeführt werden können. Welche Bedrohungen für Online-Wahlen lassen sich beobachten? Welche technischen und organisatorischen Maßnahmen können Schutz bieten? Wie kann auch bei Online-Wahlen die Einhaltung der Wahlrechtsgrundsätze sichergestellt werden?

Das BSI hat aus seinen verschiedenen Arbeitsfeldern heraus bereits eine Vielzahl von konkreten Handlungsempfehlungen zum Thema Online-Wahlen und virtuellen Abstimmungen erarbeitet. Technische Richtlinien und Schutzprofile beispielsweise geben Leitlinien für die Absicherung vor. Bei der Erarbeitung dieser Leitlinien hat das BSI im Rahmen des Modellprojektes Online-Sozialwahlen 2023 (S.12) Grundlagenarbeit geleistet.

Entsprechende Zertifizierungen sind ein wichtiges Mittel, um Mindeststandards für die Sicherheit von Online-Wahlen zu setzen (S. 14 und S. 20). Auch der IT-Grundschutz bietet grundlegende Hilfestellung bei der Gestaltung einer Online-Wahl (S.22). Die Projektgruppe ViVA (Virtuelle Versammlungen und Abstimmungen, S. 24) stellt weitere praxisnahe Tipps, Leitfragen und Empfehlungen zur Verfügung.

Welche kryptografischen Werkzeuge dabei helfen, Abstimmungsprozesse im digitalen Raum sicher zu gestalten, beleuchtet der Sonderteil ab Seite 16. Auch erste Stimmen aus der Praxis von Unternehmen und Parteien gibt es bereits, dazu mehr auf Seite 26.

Digitalisierung von Online-Wahlen

Das Modellprojekt Online-Sozialwahlen 2023

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

Mit der Technischen Richtlinie TR-03162 definiert das BSI IT-sicherheitstechnische Anforderungen an die Durchführung einer Online-Wahl und schafft somit eine wesentliche Grundlage für die sichere Digitalisierung der Sozialversicherungswahlen 2023. Einige dieser Vorgaben können auf die Digitalisierung anderer Wahlen übertragen werden.

Die Online-Sozialwahlen 2023

Im Rahmen eines Modellprojektes wird den Krankenkassen bei den Sozialversicherungswahlen 2023 neben der herkömmlichen Stimmabgabe per Briefwahl fakultativ die Möglichkeit eröffnet, Online-Wahlen durchzuführen. Mit der Technischen Richtlinie TR-03162 „IT-sicherheitstechnische Anforderungen zur Durchführung einer Online-Wahl im Rahmen des Modellprojekts nach § 194a Fünftes Buch Sozialgesetzbuch (Online-Wahl)“ macht das BSI Vorgaben für die Informationssicherheit und schafft somit eine wesentliche Grundlage für die sichere Digitalisierung der Sozialversicherungswahlen 2023.

Anwendung der Wahlrechtsgrundsätze

Werden Wahlen digitalisiert, spielt neben den rechtlichen Voraussetzungen, die erfüllt sein müssen, die Umsetzung der Wahlrechtsgrundsätze für alle Wahlen eine wichtige Rolle. Die Digitalisierung kann dabei nicht jedem Wahlrechtsgrundsatz auf dieselbe Weise gerecht werden. Die größte Herausforderung bei einer Online-Wahl ist, die Anforderungen der Wahlrechtsgrundsätze „Geheim und Öffentlich“ in gleichem Maße hinreichend zu erfüllen. Insbesondere seit einem Urteil des Bundesverfassungsgerichtes ist die Möglichkeit der Wählerinnen und Wähler, nachvollziehen zu können, ob die Online-Stimme wie angegeben in der (elektronischen) Wahlurne gespeichert wurde, nicht mehr außer Acht zu lassen. Dies bedeutet, dass auf der einen Seite die Stimmabgabe so geschützt werden muss, dass eine hohe Sicherheit in Bezug auf die Wahrung des Wahlgeheimnisses erreicht wird. Auf der anderen Seite muss trotzdem insgesamt ein ausreichendes Maß an Transparenz über das Wahlgeschehen und eine weitgehende Nachvollziehbarkeit der wesentlichen Schritte der Wahlhandlung, der Ermittlung des Wahlergebnisses und des Wahlergebnisses selbst für die Öffentlichkeit gewährleistet werden *(siehe Artikel auf S. 16)*.

Für die Digitalisierung einer Wahl spielt daher auch die bisherige Gewichtung der Wahlgrundsätze eine Rolle. Ziel sollte immer sein, den Wahlrechtsgrundsätzen so gut wie möglich gerecht zu werden. Zur Nachvollziehbarkeit dieser Entscheidungen sollte dokumentiert werden, wenn ein Wahlrechtsgrundsatz, beispielsweise aufgrund der Umsetzung eines anderen Wahlrechtsgrundsatzes und/oder zur Erhöhung der Manipulationssicherheit der Wahl, nur in geringerem Maße umgesetzt werden kann.

IT-sicherheitstechnische Anforderungen zur Absicherung der Wahl

Zur Erfüllung der Wahlrechtsgrundsätze und zum Erhalt eines validen Wahlergebnisses spielt die Sicherheit vermutlich die wichtigste Rolle. Online-Wahlen beinhalten die gleichen sensiblen Informationen wie analoge

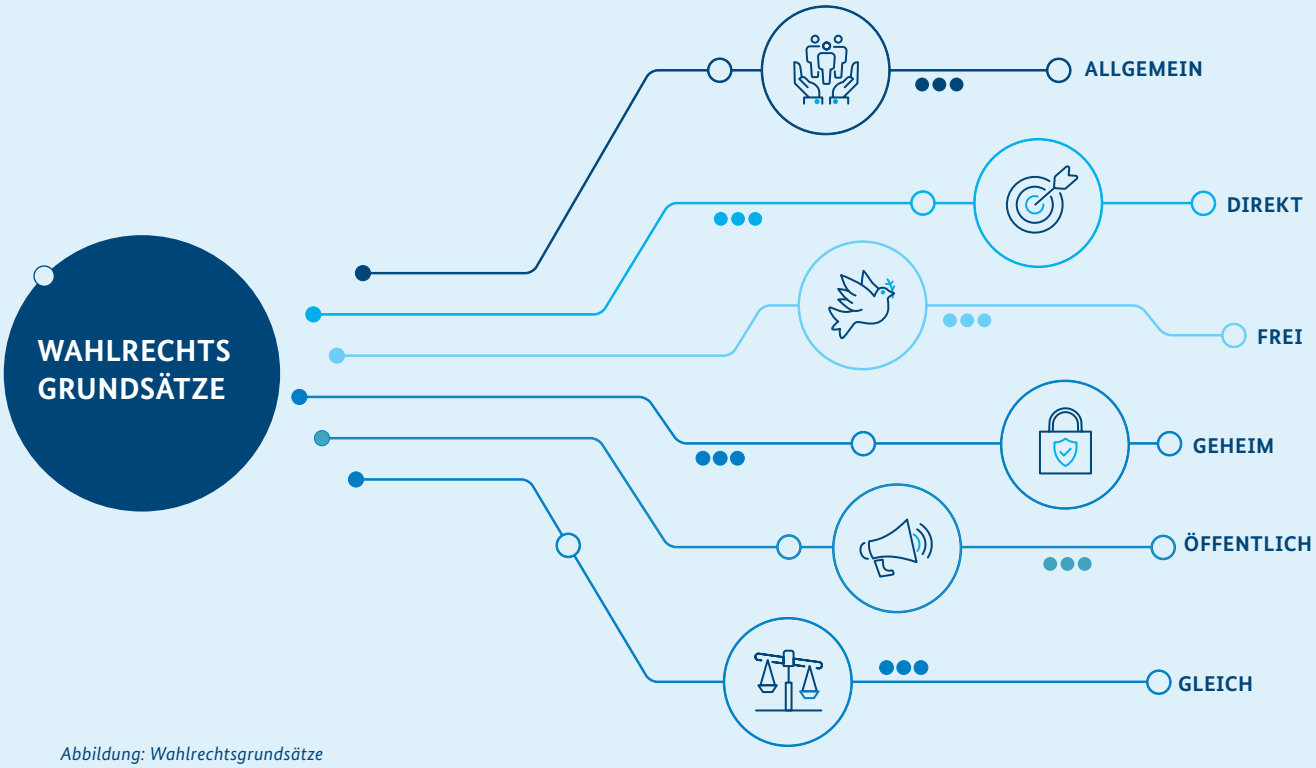


Abbildung: Wahlrechtsgrundsätze

Wahlen, sind aber anderen Bedrohungen ausgesetzt. Jede Art von Manipulation der Wahlhandlung muss ausgeschlossen werden. Der Begriff „Manipulation" beinhaltet dabei jede Form des unberechtigten Lesens, Änderns, Hinzufügens oder Löschens von Informationen sowie der Beeinflussung der Verfügbarkeit.

Bedrohungen im Rahmen von Online-Wahlen lassen sich in verschiedene Kategorien gliedern: Angriffe durch Außentäter unterschieden sich gegenüber Angriffen durch Innentäter; Angriffe auf IT-Systeme unterscheiden sich gegenüber der Beeinflussung von Wahlberechtigten.

Im Gegensatz zu Präsenz- und Briefwahlen können im schlimmsten Fall nicht nur einzelne Stimmen, sondern das komplette Wahlergebnis manipuliert werden.

Um diese Bedrohungen zu minimieren, müssen sowohl technische als auch organisatorische Maßnahmen umgesetzt werden. Dabei spielt Kryptografie eine wichtige Rolle. Neben der Transportverschlüsselung haben weitere Verschlüsselungsmechanismen sowie Signaturen und Zeitstempel eine besondere Bedeutung für die Absicherung von Online-Wahlen. Essentiell ist auch das entsprechende Schlüsselmanagement. Es muss sowohl technisch als auch organisatorisch sichergestellt werden, dass niemand unberechtigten Zugang zu den privaten Schlüsseln, ob zum Entschlüsseln, Zeitstempeln oder Signieren hat. Das sind nur zwei Beispiele für entsprechende Maßnahmen zum Schutz von Online-Wahlen.

Für das Modellprojekt Online-Sozialwahlen wurden die Methoden zur Absicherung in der TR-03162 festgesetzt. Aus diesem Projekt wurden für die Digitalisierung weiterer Wahlen, wie der Wahl zur Gleichstellungsbeauftragten, allgemeingültige sicherheitstechnische Anforderungen abgeleitet. Diese werden im BSI durch die Erstellung von Schutzprofilen für Online-Wahlprodukte und einer Technischen Richtlinie, die die Online-Wahlleitung adressiert *(siehe Artikel auf S. 14)*, umgesetzt und voraussichtlich Ende 2022 veröffentlicht. ■

Weitere Informationen:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03162/TR-03162_node.html

Zertifizierung von Online-Wahlprodukten

Zusammenspiel von Schutzprofilen und TR-03169

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

Die Zertifizierung von Online-Wahlprodukten mittels Schutzprofilen ist ein wichtiges Mittel, um Mindeststandards für Online-Wahlen zu setzen. In diesen Schutzprofilen werden Vorgaben an das Produkt formuliert. Die Zertifizierung solcher Produkte kann der Wahlleitung helfen, das richtige Produkt auszuwählen. Vor dem Einsatz dieser zertifizierten Produkte muss die Wahlleitung jedoch Entscheidungen und Vorbereitungen treffen. Das BSI wird dazu mit der TR-03169 Hilfestellungen geben.

Derzeit gibt es verschiedene Online-Wahlprodukte auf dem Markt. Soll eine Wahl oder eine Abstimmung online durchgeführt werden, stellt sich für die Online-Wahlleitung die Frage, welches Produkt das richtige ist. Online-Wahlen müssen insbesondere durch IT-sicherheitstechnische Maßnahmen geschützt werden. Jeder Anbieter bzw. Dienstleister von Online-Wahlen gibt selbstverständlich an, dass das eigene Produkt sicher ist. Doch eine IT-Sicherheitszertifizierung kann den Prozessverantwortlichen die Sicherheit geben, dass eine bestimmte Menge von Sicherheitszielen abgedeckt ist. Die Zertifizierung gibt unter anderem Auskunft darüber, ob kryptografische Verfahren nach dem aktuellen Stand der Technik eingesetzt werden, um ein authentisches Wahlergebnis zu liefern und gleichzeitig das Wahlgeheimnis zu wahren. Ein weiteres Beispiel ist das Vertrauensniveau, auf dem sich die Wählerinnen und Wähler bei der Online-Wahl anmelden und ihre Stimme abgeben können. Ist ein hohes Vertrauensniveau erforderlich, muss das Produkt den Einsatz der Online-Ausweisfunktion des Personalausweises oder eines anderen gleichwertigen Identifizierungsmittels auf diesem Niveau unterstützen.

Was decken die Schutzprofile nicht ab?

Neben der Frage, welches Vertrauensniveau für die Wahl bzw. Abstimmung überhaupt das Richtige ist, stellen sich der Wahlleitung weitere Fragen, denn eine Online-Wahl muss gut vorbereitet sein. Als erstes muss geprüft werden, ob die rechtlichen Rahmenbedingungen für eine Online-Wahl gegeben sind. Gegebenenfalls sind in einer Verordnung Anforderungen an die Online-Wahl formuliert worden, die eingehalten werden müssen (beispielsweise die Online-Wahlverordnung zum Modellprojekt Online-Sozialwahlen). Diese Anforderungen betreffen nicht nur das eingesetzte Online-Wahlprodukt selbst, sondern auch die Rahmenbedingungen, in denen es zum Einsatz kommt. Denn je nach Größe und Komplexität des Wahlvorhabens umfasst eine Online-Wahl viele Aufgaben und Prozesse, die in der Vor- und Nachbereitung, außerhalb der eigentlichen Anwendung zur Online-Wahl, durchgeführt werden. Zudem müssen auch organisatorische und betriebliche Vorkehrungen, die beim sicheren Einsatz einer Online-Wahlsoftware eine Rolle spielen, getroffen werden. Diese Rahmenbedingungen können dementsprechend nicht von der Produktzertifizierung abgedeckt werden.

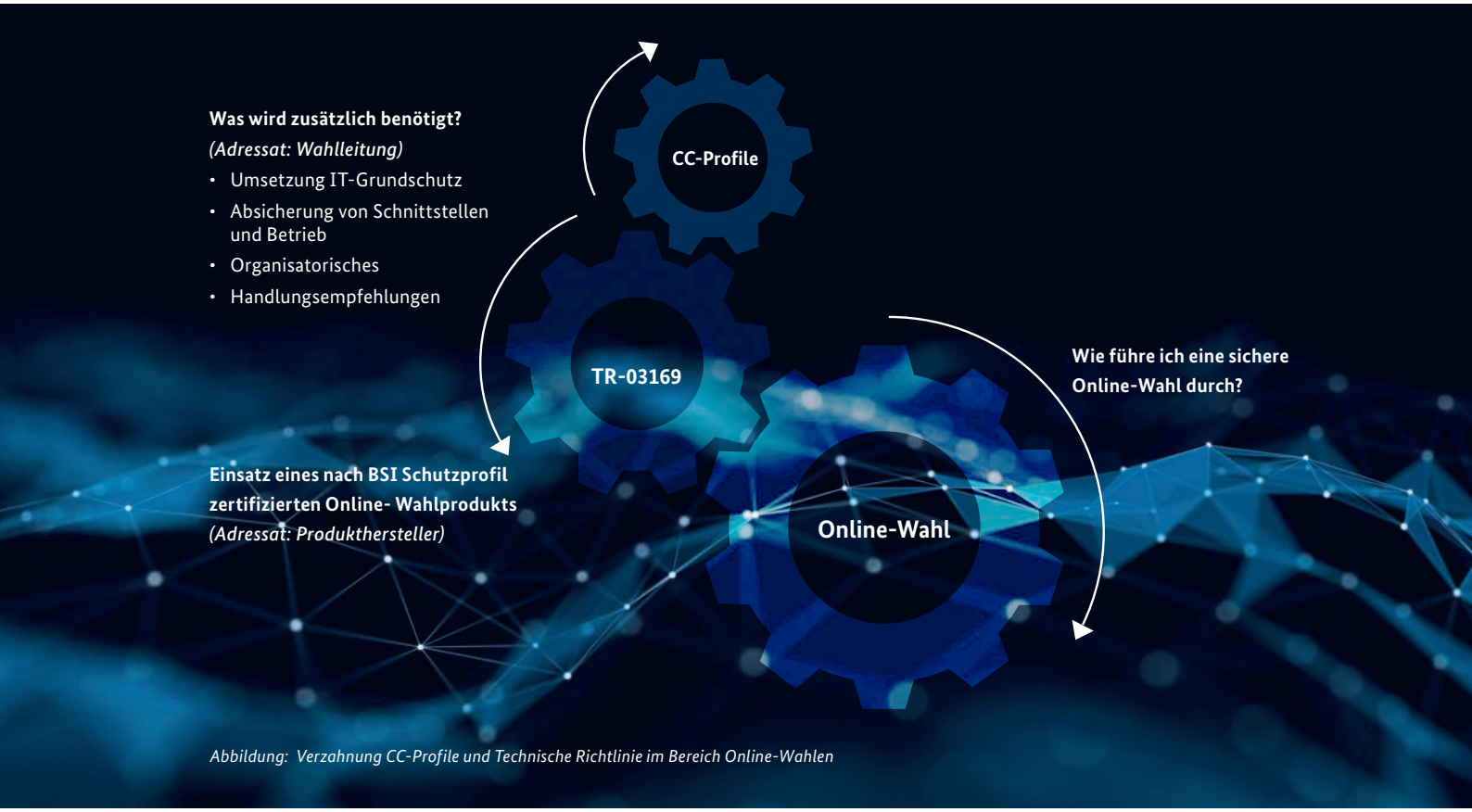


Abbildung: Verzahnung CC-Profile und Technische Richtlinie im Bereich Online-Wahlen

Warum wird die TR-03169 benötigt?

Aus diesem Grund wird das BSI neben der Produktzertifizierung die Technische Richtlinie TR-03169 (IT-sicherheitstechnische Anforderungen zur Durchführung einer elektronischen Wahl) voraussichtlich Ende 2022 zur Verfügung stellen. Die TR richtet sich entsprechend an die Wahlleitung und/oder andere Verantwortliche innerhalb einer Organisation, in der eine Online-Wahl durchgeführt werden soll, damit der vollständige Umfang zur sicheren Durchführung einer Online-Wahl adressatengerecht abgedeckt werden kann.

Dazu beschreibt die TR unter anderem:

- Vorbereitende Arbeiten einer Online-Wahl, wie das Sammeln von Daten und die Abstimmung von Inhalten zu Terminfestlegungen für den Wahlzeitraum, Wahlkennzeichen beziehungsweise Wählerverzeichnis und Wahlkandidatinnen und -kandidaten bzw. Wahllisten. Diese Arbeiten müssen außerhalb des Online-Wahlsystems durchgeführt werden. Die dabei zusammengetragenen Informationen müssen dann sicher in das Online-Wahlsystem übertragen werden.

- Die Anwendung von IT-Grundschutz insbesondere mit Blick auf die spezifischen Anforderungen von Online-Wahlen *(siehe Artikel auf S. 22)*.

- Handlungsempfehlungen für Prozessverantwortliche bei der Durchführung und Nachbereitung einer Online-Wahl.

- Wichtige Punkte zur Beachtung bei der Nutzung von externen Rechenzentren für den Betrieb von Anwendungen im Zusammenhang mit der Online-Wahl.

Der Fokus der TR liegt also vor allem darauf, der Wahlleitung die notwendigen Informationen an die Hand zu geben, um eine Online-Wahl von Anfang bis Ende so sicher wie möglich zu gestalten. Dabei ist vor allem wichtig, dass der Wahlleitung die eigenen Handlungsmöglichkeiten und -verpflichtungen klar aufgezeigt werden. Um die Komplexität einzelner Themenbereiche für die Wahlleitung zu reduzieren, liefert die TR auch Informationen über Möglichkeiten zur Kontrolle, wie beispielsweise Zertifizierungen oder Revisionen.

Mit der Zertifizierung eines Produkts für Online-Wahlen werden auf diese Weise die Grundvoraussetzungen für die sichere Abwicklung einer Online-Wahl auf Anwendungsebene geschaffen. Die TR beschreibt die zusätzlichen Rahmenbedingungen für die sichere Durchführung einer Online-Wahl. Gemeinsam bieten die Produktzertifizierung und die TR-03169 das nötige Handwerkszeug, das es braucht, um sich dem Thema Online-Wahl in allen wesentlichen Teilbereichen annehmen zu können. ■

Geheime Online-Wahlen

Zwischen Transparenz und Wahlgeheimnis

von Dr. Gottfried Herold, ehemals Referat Prüfung von Kryptoverfahren und Lea Nagler, Referat Vorgaben an und Entwicklung von Kryptoverfahren

Abstimmungen digitalisieren: Wie funktioniert der Prozess und welche Herausforderungen sind zu meistern? Ein kleiner Blick in die kryptografische Werkzeugkiste.

Um demokratisch legitimierte Entscheidungen zu treffen, muss die zugehörige Abstimmung einige Eigenschaften haben. Dazu können die Wahlgrundsätze allgemein, direkt, frei, geheim und gleich zählen. Zusätzlich sollte die Abstimmung auf eine Weise öffentlich sein, dass die Wählerinnen und Wähler darauf vertrauen können, dass das System als Ganzes diese Eigenschaften besitzt. Im Kontext von Online-Wahlen, womit Wahlen gemeint sind, bei denen mindestens die tatsächliche Stimmabgabe über das Internet erfolgt, werden manche dieser Eigenschaften durch kryptografische Maßnahmen erreicht. Die in kryptografischen Wahlprotokollen eingesetzten Grundbausteine sind sehr vielfältig und komplex. Im Folgenden sollen ausgehend von einem vereinfachten Protokoll zwei Ansätze solcher Protokolle grob umrissen werden. Dabei liegt der Fokus auf der Auszählung. Beide Ansätze gehören zu allgemein diskutierten Lösungsvorschlägen für das Problem der geheimen Online-Wahl.

Offene Wahl

Eine offene Wahl, an der lediglich die Wählerinnen und Wähler und ein Wahlserver beteiligt sind, könnte man wie folgt realisieren: Zur Überprüfung der Wahlberechtigung besitzt der Wahlserver eine Liste der Wahlberechtigten mit deren öffentlichen Signaturschlüsseln. Die Wählerinnen und Wähler übermitteln dem Wahlserver ihre Stimme gemeinsam mit einer Signatur und einem Verweis auf ihre Identität. Der Wahlserver kann dann die Liste der eingegangenen Stimmen bereinigen, sodass pro wählender Person nur eine gültige Stimme mit gültiger Signatur enthalten ist. Mit dieser bereinigten Liste ermittelt und veröffentlicht der Server nun das Ergebnis. Veröffentlicht der Server zusätzlich sämtliche Listen (Signaturschlüssel, eingegangene Stimmen, bereinigte Stimmen), können alle Beteiligten prüfen, ob die eigene Stimme eingetroffen ist und das Gesamtergebnis korrekt ermittelt wurde.

Um diesen Ablauf zu einer geheimen Wahl zu ergänzen, wäre eine erste Idee, die Stimmen mit einem Public-Key-Verfahren verschlüsselt zu versenden. Nun ist die Wahlentscheidung zwar geheim gegenüber Dritten, jedoch nicht notwendigerweise gegenüber dem Wahlserver, der die Stimmen auf Gültigkeit prüfen und auswerten muss. Die Schwierigkeit besteht darin, dass der Wahlserver einerseits zur Prüfung der Wahlberechtigung eine Verbindung zwischen Abgabe und Identität herstellen muss, andererseits die Wahlentscheidung selbst nicht einer Identität zuordnen können soll. Es muss also eine Möglichkeit gefunden werden, nach der Prüfung der Berechtigung die Identität von der verschlüsselten Stimme zu trennen:

Entweder das Ergebnis wird in verschlüsseltem Zustand ermittelt (homomorphe Auszählung) oder das Mischen in der physikalischen Wahlurne wird simuliert (verifizierbares Mischen).

Homomorphe Auszählung

Homomorphe Auszählungsverfahren vermeiden die Entschlüsselung einzelner Stimmen. Bei einer Wahl zwischen zwei Optionen (z. B. „Ja“/„Nein“) könnte festgelegt werden, dass eine Ja-Stimme einer 1, eine Nein-Stimme einer 0 entspricht. Die Summe der abgegebenen Stimmen ergibt dann die Anzahl der Ja-Stimmen. Es ist ausreichend, diese Summe der Stimmen mit der Anzahl der abgegebenen gültigen Stimmen zu vergleichen. Es gibt spezielle, sogenannte Homomorphe Verschlüsselungsverfahren, die es ermöglichen, eine solche Summation mit den verschlüsselten Stimmen durchzuführen, ohne dafür die einzelnen Stimmen entschlüsseln zu müssen. Das Ergebnis ist dann die Anzahl der Ja-Stimmen in verschlüsselter Form und nur dieses Ergebnis wird entschlüsselt.

Das Problem der Geheimhaltung gegenüber dem Wahlserver ist damit jedoch noch nicht gelöst. Alle, die Zugriff auf den Schlüssel zur Entschlüsselung des Ergebnisses haben, können damit auch einzelne Stimmen entschlüsseln. Die Verwendung eines homomorphen Verfahrens mit Threshold Decryption kann dieses Problem lösen. Dies ist sozusagen die digitale Variante des Vier-Augen-Prinzips: Das Vertrauen wird auf mehrere Server verteilt, die jeweils nur einen Teilschlüssel besitzen. Jeder Server führt eine Teiloperation durch, so dass der tatsächliche Schlüssel nie als Ganzes vorliegt. Sind genügend Server ehrlich und operieren nur auf dem Endergebnis, so gelingt es unehrlichen Servern nicht, das Wahlgeheimnis zu verletzen.

Ein Schutz vor unehrlichen Servern ist also gegeben. Vor unehrlichen Wählerinnen und Wählern ist das Verfahren nicht sicher, da eine direkte Prüfung der Gültigkeit des Formats der Stimme nicht erfolgen kann. Im obigen Beispiel könnten Wählerinnen und Wähler versuchen, statt einer 1 eine 2 verschlüsselt zu versenden, um so ihr Stimmgewicht zu verdoppeln. Es muss also ein Beweis über die Form der Stimme erbracht werden, der die Stimme selbst nicht offenlegt. Dies können nicht-interaktive Zero-Knowledge-Proofs leisten.

Ein Nachteil dieses Ansatzes ist, dass sich nur Wahlsysteme umsetzen lassen, deren Ergebnis durch eine Operation wie die Addition ermittelt werden kann. Dies ist jedoch nicht bei jeder Wahl der Fall. Das motiviert

Signatur	Digitale Unterschrift, die vor nachträglicher Manipulation schützt.
Public-Key-Verfahren	Verschlüsselungsverfahren, das für Ver- und Entschlüsselung getrennte Schlüssel hat. Die Verschlüsselung ist allen möglich, die den Public-Key besitzen, dieser befähigt aber nicht zur Entschlüsselung.
Homomorphes Verschlüsselungsverfahren	Verschlüsselungsverfahren, das Operationen wie die Addition im verschlüsselten Zustand erlaubt.
Threshold Decryption	Entschlüsselung, die von mehreren Parteien in Zusammenarbeit erfolgen muss.
Bulletin Board	Öffentliches Protokoll der versendeten Nachrichten und ausgeführten Operationen.
Nicht-interaktiver Zero-Knowledge-Proof	Beweis über eine Eigenschaft eines Geheimnisses, der letzteres nicht lüftet und keine Interaktion zwischen Beweisenden und Herausfordernden benötigt.
Rerandomisierung	Erneuerung der im Chiffrat enthaltenen Zufallskomponente.
Mix-Net	Zusammenspiel mehrerer Server, die Chiffrate rerandomisieren und zufällig permutieren.
Individuelle Verifizierbarkeit	Möglichkeit der Wählerinnen und Wähler, die korrekte Auszählung der eigenen Stimme nachzuvollziehen.
Universelle Verifizierbarkeit	Möglichkeit, die Korrektheit des gesamten Verfahrens nachzuvollziehen.

den zweiten Ansatz, bei dem die Einzelstimmen zur Ermittlung des Ergebnisses entschlüsselt werden.

Verifizierbares Mischen

Der Wahlserver trennt zunächst die verschlüsselten Stimmen von Signatur und Identität. Danach bringt er sie in eine neue, zufällige Reihenfolge. Dieser Schritt ist nicht nur deshalb wichtig, weil Signatur und Identität eine Verbindung zwischen Wahlentscheidung und Wählenden darstellen, sondern auch, weil der Zeitpunkt der Versendung Einfluss auf den Platz in der Liste der abgegebenen Stimmen hat. Das könnte Beobachterinnen und Beobachtern ermöglichen, auch ohne Identitätshinweis Rückschlüsse auf die wählende Person zu ziehen. Werden im Zuge der Transparenz sämtliche Aktionen öffentlich sichtbar protokolliert (Bulletin Board), ist dieser Vorgang noch wichtiger.

In diesem Kontext wird auch ersichtlich, dass das bloße Mischen der genannten Informationen noch nicht reicht: Die Chiffrate sind noch dieselben und könnten mit den abgegebenen Chiffraten, die noch einer Identität zuordenbar sind, verglichen werden. Um das zu verhindern, müssen sie transformiert werden und das ohne den Klartext zu verändern oder zu kennen. Eine Möglichkeit dies zu erreichen ist die Rerandomisierung.

Dazu wird die Tatsache genutzt, dass Verschlüsselungsverfahren in der Regel nicht deterministisch sind. Das bedeutet, dass sich zwei Chiffrate zum selben Klartext und Schlüssel im Allgemeinen voneinander unterscheiden. Im Falle von Wahlen, die mit einem Public-Key-Verfahren geschützt werden, wird ihre Notwendigkeit schnell deutlich: Beobachten Angreifende die Verteilung der Chiffrate und vergleichen sie mit dem veröffent-

lichten Wahlergebnis, so können sie bei jedem Chiffrat erkennen, für welchen Klartext es steht, und damit das Wahlgeheimnis für alle Stimmen auf einmal brechen, ohne auch nur den Public-Key zu kennen. Damit dies nicht geschieht, muss also bei der Verschlüsselung eine Zufallskomponente das Chiffrat verschleiern. Die Idee ist nun, diese Zufallskomponente zu erneuern. Aus Sicht von Beobachterinnen und Beobachtern ist der Bezug zwischen verschlüsselter Stimme und Identität dann zerstört. Damit dies auch für den einzelnen Wahlserver gilt, werden mehrere Server eingesetzt, die diese Operation unabhängig nacheinander ausführen und gemeinsam das Mix-Net bilden.

Die Stimmen sind damit geheim, sie können allerdings von einem unehrlichen Server auf folgende Weise manipuliert werden: Dieser könnte Stimmen vervielfältigen und andere stattdessen löschen. Um dies zu verhindern, wird wie bei der homomorphen Verschlüsselung ein Zero-Knowledge-Proof verwendet. Am Ende des Mischvorgangs können alle Stimmen mit Threshold Decryption entschlüsselt und danach ausgewertet werden.

Eine Frage des Vertrauens?

In den obigen Ansätzen wurde vor allem die Auszählung betrachtet. Eine Wahl besteht jedoch aus mehreren Teilschritten, die als Gesamtheit überprüfbar sein sollten. Die Möglichkeit, dass jeder einzelne den Eingang und die Auszählung seiner Stimme prüfen kann, bezeichnet man als „individuelle Verifizierbarkeit“. Diese setzt sich aus folgenden drei Teilverifizierungen zusammen: (1) Übertragung der Wahlentscheidung in Form einer (verschlüsselten) Stimme (Cast-as-Intended), (2) Übermittlung und Speicherung (Stored-as-Cast) und (3) Auszählung (Tallied-as-Stored).

Die Möglichkeit, dass unabhängige Auditorinnen und Auditoren die Korrektheit der gesamten Wahl überprüfen kann, bezeichnet man als universelle Verifizierbarkeit. Beide Eigenschaften sind wichtig, da sie das Vertrauen in ein Wahlsystem erhöhen.

Durch die Verschlüsselung der Stimmen gehen Teile dieser Eigenschaften verloren und müssen mit anderen Mitteln wiederhergestellt werden. Im Falle der homomorphen Verschlüsselung beispielsweise stellen die Zero-Knowledge-Proofs die Überprüfbarkeit der Gültigkeit der Stimmen wieder her und dienen damit der universellen Verifizierbarkeit.

Trotz geeigneter Mechanismen, die der Nachvollziehbarkeit dienen, ist aus Sicht des BSI für den Einsatz von Online-Wahlprodukten eine gründliche Prüfung oder Zertifizierung erforderlich. Die Produkte zeichnen sich durch ein komplexes Zusammenspiel vieler unterschiedlicher Mechanismen aus. Diese müssen richtig zusammengefügt werden, damit eine Online-Wahl sicher funktionieren kann. Ein Produkt für Online-Wahlen sollte damit allen Anforderungen an Informationssicherheit genügen – genau wie jedes andere IT-Produkt. ■

Weitere Informationen:

https://oparu.uni-ulm.de/xmlui/handle/123456789/22747?locale-attribute=de

Sicherheit gestalten

Wie Online-Wahlprodukte die Software-Zertifizierung voranbringen

von Fritz Bollmann und Michael Meissner, Referat Zertifizierung Software

Produkte, die im Bereich von Online-Wahlen eingesetzt werden, unterliegen zum einen hohen IT-Sicherheitsanforderungen, deren Umsetzung über Zertifizierungen nachgewiesen werden können. Zum anderen werden solche Produkte in der Regel in sehr kurzen Release-Zyklen veröffentlicht. Der gesetzeskonforme Einsatz von zertifizierten Produkten, die kurzen, regelmäßigen Release-Zyklen unterliegen, erfordern ein Weiterdenken in der Produktzertifizierung.

Die Common Criteria (CC) sind eine der wenigen international anerkannten IT-Sicherheitskriterien, mit denen hohe Vertrauenswürdigkeitsaussagen getätigt werden können. Dabei sind die CC so flexibel, dass Hersteller oder Autorinnen und Autoren von Schutzprofilen sowohl die Höhe der Vertrauenswürdigkeit als auch die Wahl der Sicherheitsfunktionen frei und entsprechend ihrer individuellen Anforderungen festlegen können.

Wenn eine hohe Vertrauenswürdigkeit und damit auch eine hohe Sicherheitsaussage benötigt werden, erhöht das automatisch die Evaluierungsaufwände, da nachgewiesene Sicherheit nur auf Wissen und Fakten beruhen kann. In öffentlichen Aussagen wird häufig kritisiert, dass CC-Zertifizierungen aufwändig seien und lange dauern würden. Dies liegt jedoch in der Regel nicht an der CC, sondern an den notwendigen Aufwänden bei hohen Vertrauenswürdigkeitsanforderungen.

Naheliegende Stellschrauben, um Aufwände in einer Zertifizierung zu senken, sind daher die Wahl niedrigerer Evaluierungsstufen und die Beschränkung der zu prüfenden Sicherheitsfunktionen.

Neben den CC bietet das BSI zum Beispiel mit der Beschleunigten Sicherheitszertifizierung *(BSZ, siehe Artikel auf S. 6)* und dem IT-Sicherheitskennzeichen weitere Verfahren an, die es ermöglichen, für möglichst viele Produkte und Anwendungsszenarien angemessene Sicherheitsaussagen zu treffen. Die BSZ bedient sich beispielsweise einer stichprobenartigen, risikogetriebenen Prüfung, um Sicherheitsaussagen zu treffen.

Für hohe Prüftiefen gibt es aktuell jedoch keine Alternative zur Common-Criteria-Zertifizierung. Hier müssen andere Strategien zur Beschleunigung angewendet werden.

Umgang mit Produktänderungen: Re-Zertifizierung

Die erste Produktzertifizierung eines Herstellers ist in der Regel am aufwändigsten. Entwicklungsprozesse müssen angepasst und dokumentiert werden, Evaluierungsdokumente müssen erstellt werden. Die Evaluierenden und Zertifizierenden lernen durch Audits und Besuche beim Hersteller die realen Arbeitsabläufe und Prozesse vor Ort kennen. Sie sprechen mit Entwicklerinnen und Entwicklern und sehen, wie sehr diese die Sicherheitsprozesse in der Entwicklung (und Produktion) kennen und leben. Die Erfahrung zeigt, dass Sicherheitsnachweise eines Produktes nicht nur durch das Lesen von Dokumenten erlangt werden können, sondern auch durch die Erfahrung der real gelebten Sicherheitsprozesse bei einem Hersteller.

Dadurch können Beteiligte bei einer späteren Re-Zertifizierung Schwerpunkte setzen und Aspekte wiederverwenden. Die Evaluierung wird effizienter. Mit jeder Re-Zertifizierung und mit jedem Audit wird diese Basis vertieft. Die Re-Zertifizierungs-Projekte werden auf natürliche Weise schneller. Diese Vorgehensweise beruht in der Regel auf der langjährigen Zusammenarbeit

zwischen einem Hersteller, einem Prüflabor und der Zertifizierungsstelle.

Lösungsansätze der CC-Community

Eine neue CC-Methodologie namens Patch Management soll das Kunststück schaffen, eine Re-Zertifizierung zu beschleunigen, ohne dabei Sicherheitskompromisse einzugehen. Konkret handelt es sich um einen Prozess, der die Vertrauensbildung in die Patch- und Software-Qualitätsprozesse beim Hersteller stärker fokussiert.

Ziel ist es, den vertrauensbildenden Prozess zu beschleunigen. Dazu werden einige zusätzliche Vertrauenswürdigkeitsanforderungen zur Produktpflege und Entwicklungssicherheit definiert, vergleichbar mit den erlebten Erfahrungen vor Ort. Die Ergebnisse können dann unmittelbar in einer Re-Zertifizierung wiederverwendet werden. Konkret gibt es für diese Methodologie momentan zwei Ansätze. Die eine stammt von der International Security Certification Initiative (ISCI) Working Group, die andere von der ISO (Towards Creating an Extension for Patch Management for ISO/IEC 15408 and ISO/IEC 18045). Die grundsätzliche Motivation der Ansätze ist deckungsgleich, jedoch unterscheiden sie sich in der Modellierung der zusätzlichen Anforderungen. Die ISO-Methodologie wurde bereits in einem Zertifizierungsverfahren durch das BSI pilotiert.

Insbesondere im Software-Bereich sind die Versionszyklen aufgrund der schnellen Entwicklungsdynamik kurz. Das war bislang der Nachteil der CC, da eine Zertifizierung unter hoher Vertrauenswürdigkeit oft nicht mit schnellen Versionszyklen mithalten konnte. Zum ersten Mal gibt es mit der Methodologie des Patch Managements nun die Chance, diesen Nachteil zu beheben.

Online-Wahlprodukte

Online-Wahlprodukte, für die es auch weitere Schutzprofile geben wird, stehen wie kaum ein anderes Produkt im Fokus der kritischen Öffentlichkeit und Sicherheitsbetrachtung. Dazu kommt, dass diese Produkte zu einem bestimmten Zeitpunkt einsatzbereit und auf dem aktuellen Sicherheitsstand sein müssen. Eine Wahl kann nicht verschoben werden, nur weil ein Zertifizierungsprozess noch nicht abgeschlossen ist. Die Kombination von hohem öffentlichen Fokus, notwendiger zertifizierter IT-Sicherheit, strengem Zeitrahmen und schnellen Update-Zyklen machen das Patch Management zu dem idealen Hilfsmittel für die CC-Zertifizierung von Online-Wahlprodukten.

Das BSI wird daher den neuen Ansatz des Patch Management in der Zertifizierung weiter erproben und einführen, auch um den Anforderungen im Bereich Online-Abstimmungen gerecht zu werden. Zugleich soll dies der CC-Zertifizierung auch für andere Produkttypen einen neuen Impuls geben, um trotz Beibehaltung der erwarteten hohen Vertrauenswürdigkeit die Projektlaufzeiten zu beschleunigen. ■

Informationen schützen – sicher wählen

IT-Grundschutz bei Online-Wahlen

von Sebastian Palm, Referat eID-Lösungen für die digitale Verwaltung

Online-Wahlen sind ein komplexes Thema, bei dem zahlreiche Besonderheiten berücksichtigt werden müssen. Wie verträgt sich dieses Thema mit dem IT-Grundschutz und was gibt es dabei zu beachten?

Die Technische Richtlinie TR-03169 (IT-sicherheitstechnische Anforderungen zur Durchführung einer elektronischen Wahl) richtet sich an Wahlleitungen mit dem Ziel Online-Wahlen in verschiedenen Kontexten abzusichern. So sollen zukünftig verschiedene Wahlen (zum Beispiel die Wahl der Gleichstellungsbeauftragten oder Betriebsratswahlen) mit Hilfe der TR-03169 online durchgeführt werden können. Online-Wahlen sind ein besonderes Einsatzszenario. Je nach Wahlkontext gelten unterschiedliche gesetzliche Vorgaben wie Wahlverordnungen. Zudem müssen spezifische Prozesse und Anforderungen abgebildet werden, zum Beispiel in Bezug auf Wahlverzeichnis, Wahlkennzeichen und Stimmzettel). Außerdem müssen die für Online-Wahlen charakteristischen Gefährdungen und Schadensszenarien abgeschätzt werden (zum Beispiel: „Wie schütze ich die Wahlgrundsätze allgemein, direkt, frei, geheim, öffentlich und gleich?“).

Ein wesentlicher Teil der TR-03169 ist die Umsetzung des IT-Grundschutzes. Er bietet die Möglichkeit, Anforderungen der Informationssicherheit bedarfsgerecht auf einen festgelegten Informationsverbund zuzuschneiden. Bei dem gewichtigen Thema Online-Wahlen muss für den darauf bezogenen Informationsverbund als Vorgehensweise für die Anwendung des IT-Grundschutzes die umfangreichere Standard-Absicherung gewählt werden (Im Gegensatz zur Basis- oder Kern-Absicherung).

Die einzelnen Schritte der Grundschutzmethodik bei der Durchführung gemäß der Standard-Absicherung zeigt die Abbildung.

Die eigentliche Besonderheit bei der Umsetzung von IT-Grundschutz für Online-Wahlen ergibt sich aus der Modellierung. Hier kommt die Fragestellung auf, wie dies anwendungsseitig abgebildet werden kann, da für die spezielle Anwendung Online-Wahlen kein Baustein im IT-Grundschutz-Kompendium existiert.

Im IT-Grundschutz gibt es für die Modellierung von Anwendungen einige allgemeinere Bausteine, von denen „APP.3.1 Webanwendungen“ und „APP.6 Allgemeine Software“ diejenigen sind, die vermutlich für die meisten Einsatzszenarien von Online-Wahlen herangezogen werden können. Dabei ist APP.3.1 auch nur dann sinnvoll, wenn es sich bei dem eingesetzten Online-Wahlprodukt tatsächlich um eine Webanwendung im Sinne des entsprechenden Bausteins handelt. Bei einer Eigenentwicklung müssten beispielsweise noch weitere Bausteine herangezogen werden (zum Beispiel APP.7).

Die zur Verfügung stehenden Bausteine sind auf Grund der Komplexität einer Online-Wahl nicht unbedingt ausreichend für eine Modellierung und betrachten nicht alle möglicherweise relevanten Anwendungsfälle und Gefährdungen, wie die Prozesse zur Erstellung und Überführung besonders schützenswerter Daten des Wahlvorgangs in die Wahlanwendung (zum Beispiel Wahlverzeichnis, Stimmzettel). Um mit dieser Problematik umzugehen, sieht der IT-Grundschutz vor, für das betroffene Zielobjekt (also in diesem Fall die Anwendung zur Online-Wahl) eine Risikoanalyse vorzunehmen, da es nicht hinreichend durch die Bausteine aus dem IT-Grundschutz-Kompendium abgebildet werden kann.

Alternativ kann man für ein Zielobjekt, für das es im IT-Grundschutz keinen passenden Baustein gibt, einen eigenen benutzerdefinierten Baustein erstellen. Da mit der Erstellung eines benutzerdefinierten Bausteins ein gewisser Aufwand verbunden ist, sollte erwogen werden, ob der Baustein wiederholt Anwendung finden kann. Bei einem einmaligen oder seltenen Anwendungsfall lohnt sich die Erstellung eines eigenen benutzerdefinierten Bausteins gegebenenfalls nicht. Benutzerdefinierte Bausteine können in Abstimmungen mit dem IT-Grundschutz-Referat des BSI erstellt werden. Eine Vorlage, Umsetzungshinweise und weitere Informationen zu benutzerdefinierten Bausteinen gibt es auf der Webseite des BSI.

Aktuell ist ein IT-Grundschutz-Profil „Schnellmeldungen von Wahlergebnissen“ in Erstellung, in dem die Wahlunterstützung ein wesentlicher Bestandteil sein wird. Mit einer Fertigstellung ist Anfang 2022 zu rechnen.

Common Criteria Protection Profiles und Technische Richtlinien *(siehe Artikel S. 20)* sind eine gute Grundlage zur Auswahl von Maßnahmen im Rahmen der Erstellung einer Risikoanalyse. Sie sind nicht als abschließend zu betrachten, und es sollten weitere passende Maßnahmen für die im Rahmen der Risikoanalyse gefundenen Gefährdungen evaluiert werden. Dies ist insbesondere wichtig, da jedes Einsatzszenario, jede Betriebsumgebung und jede Anwendung unterschiedlich ist und bei der Risikoanalyse diesen Unterschieden und den dadurch entstehenden Anforderungen Rechnung getragen werden muss. ■

Weitere Informationen:

www.bsi.bund.de/IT-Grundschutz

Abbildung: Vorgehensweise IT-Grundschutz: Standard-Absicherung (Quelle: BSI Standard 200-2)

Virtuelle Veranstaltungen und Abstimmungen

Praxisnahe Informationen und Hilfestellungen für eine erfolgreiche Digitalisierung

von Michael Amler, Referat Nationales Verbindungswesen, und Dr. Florian Seiller, Referat Strategien und neue Ansätze der Informationssicherheit

Im Zuge der Corona-Pandemie ist der Bedarf an Lösungen für virtuelle Versammlungen und Abstimmungen sprunghaft gestiegen. Doch wie lassen sich solche Formate vor dem Hintergrund der wachsenden Bedrohungslage im Cyber-Raum möglichst sicher durchführen? Das BSI hat dazu Szenarien, Leitfragen, Hinweise und praxisnahe Hilfestellungen veröffentlicht und leistet beratende Unterstützung.

Die Corona-Pandemie hat der Digitalisierung einen gewaltigen Schub beschert. Präsenzveranstaltungen unterschiedlichster Größe, wie Vereins- oder Aktionärsversammlungen, Vorlesungen und Seminare an Universitäten, Meetings von Unternehmen oder Plenar- und Gremiensitzungen von Parlamenten oder Parteien konnten über Monate hinweg nicht oder nur sehr eingeschränkt stattfinden. Die Nutzung von Web- und Videokonferenz-Tools und Plattformen zum kollaborativen Arbeiten ist infolgedessen sprunghaft angestiegen und dürfte mittlerweile fest zum New Normal gehören. Doch wie ist es um die IT-Sicherheit virtueller oder hybrider Konferenz- oder Versammlungsformate bestellt? Worauf ist zu achten, damit Informationen in der digitalen Welt sicher übertragen und ausgetauscht werden können? Welche Sicherheitsrisiken gibt es und wie können die Grundwerte der Informationssicherheit (Verfügbarkeit, Authentizität / Integrität und Vertraulichkeit) angemessen geschützt werden? Kurzum: Wie lassen sich virtuelle Versammlungen und Abstimmungen mit einem dem jeweiligen Anlass beziehungsweise den individuellen Anforderungen entsprechenden Maß an Sicherheit durchführen?

Projektgruppe Virtuelle Versammlungen und Abstimmungen (ViVA) des BSI

Das BSI hat sich seit April 2020 verstärkt mit dem Themenbereich „Virtuelle Versammlungen und Abstimmungen“ (ViVA) befasst. Das Ergebnis dieser Arbeit sind mehrere Veröffentlichungen mit Szenarien, Leitfragen, Hinweisen und praxisnahen Tipps, die auf der Internetseite des BSI abrufbar sind und Herstellern, Betreibern und Veranstaltern als Hilfestellung dienen können – von der Planung bis zur Umsetzung.

Das Papier „Ideen und Szenarien für Staat, Wirtschaft und Gesellschaft“, das als Einstieg gedacht ist, enthält Ideen und Szenarien rund um virtuelle Versammlungen sowie (nicht geheime) Abstimmungen und liefert erste Antworten, wie kleine, mittlere und größere digitale Versammlungsformate mit normalem Schutzbedarf sicher realisiert werden können.

Die Durchführung elektronischer Abstimmungen ist mit gewissen Risiken verbunden. Dies gilt in besonderem Maße für geheime Abstimmungen. Die Veröffentlichung „Ansätze zur Risikoabwägung bei digitalen geheimen Abstimmungen im Rahmen von Versammlungen“ nimmt primär betroffene Wahlgrundsätze in den Blick und stellt grundsätzliche Fragen, die vonseiten der Veranstalterinnen und Veranstalter zu klären sind, bevor eine geheime Abstimmung elektronisch umgesetzt wird.

Das Papier „Anforderungen an Produkte für virtuelle Versammlungen und Abstimmungen“, das auch in englischer Sprache verfügbar ist und in dessen Rahmen das BSI mit verschiedenen in- und ausländischen Partnern und Anbietern in Kontakt stand, enthält einen umfangreichen Katalog an Produktanforderungen unterteilt in die Bereiche Leistungs- und Sicherheitsmerkmale, Sicherheitsnachweise und Tests sowie Detektion. Der Anforderungskatalog richtet sich in erster Linie an Hersteller und Betreiber von Produkten und Dienstleistungen für virtuelle Versammlungen und Abstimmungen, kann aber zugleich als Orientierungshilfe für die Produktauswahl dienen.

Weitere BSI-Empfehlungen zur Erhöhung der Informationssicherheit

Systematische Ansätze zur substantiellen Erhöhung des Sicherheitsniveaus von virtuellen Versammlungen und Abstimmungen bieten zudem die bewährten Grundlagendokumente des BSI, die neben technischen auch infrastrukturelle, organisatorische und personelle Aspekte in den Blick nehmen. Zu nennen sind hier etwa der IT-Grundschutz mit dem IT-Grundschutz-Kompendium und den IT-Grundschutz-Profilen, das Kompendium Videokonferenzsysteme sowie der BSI-Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue, (*siehe Artikel auf S. 22*).

Praxisbeispiel Parteitage

Eine besondere Herausforderung stellt die sichere Gestaltung von digitalen Parteitagen dar. Erstmals mussten sich 2020 im Bundestag vertretene Parteien komplett virtuell treffen, diskutieren, Positionen finden und auch Personen und Ämter wählen.

Dazu brauchte es nicht nur Gesetzesänderungen. Fragen nach der Informationssicherheit rückten plötzlich in den Fokus: Wie können geheime Wahlen gestaltet werden? Welche Risiken gehen die Parteien dabei ein? Wie können sich mehrere hundert Delegierte beteiligen?

Der politische Fokus der Veranstaltung liegt nicht nur auf ihren Inhalten. Auch politisch motivierte Angriffsversuche und ihre Folgen sind zu berücksichtigen.

Das BSI hat hierzu generelle Unterstützung angeboten und die Parteien auf deren Anfrage bei der sicheren Umsetzung dieser digitalen Veranstaltungen begleitet, u. a. durch die Vor-Ort-Präsenz einer Verbindungsperson. Die gesammelten Erfahrungswerte flossen wiederum in die erwähnten öffentlichen Papiere ein. Dreh- und Angelpunkt eines sicheren Parteitags ist dabei vor allem die Vorbereitung eines funktionierenden Vorfallsmanagements und einer Krisenkommunikation wie auch ausreichender Redundanz- und Mitigationsmaßnahmen.

Parteitag – zusätzliche Funkverbindung zum Berliner Fernsehturm, um für einen Netzausfall Redundanz zu schaffen

Weitere Entwicklung

Bevor IT-sicherheitstechnische Lösungen erarbeitet werden können, müssen – unabhängig von der Art der Versammlung oder Abstimmung – von den Anwenderinnen und Anwendern – Risiken und Einsatzzweck sorgfältig abgewogen und die gewünschten Anforderungen definiert werden. Hundertprozentigen Schutz kann kein System gewährleisten.

Die Entwicklung des gesamten Bereichs ist sehr dynamisch und seit über einem Jahr davon geprägt, sektorübergreifend voneinander zu lernen. Das BSI und die Projektgruppe ViVA leisten hierzu einen Beitrag und bieten mit den erarbeiteten Papieren und den darin enthaltenen praxisnahen Tipps, Leitfragen und Empfehlungen einen umfangreichen Orientierungsrahmen, um virtuelle Veranstaltungen und Abstimmungen mit einem hohen Maß an Sicherheit durchführen zu können. ■

Weitere Informationen:

https://www.bsi.bund.de/viva
Kontakt: viva@bsi.bund.de

Digitale Wahlen und Abstimmungsprozesse

Stimmen aus der Praxis

von Agnieszka Pawlowska, Referat Cyber-Sicherheit für die Wirtschaft und Allianz für Cyber-Sicherheit

Die Überführung analoger Abstimmungsprozesse ins Digitale stellt eine große Chance aber auch Herausforderung für Unternehmen und für die Parteienlandschaft dar. Die Allianz für Cyber-Sicherheit (ACS) hat in ihren beiden Formaten, dem Cyber-Sicherheits-Web-Talk und ihrem Podcast CYBERSNACS, Stimmen aus der Praxis eingefangen.

Lassen sich Versammlungen und Abstimmungsprozesse einfach so ins Digitale übertragen? Diese Frage mussten sich 2020 und 2021 auch die Parteien stellen, als es um die Durchführung ihrer Parteitage ging. Coronabedingt wurden hier in den letzten zwei Jahren verschiedene neue Wege beschritten. So führten die Grünen im September 2020 ihren ersten hybriden Parteitag durch. Die CDU stellte sich im Januar 2021 der Herausforderung, ihren ersten komplett digitalen Parteitag und die Wahl des neuen Parteivorsitzenden zu organisieren. In der vierten Folge von CYBERSNACS haben die Moderatorinnen mit Dr. Stefan Hennewig gesprochen, der in seiner Funktion als CDU-Bundesgeschäftsführer die Planung und Durchführung verantwortete.

Diejenigen, die sich plötzlich vor der Aufgabe sahen, Vor-Ort-Veranstaltungen ins Digitale zu verlagern, wissen: Eine Eins-zu-Eins-Übertragung ist nicht möglich. Ein vielstimmiges Fazit nach über einem Jahr Pandemie lautet, dass die Organisation digitaler Veranstaltungen deutlich aufwändiger sein kann als die analoger.

So auch beim Parteitag der CDU, der samt Online-Wahlen zum Parteivorsitz viele Anforderungen erfüllen musste. Dazu mussten zunächst die über zwölf verschiedenen und mitwirkenden „Gewerke“ - also technisch und organisatorisch beteiligte Einheiten - miteinander koordiniert werden. Dies galt insbesondere für die Softwareanbieter des digitalen Plenarsaals und die mit der Durchführung der Abstimmung beauftragten Firma. Eine einfache öffentliche Abstimmung, analog zum „Hand heben“ im Konferenzsaal, lässt sich heutzutage bereits mit den gängigen Videokonferenzsystemen abbilden. Die Herausforderung beginnt bei der geheimen Wahl. Hier wurde ein weiterer, darauf spezialisierter Dienstleister mit der Durchführung beauftragt. Dieser sollte neben dem sicheren, unangreifbaren Ablauf auch Verfahren zur Nachvollziehbarkeit der Wahl gemäß Artikel 21 des Grundgesetzes anbieten können.

CYBER SNACS

Zudem unterliegen Parteiwahlen strengeren Regularien, die die Leitplanken in der Durchführung enger setzen, als dies beispielsweise bei Abstimmungen auf Aktionärsversammlungen der Fall wäre. Aus diesem Grund erfolgte die Wahl des neuen Parteivorsitzenden in einem zweistufigen Verfahren. Eine Gesetzesänderung im Oktober 2020 ermöglichte die Durchführung der sogenannten digitalen Vorauswahl. Nach der erfolgten digitalen Abstimmung musste das Ergebnis per Briefwahl von den Delegierten bestätigt werden.

Die Vorteile digitaler Versammlungen liegen auf der Hand: Längere Anreisen fallen weg, Partizipation und Teilhabe werden leichter ermöglicht. Wie sieht es aber mit dem Austausch abseits des regulären Programms aus? Netzwerken ist meist mindestens ebenso wichtig wie die Reden und offiziellen Programmpunkte. Dank des Einsatzes mehrerer Geräte haben sich auch hier kreative Wege gefunden. Während der Parteitag auf dem einen Gerät lief, konnten sich Teilnehmende in kleinerem Kreis über die gehörten Reden in privat organisierten Zoom-Meetings austauschen.

Zwei Stunden Cyber-Sicherheit zu Aktionärsversammlungen und sicheren Wahlen

Weitere Blickwinkel auf sichere digitale Wahlen präsentierte die ACS im März 2021 im Cyber-Sicherheits-Web-Talk. Als Gäste berichteten aus Anbietersicht Frau Anna-Maria Palzkill von der Firma POLYAS GmbH und aus Teilnehmersicht Herr Prof. Dr.-Ing. Andreas Mayer von der Hochschule Heilbronn über ihre Erfahrungen. In ihren Vorträgen und der anschließenden Diskussion sprachen sie darüber, worauf man achten sollte, damit Informationen sicher übertragen und ausgetauscht werden können, und wie die Schutzziele Integrität, Authentizität, Vertraulichkeit und Verfügbarkeit gewährleistet werden können. ■

Mit den beiden Formaten Cyber-Sicherheits-Web-Talk und CYBERSNACS – dem Podcast der Allianz für Cyber-Sicherheit – sind Sie immer auf dem neuesten Stand in Sachen Cyber-Sicherheit. Informieren Sie sich auf unserer Webseite und abonnieren Sie den Podcast – überall da, wo es Podcasts gibt.

Weitere Informationen:

Cyber-Sicherheits-Web-Talk:
https://www.allianz-fuer-cybersicherheit.de/webtalk

CYBERSNACS:
https://www.allianz-fuer-cybersicherheit.de/cybersnacs

CYBERSNACS #04: Im Gespräch mit Dr. Stefan Hennewig (CDU-Bundesgeschäftsführer):
https://cybersnacs.podigee.io/4

DAS BSI

Das BSI und Landtagswahlen

Resilienz stärken und Wahlen sicher gestalten

von Michael Amler, Referat Nationales Verbindungswesen

Das Umfeld parlamentarischer Wahlen wird immer digitaler. Damit steigt nicht nur die Bedrohungslage für die Bundestagswahl 2021. Auch bei insgesamt fünf Landtagswahlen fallen demokratische und technische Resilienz zusammen. Das BSI leistet Unterstützung – durch Webinare, Workshops und Nachtschichten.

In Zeiten, in denen demokratische Grundwerte lauthals in Frage gestellt werden, wird die Wehrhaftigkeit der Demokratie immer wichtiger. Die Wahl der Volksvertretung spielt dabei eine besondere Rolle. Sie stellt in der repräsentativen Demokratie den grundlegenden Legitimationsakt dar. Wahlen sind das Herzstück unserer Demokratie.

Obwohl der Wahlakt selbst, mit Stift und Papier, in der Wahlkabine oder mit der Briefwahl, ein höchst analoger Vorgang ist, wächst die Bedeutung des BSI für den Wahlprozess. Bürgerinnen und Bürger informieren sich vermehrt online, der Wahlkampf findet zunehmend im Netz statt, Parteien treffen sich virtuell, um ihre Programme vorzustellen und Listenplätze zu vergeben, Wahlergebnisse werden digital übermittelt und festgehalten – der digitale Raum nimmt einen immer größeren Platz im Umfeld der Wahlen ein.

Bedrohungslage und BSI-Unterstützung bei Wahlen

Die Bedrohungslage bei Wahlen ist vielseitig, und sie ist komplex. Die Angriffsszenarien reichen von Cyber-Stalking, Beschimpfungen im Netz sowie Identitäts- oder Datendiebstahl samt der medienwirksamen Veröffentlichung so erbeuteter Informationen (sogenanntes Doxing) über Störung und Sabotage durch Verschlüsselungstrojaner bis hin zur Verbreitung von Desinformation. Dementsprechend spielt auf Bundes- wie auch Landesebene neben Wahlleitung, Innenministerium und Verfassungsschutz auch das BSI zunehmend eine tragende Rolle. Denn die Digitalisierung ist nur eine Seite der Medaille – die andere nennt sich Informationssicherheit. Beide Seiten gehören untrennbar zusammen.

Das BSI leistet umfangreiche Hilfe zur Absicherung der Bundestagswahlen. Mit dem „Nationalen Verbindungswesen“ in Berlin, Hamburg, Stuttgart und Wiesbaden und der „Informationssicherheitsberatung für Länder und Kommunen“ hat das BSI die Möglichkeit, auch die zuständigen Stellen der Länder auf deren Ersuchen bei der Absicherung der Wahlen zu unterstützen – ganz im Sinne eines kooperativen und komplementären Ansatzes. Denn Informationssicherheit kann hier nur gesamtstaatlich, wenn nicht gar Ländergrenzen überschreitend, erfolgreich sein.

Durch die Vorarbeiten zur Stärkung der Integrität und Verfügbarkeit des Kernwahlprozesses sowie der Erhöhung der Resilienz gegen technische Manipulationsversuche im Rahmen der Bundestagswahlen hat das BSI wertvolle Erfahrungswerte auch für Landtagswahlen gesammelt. Dieses vorhandene Fachwissen erlaubt – natürlich unter

Berücksichtigung der rechtlichen und Ressourcen-Rahmenbedingungen – ein vielfältiges Angebotspaket, aus dem sich Landeswahlleitungen, IT-Sicherheitsbeauftragte und weitere Verantwortliche das Passende heraussuchen können.

Kern der Leistungen bilden dabei Workshops, in denen die bereits bestehenden Konzepte und Absicherungsmaßnahmen für die Landtagswahl besprochen werden, das Bedrohungslagebild dargestellt wird, das Krisenmanagement vorbereitet, offene Fragen besprochen sowie Informationspakete und weitere Unterstützung angeboten werden.

Vor-Ort-Präsenz und technische Unterstützung

Wie vielfältig das Angebotsspektrum des BSI ist, haben bereits die ersten Landtagswahlen 2021 gezeigt. Beispielsweise unterstützte eine BSI-Verbindungsperson am Wahltag vor Ort im Statistischen Landesamt. Die Präsenz dauerte bis nach Mitternacht, als nach Abschluss der Auszählung aller Stimmbezirke das vorläufige Wahlergebnis verkündet wurde. Damit stand ein direkter Draht ins BSI zur Verfügung und Fachfragen wurden geklärt. Vor allem aber konnten auf diesem kurzen Weg Erfahrungswerte zu Abläufen und Sicherheitsmaßnahmen gesammelt werden. Während so einer langen Nacht, bis auch der letzte Stimmbezirk ausgezählt war, kamen teilweise auch persönliche Geschichten über selbstentwickelte und selbstgehostete Software im Zusammenhang mit den Wahlen zur Sprache.

Mithilfe sogenannter Webchecks der Veröffentlichungsseite der Wahlergebnisse konnten Verbesserungen am System vorgeschlagen werden.

Webcheck: Mit einem Webcheck des BSI wird der Sicherheitsstand der Internetpräsenz einer Behörde oder einer Institution geprüft. Hierbei werden die Tests größtenteils durch den Einsatz automatisierter Methoden über das Internet durchgeführt.

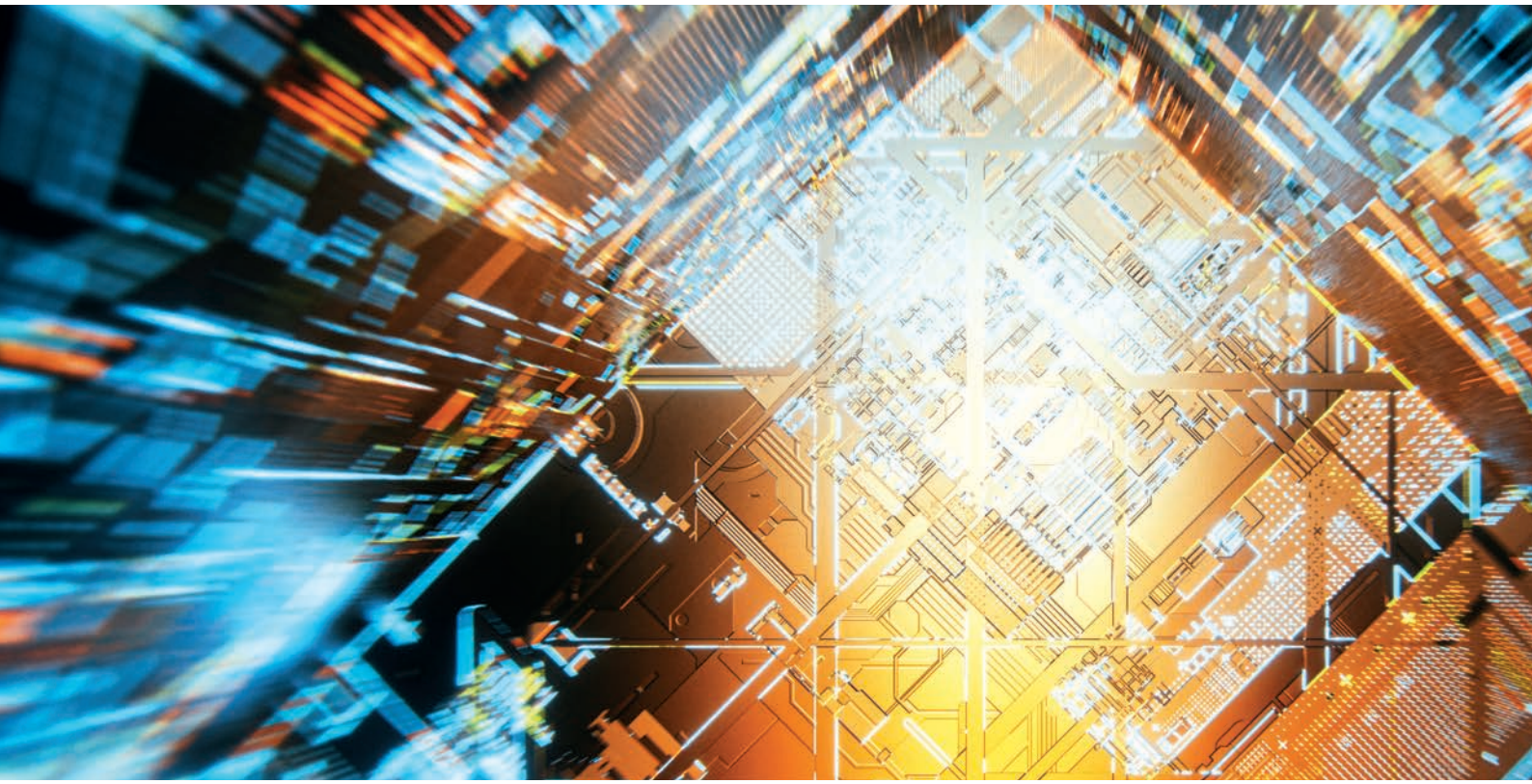
Informationssicherheit für den Wahlprozess der Schnellmeldungen

Eine der vielleicht wichtigsten BSI-Unterstützungsleistungen für die Bundes- und Landtagswahlen ist aber vermutlich der „Anforderungskatalog zur Informationssicherheit bei der Ermittlung des vorläufigen Wahlergebnisses“, der sich an die Bundes- und Landeswahlleitungen sowie Kommunen richtet. Im Auftrag des Bundeswahlleiters durch das BSI erstellt, enthält er ganz konkrete und praxisnahe Sicherheitsanforderungen, Arbeitshilfen und Checklisten, die rund um den Wahltag die Informationssicherheit bei den sog. Schnellmeldungen für das vorläufige Wahlergebnis gewährleisten können (§ 71 - Bundeswahlordnung (BWO) bei Wahlen zum Deutschen Bundestag). Darüber hinaus soll er ab Anfang 2022 zu einem IT-Grundschutz-Profil aufgewertet werden und Bund und Ländern zur Verfügung stehen.

Begleitend wurde im August in Kooperation mit dem Bundeswahlleiter eine Webinar-Serie zur „Informationssicherheit zur Absicherung des Schnellmeldeprozesses“ angeboten, an der nahezu 2.400 Teilnehmerinnen und Teilnehmer aus der Kommunalverwaltung teilnahmen – angesichts sehr heterogener IT-Strukturen und -Voraussetzungen eine große Herausforderung aus Sicht der Informationssicherheit.

Ausblick

Diese Prozesse und Leistungen reißen die Arbeit des BSI im Umfeld der Wahlen 2021 nur an. Sie ist in Bewegung und werden ständig weiterentwickelt. Denn allein im Jahr 2022 stehen erneut vier Landtagswahlen an. Das BSI möchte auch diese unterstützen und beabsichtigt, im Rahmen zukünftiger parlamentarischer Wahlen (landes- und bundesweit) die gewonnenen, gemeinsamen Erfahrungswerte zu teilen, mit Vertreterinnen und Vertretern aus den Bundesländern und den kommunalen Spitzenverbänden unter anderem weitere spezifische Webinare anzubieten und selbstverständlich auch ganz konkrete Unterstützung zu leisten. ■



Die Digitalisierung gestalten – auch im BSI

Eine Bundesbehörde stellt die Weichen für die Zukunft

von Tim Griese, Leiter der Projektgruppe Digitalisierung im BSI

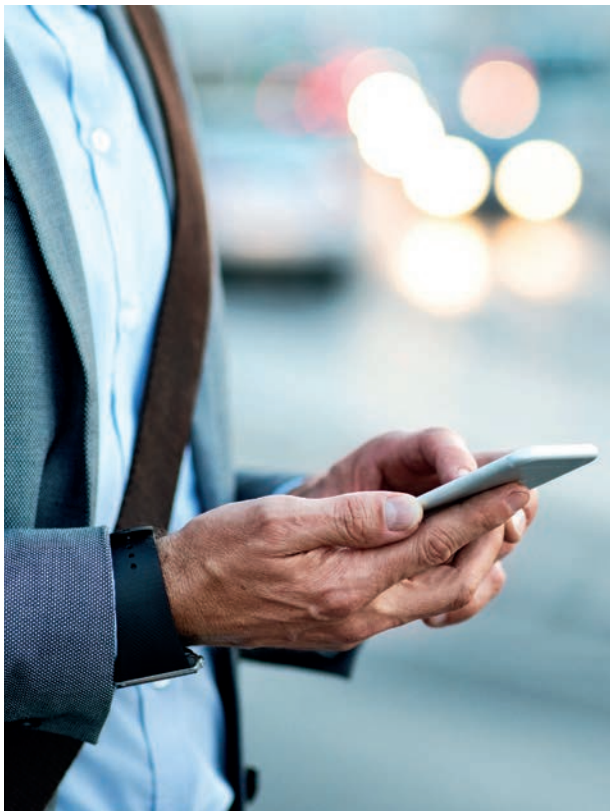
Das BSI ist die Cyber-Sicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland. Diese Rolle hat die Legislative mit dem 2021 in Kraft getretenen IT-Sicherheitsgesetz 2.0 nochmal ausdrücklich gestärkt und erweitert. Aber auch schon zuvor hat das BSI aufgrund der stetig wachsenden Bedeutung der Digitalisierung neue Aufgaben erhalten und ist personell gewachsen. Zwischen 2016 und 2021 hat sich die Zahl der Beschäftigten nahezu verdreifacht. Neue Aufgaben, Zielgruppen und personelles Wachstum bedingen auch eine Weiterentwicklung der Binnenstrukturen und Prozesse sowie des organisatorischen Aufbaus. Somit ist das BSI nicht nur in und für Deutschland der Gestalter der sicheren Digitalisierung. Auch im BSI selbst wird die Digitalisierung aktiv vorangetrieben.

Die Anforderungen, die die Zielgruppen in Staat, Wirtschaft, Forschung und Gesellschaft im Zuge der Digitalisierung an das BSI stellen, nehmen jeden Tag zu. Behörden in Bund, Ländern und Kommunen, die Politik, Unternehmen, Institutionen, Forschungseinrichtungen, Verbände sowie nicht zuletzt die Verbraucherinnen und Verbraucher erwarten vom BSI konkrete Lösungen und Hilfestellung für ihre Probleme und Herausforderungen. Fachlich anspruchsvolle Bewerberinnen und Bewerber ebenso wie alle Mitarbeitenden des BSI erwarten hochfunktionale Formen der Zusammenarbeit mit einem modernen Arbeitsplatz, der dem ausgezeichneten Ruf als einer der besten Arbeitgeber im IT-Bereich gerecht wird, den sich das BSI in den letzten Jahren erarbeitet hat.

Das BSI der Zukunft: prozessual und digital

Um diesen Erwartungshaltungen gerecht zu werden und seine Dienstleistungen in gleichbleibend hoher Qualität effizient, skalierbar und standortübergreifend zu erbringen, muss sich das BSI durchgehend prozessual und digital aufstellen. Ziel ist es, spätestens 2025 eine Behörde zu sein, die auf Basis skalierbarer, verlässlicher und digitaler Prozesse praxis- und zielgruppengerechte Angebote und Dienstleistungen bereitstellt und so ihrem gesetzlichen Auftrag ebenso wie ihrer hohen gesellschaftlichen Verantwortung umfassend nachkommt.

Bereits 2017 hat das BSI damit begonnen, vorhandene Prozesse zu dokumentieren und in einer Prozesslandkarte abzubilden, die kontinuierlich weiterentwickelt und angepasst wird – etwa, wenn das BSI neue Aufgaben erhält oder neue Rahmenbedingungen entstehen. Auf Basis der Prozesslandkarte werden die internen Abläufe stetig analysiert, mögliche Digitalisierungspotenziale erschlossen und der Wandel des BSI in eine prozess- und wirkungsorientierte Organisation vorangetrieben.



Neue Organisationsstruktur

Die Prozessorientierung spiegelt sich auch in der Organisationsstruktur des BSI wider. Die 2019 neu eingerichtete Abteilung „Technik-Kompetenzzentren“ bündelt Kompetenz und Bearbeitung zentraler, technischer Zukunftsthemen wie Künstliche Intelligenz, sichere Halbleiter oder Cloud-Computing und stellt ihre Ergebnisse den anderen Abteilungen des BSI zur Verfügung. Diese verfügen über Service-Bereiche, die den Zielgruppen des BSI in Staat, Wirtschaft und Gesellschaft zugeordnet sind und bündeln entsprechende Angebote und Dienstleistungen.

Zur Unterstützung und Beschleunigung der fortlaufenden Prozessorientierung hat das BSI 2019 eine Digitale Agenda formuliert, um vorhandene Digitalisierungspotenziale zu identifizieren und auszuschöpfen. Digitalisierung stellt mehr dar als nur die Übertragung von papierbasierten Prozessen in die digitale Welt. Sie bietet vielmehr die Chance, Abläufe neu zu denken, zu optimieren und – durch entsprechende Kennzahlen – Erfolge messbar zu machen. Zudem ermöglichen digitale Lösungen eine höhere Flexibilität und Skalierbarkeit bei der Umsetzung neuer Aufgaben oder steigender Nachfrage seitens der beteiligten Akteure und Akteurinnen. Schließlich schaffen digitale Datenbanken oder ein digitales Wissensmanagement mit hohen Synergien die Grundlage für eine standardisierte Leistungserbringung auf gleichbleibend hohem Niveau.

Effiziente, digitalisierte Prozesse zu schaffen, bedeutet an vielen Stellen zunächst ein Investment, für die Abteilungen des BSI, aber auch für viele Mitarbeitende. Am Ende aber wird sich dies auszahlen, denn die interne Digitalisierung trägt dazu bei, dass das BSI als Vorbild einer digitalen Behörde seine gesetzlichen Aufgaben noch besser erfüllen kann. Die Mitarbeitenden können sich zielgerichteter auf ihre fachlichen Aufgaben konzentrieren, damit die Abteilungen des BSI ihre vielfältigen Produkte und Dienstleistungen auch weiterhin in hoher Qualität und mit starkem Kundenfokus erbringen können. ■

BSI stärkt Präsenz und Vernetzung

Neuer Stützpunkt in Saarbrücken und neuer Dienstsitz in Freital

Das BSI hat in diesem Jahr zwei neue Liegenschaften eröffnet: Mit dem Stützpunkt Saarbrücken vernetzt sich das BSI mit dem Saarland Informatics Campus und stärkt seine Zusammenarbeit mit europäischen Institutionen. Am Standort Freital profitiert die Cyber-Sicherheitsbehörde des Bundes vom Innovationscluster der Region Dresden und kann so Synergieeffekte für ihre Arbeit nutzen.

Das BSI in Saarbrücken – ein weiterer Schritt zur Gestaltung sicherer KI-Technologie in Deutschland und Europa

Künstliche Intelligenz (KI) ist ein wesentlicher Treiber der Digitalisierung und wird zunehmend in kritischen Anwendungsfällen eingesetzt: Sei es in medizinischen Diagnose- und Prognoseanwendungen, zur biometrischen Identifikation, bei Fahrassistenzsystemen im Auto, zur Betrugserkennung in der Finanzwirtschaft oder beim Betrieb von autonomen Landwirtschaftsmaschinen. Bei diesen und vergleichbaren Anwendungen spielen Sicherheitsaspekte eine wichtige Rolle. Das BSI begleitet diese dynamische Entwicklung aktiv und konstruktiv mit dem Ziel, die Nutzung von KI-Technologien in Deutschland und Europa so sicher wie möglich zu gestalten. Seit dem 14. Juni 2021 ist das BSI mit einem neuen Stützpunkt in Saarbrücken vertreten. Die 30 geplanten Stellen dort sollen die Arbeiten der Behörde im Bereich der Künstlichen Intelligenz weiter intensivieren. Die Stadt ist ein Standort mit einer Vielzahl von hochgradigen wissenschaftlichen Instituten und Forschungseinrichtungen im Bereich der IT-Sicherheit und der Künstlichen Intelligenz und bietet aufgrund der geografischen Lage ideale Voraussetzungen für eine intensive Zusammenarbeit mit europäischen Partnern.

BSI-Präsident Arne Schönbohm bringt es auf den Punkt: „Wir finden in Saarbrücken beste Voraussetzungen für unsere Arbeit an einem Top-Thema der Gegenwart: Künstliche Intelligenz. Als Cyber-Sicherheitsbehörde des Bundes vernetzen wir uns ganz bewusst mit der nationalen Forschungslandschaft. Darüber hinaus ist Saarbrücken ein idealer Standort, um unsere Zusammenarbeit mit europäischen Institutionen, Organen und Staaten weiter zu intensivieren. Das BSI verfolgt das klare Ziel, eine

weltweit führende Rolle bei der Gestaltung von sicheren KI-Systemen aufzubauen. Wir freuen uns über unseren neuen Stützpunkt und die Chancen, die sich hier für das BSI ergeben. Der saarländischen Landesregierung danke ich ausdrücklich für die hervorragende Unterstützung bei der Ansiedlung in dieser schönen Stadt!“

Das BSI in Freital – neuer Dienstsitz in Sachsen

Am 1. Juli 2021 feierten Bundesinnenminister Horst Seehofer, der sächsische Innenminister Prof. Dr. Roland Wöller, der Freitaler Oberbürgermeister Uwe Rumberg, der Landrat Michael Geisler und BSI-Präsident Arne Schönbohm die Eröffnung des zweiten Dienstsitzes des BSI in Freital. Das Silicon Saxony – so wird die Region Chemnitz-Freiberg-Dresden inzwischen genannt – hat sich in den vergangenen Jahren zu einem der wichtigsten Standorte der Chipindustrie entwickelt. Im Bereich der Mikroelektronik gehört die Region in Sachsen zu den bedeutendsten in Europa.

Digitalisierung und Informationssicherheit gehören untrennbar zusammen

Große Industrieunternehmen und neue Forschungseinrichtungen haben sich in der Region angesiedelt und kreieren so ein neues Zentrum der Digitalisierung in Deutschland. Als zentrales Kompetenzzentrum für Informationssicherheit gestaltet das BSI die sichere Digitalisierung in Deutschland. Der Schwerpunkt der Arbeit, die in Freital geleistet wird, liegt vor allem in der Entwicklung von sicherem 5G, dem Digitalen Verbraucherschutz sowie der Einführung des IT-Sicherheitskennzeichens. Dieses sorgt in Zukunft für mehr Tranzparenz bei grundlegenden Sicherheitseigenschaften digitaler Produkte für Verbraucherinnen und Verbraucher. Freital bietet ideale Voraussetzungen, nicht nur die Entwicklung der Technik, sondern auch die IT-Sicherheit der Zukunft eng zu begleiten. Weitere Schwerpunkte in Freital sind außerdem Penetrationstests und die technische Analyse. Auch das BSI Service-Center wird in Zukunft aus Freital betrieben. Der sächsische Innenminister Prof. Dr. Roland Wöller sagt dazu: „Notwendige Voraussetzung für die erfolgreiche Digitalisierung ist ein hoher Standard in der Informationssicherheit, gerade wenn unsere eigene Sicherheit hiervon abhängt. Auch der digitale Verbraucherschutz ist ein wichtiges Thema, welches jeden angeht. Genau hieran wird in der Cyber-Sicherheitsbehörde bei uns in Freital im Landkreis Sächsische Schweiz-Osterzgebirge täglich gearbeitet.“

Eine neue Perspektive für Arbeitnehmerinnen und Arbeitnehmer

Durch den neuen Dienstsitz des BSI in Freital wird eine Symbiose geschaffen, von der alle profitieren – das trifft nicht nur auf den Bereich der Cyber-Sicherheit zu. Die Bundesregierung verfolgt das Ziel, Neuansiedlungen von Behörden bevorzugt in strukturschwachen bzw. vom Strukturwandel betroffenen Regionen vorzunehmen. Mit der Ansiedlung hochwertiger Arbeitsplätze wird ein Beitrag zur Sicherstellung gleichwertiger Lebensverhältnisse und für die Zukunft ländlicher Regionen geleistet. „Nur durch strukturelle Veränderungen wie diese, kann der Staat gewährleisten, dass die Menschen dort, wo sie leben wollen, auch leben können“, sagte Bundesminister Seehofer bei der Eröffnung. „Eine solche Strukturpolitik ist wirklich ein Dienst für die Menschen in dieser Region.“

Saarländischer Ministerpräsident Tobias Hans und BSI-Präsident Arne Schönbohm

Sächsischer Staatsminister des Innern, Prof. Dr. Roland Wöller, Bundesminister des Innern, für Bau und Heimat, Horst Seehofer und BSI-Präsident, Arne Schönbohm

Der neue Standort sorgt nicht nur für mehr IT-Sicherheit in Deutschland – sondern auch für Beschäftigung in der Region. Bisher sind 205 Arbeitsplätze für die neue Liegenschaft geplant. Dazu sagt BSI-Präsident Arne Schönbohm: „Wenn der BSI-Standort in Freital einen Beitrag zum Gedeihen dieses Ökosystems in der gesamten Region leistet, freut mich das für den Technologie-Standort Deutschland, für das Silicon Saxony als wichtigsten Standort der Chipindustrie in unserem Land und natürlich für das BSI.“ Auch für junge Menschen schafft das BSI in Freital eine wichtige Perspektive, wie der Freitaler Oberbürgermeister Uwe Rumberg herausstellt: „Besonders nach 1990 hatten viele Städte einen immensen Bevölkerungsschwund zu verkraften – durch den neuen Standort können junge Menschen hier wieder eine neue Perspektive finden.“ So aufgestellt kann das BSI heute und in Zukunft den technologischen Wandel der IT begleiten und sicherstellen. ■

Gute Verbesserung

Mitgestaltung bei neuen Wegen mithilfe der Mitarbeitendenbefragung

von Anna Breise, Referat Personalentwicklung

„Ohne unsere Mitarbeitenden gibt es kein leistungsstarkes BSI. Daher ist es wichtig, dass sie gerne und gesund ihrer Arbeit nachgehen können. Die MAB bietet eine hervorragende Möglichkeit, sich aktiv, sowohl offen als auch anonym, an der Ausgestaltung der Zukunft des BSI zu beteiligen."

– Vizepräsident des BSI, Dr. Gerhard Schabhüser

„Nichts ist beständiger als der Wandel" – dieses Motto beschreibt mehr als treffend das Umfeld, in dem sich das BSI als Cyber-Sicherheitsbehörde bewegt. Mit den rasanten Entwicklungen der Digitalisierung verändern sich auch die Ansprüche an die IT-Sicherheit. Für das BSI ist dieser Wandel mit neuen Aufgaben, aber auch Verantwortlichkeiten verbunden. Gleichzeitig steht das BSI im Wettbewerb um die besten Köpfe, also um Bewerberinnen und Bewerber, die bestimmte Vorstellungen an einen modernen Arbeitsplatz mitbringen. Mit den Auswirkungen dieser Herausforderungen auf die Zusammenarbeit, das Wohlbefinden und die Arbeitsfähigkeit der Mitarbeitenden setzt sich das BSI aktiv auseinander, denn motivierte Menschen bilden das Rückgrat der Organisation.

Bei der strukturierten und ganzheitlichen Begleitung dieser Entwicklungen hilft die Mitarbeitendenbefragung (MAB). Bei der Befragung im November 2020 wurden den Mitarbeitenden nicht nur Fragen im obligatorischen Rahmen der Psychischen Gefährdungsbeurteilung gestellt, sondern darüber hinaus viele weitere kulturelle Aspekte abgefragt.

Beim MAB-Prozess, der aus der Personalentwicklung gesteuert wird, sind drei Aspekte besonders wichtig:

1. Partizipation: Das Potential unserer Beschäftigten wird voll ausgeschöpft und Raum für Beteiligung geschaffen.
2. Ganzheitlichkeit: Die Themen werden in Beziehungen und in einem vernetzten System miteinander gesehen.
3. Transparenz: Die Kommunikation wird auf unterschiedlichen Kanälen über Hierarchieebenen hinweg offen und zielgruppenorientiert gestaltet.

Partizipation – die Zukunft des BSI mitgestalten

Unsere Arbeit, schon die reine Arbeitszeit, nimmt einen großen Teil des Lebens ein. Allein das sollte für alle Mitarbeitenden Grund genug sein, die Rahmenbedingungen aktiv mitzugestalten. Schließlich betreffen die Themen rund um Gesundheit und Arbeitszufriedenheit Mitarbeitende sowie Führungskräfte gleichermaßen – unabhängig von Aufgabe, Standort oder Alter. Die Meinung und die Meinungsvielfalt der Beschäftigten sind für das BSI daher besonders wichtig. Deshalb wurde jede Phase der MAB unter möglichst breiter Beteiligung gestaltet. Seit der Vorbereitung der MAB gab es eine Arbeitsgruppe mit Vertretungen der Fachabteilungen und Gremien. In mehreren Vertiefungsworkshops konnten Teilnehmende über die Herausforderungen sprechen und gleichzeitig Ideen für Lösungsansätze einbringen. Mithilfe von Videokonferenzen und digitalen Boards ließen sich trotz der Arbeit aus dem Home-Office effektive und interaktive Gruppenarbeiten organisieren.

„Die Ergebnisse der Mitarbeitendenbefragung sind für uns ein wertvoller Input für die Ausgestaltung des New Normal, um zu verstehen, wie unsere Mitarbeitenden zukünftig arbeiten wollen. Die Bedürfnisse unser Mitarbeitenden zu kennen, ist für uns ein wichtiger Aspekt, um als Arbeitgeber attraktive Arbeitsbedingungen zu bieten."

Dr. Ildiko Knaack, ständige Vertreterin der Abteilungsleitung Z

82 %
haben an der **MAB** teilgenommen

84% **können ARBEIT- & PRIVATLEBEN vereinbaren**

87% finden das BSI leistet einen wichtigen Beitrag für die **Gesellschaft**

83% KÖNNEN MIT IHRER FÜHRUNGSKRAFT ÜBER ARBEITSPROBLEME SPRECHEN

86% können sich auf ihre **KOLLEGINNEN UND KOLLEGEN** verlassen

83% **würden das BSI als Arbeitgeber weiterempfehlen**

„Ein wertschätzendes Miteinander und eine Führungskultur, die auf allen Ebenen gekennzeichnet ist von Transparenz, Innovation und Verantwortungsübernahme ist die Basis für den Erfolg des BSI als Gestalter der Informationssicherheit in der Digitalisierung. Die Ergebnisse der MAB fließen daher natürlich auch in den bereits 2019 gestarteten Prozess zur Weiterentwicklung unserer Führungskultur ‚Führung@BSI_2025' ein. Wir können gezielt dort ansetzen, wo es ‚drückt', aber auch das bereits vielfach Gute noch besser machen."

Anke Gaul, Referatsleiterin Personalentwicklung

Ganzheitlichkeit – Gemeinsam aufs Ganze gehen

Neben vielen positiven Ergebnissen, wie einer hohen Sinnstiftung und Identifikation mit dem BSI, einer kollegialen Atmosphäre sowie einer guten Vereinbarkeit von Beruf und Privatem, ließen sich auch Handlungsfelder, wie zum Beispiel das Thema Arbeitsverdichtung, identifizieren. Durch die Befragung wurde deutlich, dass sich die Organisation bei vielen Themen bereits auf dem richtigen Weg befindet und bereits Lösungsmaßnahmen initiiert, wie beim Wissensmanagement. Auf andere Themen konnte mit der MAB ein neuer Blick ermöglicht werden: so wurden auch aktuelle Entwicklungen mit einbezogen, wie zum Beispiel das Arbeiten im BSI unter Corona-Bedingungen. Fakt ist: Singuläre Lösungen können im Wandel nur bedingt wirken. Bei der Entwicklung von Maßnahmen kommt es daher darauf an, einen ganzheitlichen Blick auf das BSI zu werfen und zu erkennen, an welchen Stellen die Erkenntnisse aus der MAB mit laufenden oder geplanten Aktivitäten verzahnt werden sollten. Die nachhaltige Wirkung solcher Maßnahmen entfaltet sich durch Synergieeffekte zwischen den Themen.

Transparent – wieso, deshalb, darum

Den Überblick über die Themen und die Verzahnung zu behalten, ist nicht leicht. Eine klare und kontinuierliche Kommunikation rund um den MAB-Prozess ist kritisch für den Erfolg, wenn es um nachhaltige Verbesserung geht. Das Ziel war und bleibt es, alle Mitarbeitenden bei der MAB-Reise mit auf den Weg zu nehmen. Mit der Kampagne „100 gute Gründe für die MAB" sollte schon vor dem Start der MAB zusammengefasst werden, was die Belegschaft wirklich bewegt und worauf es für sie bei der Befragung ankommt. Berichte in den internen BSI-News, im Wiki sowie Videobotschaften der Amtsleitung haben gezeigt, dass die Rückmeldungen der Mitarbeitenden ernst genommen und verarbeitet werden. Gleichzeitig ist es wichtig zu vermitteln, dass auch Teams und auch der oder die Einzelne Einfluss auf ihr Umfeld nehmen und Veränderungen bewirken können.

Lage der IT-Sicherheit in Deutschland 2021

Im Berichtszeitraum vom 1. Juni 2020 bis zum 31. Mai 2021

Mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland legt das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die Cyber-Sicherheitsbehörde des Bundes jährlich einen umfassenden und fundierten Überblick über die Bedrohungen im Cyber-Raum vor.

IT-Sicherheitslage bleibt angespannt bis kritisch

Auch in diesem Jahr steht der Bericht unter dem Eindruck der COVID-19-Pandemie. Sie hat mit ihren gesamtgesellschaftlichen Auswirkungen auch Folgen für die Arbeitssituation in praktisch allen Behörden, Organisationen und Unternehmen. Unter anderem mit der enormen Zunahme der Arbeit im Homeoffice haben sich neue Herausforderungen für die Informationssicherheit ergeben. Im Bereich Malware stieg die Anzahl der Schadprogramm-Varianten zeitweise rasant an. Bis zu 553.000 neue Varianten an nur einem Tag war der höchste, jemals gemessene Wert. Beherrschendes Thema bleibt darüber hinaus die zunehmende Bedrohungslage durch Ransomware.

Cyber-Erpressungen entwickeln sich zur größten Bedrohung

Das vergangene Jahr war geprägt von einer deutlichen Ausweitung cyber-krimineller Erpressungsmethoden. So verschlüsseln Cyber-Kriminelle Daten von Unternehmen und Institutionen in ausgefeilten mehrstufigen Angriffen, um Lösegeld zu erpressen. Auch wenn es im Januar 2021 gelang, die Infrastruktur der Schadsoftware Emotet zu zerschlagen, ist die Gefahr nicht gebannt. Der Lagebericht zeigt deutlich, wie Cyber-Kriminelle ihre Angriffsmethoden weiterentwickeln und wie schädlich Ransomware-Angriffe für eine betroffene Organisation sein können. Auch haben DDoS-Angriffe weiter an Intensität und Zahl zugenommen und werden für Erpressungen genutzt.

Schwachstellen als eine der größten Herausforderungen

Schwachstellen in Hard- und Software-Produkten sind und bleiben eine der größten Herausforderungen der Informationssicherheit. Cyber-Kriminelle sind aufgrund ihrer technischen Möglichkeiten dazu fähig, Schwachstellen auszunutzen – in vielen Fällen ohne weiteres Zutun der Anwenderinnen und Anwender. Eine im März 2021 geschlossene Lücke in Exchange-Servern von Microsoft steht dabei sinnbildlich für das Ausmaß der Herausforderung. Direkt nach Bekanntwerden der Lücke wurden großflächig Versuche beobachtet, verwundbare Exchange-Server aufzuspüren und zu kompromittieren. Das BSI hat in diesem Zusammenhang erst zum dritten Mal in seiner Geschichte die zweithöchste IT-Krisenstufe ausgerufen. Der hohe Anteil detektierter verwundbarer Server von 98 Prozent konnte nach zwei Wochen auf unter zehn Prozent gesenkt werden. Jedoch können bestehende Kompromittierungen noch Wochen oder Monate später zu Cyber-Angriffen mit Schadenswirkung führen.

Der Faktor Mensch

Nach wie vor eine wichtige Rolle spielt der Faktor Mensch als Einfallstor für Angriffe. Die Unsicherheit und Überforderung durch die COVID-19-Pandemie, der reale und empfundene Zeitdruck sowie die gesellschaftliche und mediale Dominanz des bestimmenden Themas wurden im Berichtszeitraum von Kriminellen ausgenutzt, um Opfer durch Phishing-Angriffe und andere Betrugsformen zur Herausgabe sensibler Informationen oder personenbezogener Daten zu bewegen. Daten-Leaks, Cyber-Angriffe auf Videokonferenzen, schlecht abgesicherte VPN-Server oder der Einsatz privater IT im beruflichen Kontext führten zudem ebenso zu Sicherheitsvorfällen wie langfristig und mit großem Aufwand geplante Angriffe auf einzeln ausgewählte, herausgehobene Ziele. Auch DDoS-Attacken, Schwächen in

RANSOMWARE/DDOS

Deutliche Ausweitung cyber-krimineller Erpressungsmethoden

+ 360 % Daten-Leak-Seiten

Schweigegeld-Erpressung

Lösegeld-Erpressung

Schutzgeld-Erpressung

Neuer Trend

144 MIO. neue Schadprogramm-Varianten

+22 % gegenüber 2020: **117,4 MIO.**

DURCHSCHNITTLICH **394.000** neue **Schadprogramm-Varianten** pro Tag

2020: 322.000

IM HÖCHSTWERT **553.000**

2020: 470.000

kryptografischen Verfahren oder hybride Bedrohungen durch fremde Staaten und deren Proxies sorgten für Sicherheitsvorfälle.

Die Digitalisierung scheitert ohne Cyber-Sicherheit

Die Entwicklungen der vergangenen zwölf Monate belegen, dass die Bedrohung durch Cyber-Kriminelle für die digitale Gesellschaft und die vernetzte Arbeitswelt weiter ansteigt. Mit der Verabschiedung des IT-Sicherheitsgesetzes 2.0 im April 2021 wurde das BSI weiter gestärkt und mit zusätzlichen Kompetenzen bei der Detektion von Sicherheitslücken und bei der Abwehr von Cyber-Angriffen ausgestattet. Der Gesetzgeber misst der Cyber- und Informationssicherheit in Deutschland damit eine höhere Bedeutung zu und hat zugleich die Voraussetzungen für eine sichere Digitalisierung geschaffen. Diesen Weg gilt es, konsequent weiter zu beschreiten.

Dem gegenüber steht jedoch die rasante Entwicklung im Bereich der Cyber-Bedrohungen, die durch eine zunehmende Vernetzung noch begünstigt wird. So bringt die Digitalisierung mit all ihren Chancen und Möglichkeiten auch viele Gefahren und eine wachsende Angriffsfläche mit sich. Aus diesem Grund muss die Digitalisierung neu gedacht werden. Informationssicherheit muss einen deutlich höheren Stellenwert einnehmen und zur Grundlage aller Digitalisierungsprojekte werden. Der Bericht zur Lage der IT-Sicherheit in Deutschland 2021 zeigt deutlich wie nie, dass es eine erfolgreiche Digitalisierung von Staat, Wirtschaft und Gesellschaft nur mit einem richtigen Maß an Cyber-Sicherheit geben wird. ■

Weitere Informationen:

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

12 Monate Cyber-Sicherheit im Überblick

Juni

- Vereinbarung zwischen BSI und Verbraucherschutzzentrale
- BSI bringt das Thema Cyber-Sicherheit in deutsche EU-Ratspräsidentschaft ein
- Vorstellung der Corona-Warn-*App*
- BSI und VDA: Gemeinsam für mehr Cyber-Sicherheit im Auto

Juli

- BSI veröffentlicht Prüfspezifikationen für Breitband-Router
- BSI wirkt an europäischem Standard für vernetzte Geräte im Smart Home mit
- Nachweis von Sicherheitsmängeln in der Telematik-Infrastruktur durch Fehlkonfigurationen

August

- Argentinien: Ransomware-Angriff bei Einwanderungsbehörde mit Abfluss von Passdaten
- Neuseeland: Erpressungsversuch via *DDoS-Angriffen* auf die Börse NZX
- Erpressungsversuche via *DDoS*-Angriffen im Finanzsektor und auf Bezahldienstleister
- Sicherheitsanforderungen für Telekommunikationsnetze veröffentlicht
- Handlungsempfehlungen zur Migration zu Post-Quanten-Kryptografie aktualisiert

September

- *Ransomware*-Angriff auf Universitätsklinikum in NRW
- EvilQuest: Schadsoftware, die sich gegen Apples Betriebssystem MacOS richtet
- *DDoS*-Erpressungen bei Internet-Service-*Providern* (auch Oktober)
- Erfolgreiches BSI-Team bei der Krypto-Konferenz CHES-Challenge
- BSI und EASA für mehr Cyber-Sicherheit in der Luftfahrt
- BSI und ProPK veröffentlichen Digitalbarometer 2020
- Start des BSI-Podcasts „Update verfügbar“

Oktober

- Cyber-Erpressung mit Sextortion-Kampagne
- BSI und Kraftfahrt-Bundesamt: Verwaltungsvereinbarung für Cyber-Sicherheit im Automotive-Bereich
- Veröffentlichung der Cyberfibel durch BSI und Deutschland sicher im Netz e. V.
- ECSM: Livestream-Reihe mit der Bundezentrale für politische Bildung zu Cyber-Sicherheit, Desinformation und *Deepfakes*
- BSI veröffentlicht „Leitfaden für Ihr virtuelles Event“
- BSI veröffentlicht Sicherheitsanforderungen für Online-Sozialwahlen

November

- *Ransomware*-Angriff auf Flughafen Saarbrücken
- Offizielle Cyber-Sicherheitskonferenz der deutschen EU-Ratspräsidentschaft durch BMI und BSI
- Symposium „Digitalisierung, Cyber-Sicherheit & Ich-Perspektiven im Gesundheitswesen“ am Universitätsklinikum Bonn
- Kooperationsvereinbarung zwischen BSI und Fraunhofer IAIS zur gemeinsamen Entwicklung von Prüfverfahren

2020

Globale *DDoS*-Erpressungskampagne

2021

Dezember

- Cyber-Angriff auf Europäische Arzneimittelagentur EMA
- *Ransomware*-Angriff auf große deutsche Mediengruppe
- USA: APT-Angriff auf Monitoring-Anbieter SolarWinds
- Beschluss der Informationssicherheitsrichtlinie IT-Konsolidierung Bund
- Informationssicherheitsbeauftragter für die IT-Konsolidierung Bund ernannt
- Erste Version der Normungsroadmap Künstliche Intelligenz auf Digital Gipfel vorgestellt

Januar

- Infrastruktur der Schadsoftware Emotet zerschlagen
- Cyber-Erpressung mit Sextortion-Kampagne
- Bundeskartellamt und BSI: Gemeinsam für digitalen Verbraucherschutz
- Draft des neuen BSI-Standards 200-4 zum Business Continuity Management veröffentlicht

Februar

- Höchster jemals gemessener durchschnittl. Tageszuwachs an neuen Schadprogramm-Varianten: 553.000
- „Smishing“ SMS-*Phishing*-Nachrichten mittels Android-Schadprogramm MoqHao
- BSI veranstaltet 17. Deutschen IT-Sicherheitskongress erstmalig digital
- Veröffentlichung des Kriterienkatalogs für KI-basierte *Cloud*-Dienste (AIC4)

März

- Sicherheitsupdate für Schwachstellen auf Exchange-Servern von Microsoft
- Cyber-Erpressung mit Sextortion-Kampagne
- BSI veröffentlicht „Mindeststandard für Videokonferenzdienste“
- Start der BMI-BSI-Kampagne #einfachaBSIchern

April

- Verabschiedung des IT-Sicherheitsgesetzes 2.0
- *Deepfake*-Manipulation: Erfolgreiche Täuschung mehrerer europ. Politiker
- EU-Kommission und 18 weitere Staaten: Erfolgreiche Einbindung der Online-Ausweisfunktion in eID-Schema
- Start des Projekts eMergent zur Digitalisierung im Rettungsdienst
- Allianz für Cyber-Sicherheit knackt die 5.000-Teilnehmer-Marke
- Vorstellung der Ergebnisse der BSI-Wirtschaftsumfrage zum Homeoffice

Mai

- USA: Cyber-Angriff (Darkside) auf IT-Infrastruktur des Pipeline-Betreibers Colonial Pipeline Company
- Belgien: *DDoS*-Angriff auf einen großen Internet-*Provider*
- Cyber-Erpressung mit Sextortion-Kampagne
- *UP KRITIS*: 750 Organisationen sind Teilnehmer der Plattform
- IT-SiG 2.0 tritt in Kraft

Das IT-Sicherheitsgesetz 2.0

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

von Dr. Martin Hecheltjen, Referat IT-Sicherheit und Recht

„Wir wollen das BSI als nationale Cyber-Sicherheitsbehörde ausbauen und in seiner Rolle als unabhängige und neutrale Beratungsstelle in Fragen der IT-Sicherheit stärken."

Diesen Auftrag gaben sich die Regierungsparteien der großen Koalition in ihrem Koalitionsvertrag vom 07.02.2018. Anfang 2019 kündigte Bundesinnenminister Horst Seehofer daraufhin ein neues IT-Sicherheitsgesetz 2.0 an. Bis zur Vorlage einer finalen Fassung in Bundestag und Bundesrat und dem Inkrafttreten des Gesetzes sollten jedoch noch gut drei Jahre vergehen, in denen fachlich und politisch um den konkreten Inhalt des Gesetzes gerungen wurde. Die langen und technisch komplexen Diskussionen auf allen Ebenen und das große Interesse der Öffentlichkeit an den neuen Regelungen verdeutlichen, dass IT-Sicherheit kein Spezialbereich technisch versierter IT-Fachkräfte mehr ist. Durch die voranschreitende Digitalisierung ist das Thema in der Mitte der Gesellschaft angekommen. Nicht zuletzt durch die große Anzahl von IT-Sicherheitsvorfällen in den letzten Jahren und deren Auswirkungen auf eine Vielzahl von Bürgerinnen und Bürgern und Unternehmen ist deutlich geworden, dass eine erfolgreiche Digitalisierung nur gelingen kann, wenn Politik, Wirtschaft und Gesellschaft das Thema IT-Sicherheit stets mit im Blick behalten.

Das nun vorliegende IT-Sicherheitsgesetz 2.0 ist die umfassendste Erweiterung des BSI-Gesetzes seit seiner Novellierung im Jahr 2009. Es stellt einen wesentlichen Schritt für die Stärkung der Netz- und Informationssicherheit in Deutschland dar. Die Aufgaben und Befugnisse des BSI werden in nahezu all seinen Tätigkeitsfeldern in den Bereichen Staat, Wirtschaft und Gesellschaft erweitert oder jedenfalls geschärft.

Das BSI ist die zuständige Stelle für Informationssicherheit auf nationaler Ebene.

Das BSI gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion. Es hat sich, seit seiner Gründung 1991, von einem IT-Sicherheitsdienstleister des Bundes zu einem ressortübergreifenden Kompetenzzentrum für Fragen der Informationssicherheit in Staat, Wirtschaft und Gesellschaft entwickelt. Diese konstante Weiterentwicklung der vielfältigen Aufgaben des BSI findet seinen Niederschlag nun auch ausdrücklich in § 1 BSIG-Gesetz, wonach das BSI „die zuständige Stelle für die Informationssicherheit auf nationaler Ebene" ist.

Verbraucherschutz und IT-Sicherheitskennzeichen
Neben dem Schutz der Kommunikationstechnik des Bundes und der Aufsicht über Kritische Infrastrukturen gehörte die Beratung und Warnung von Bürgerinnen und Bürgern in Fragen der IT-Sicherheit schon vor 2021 zu den Aufgaben des BSI. Durch die neue gesetzliche Aufgabe „Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik" ist es dem BSI möglich, zukünftig einen noch stärkeren Fokus auf Verbraucherschutzthemen im Bereich der IT-Sicherheit zu legen. Mit Blick auf die zunehmende Vernetzung von IT-Produkten des Alltags sind die Informationen von Verbraucherinnen und Verbrauchern und die Erarbeitung von grundlegenden Anforderungen an die IT-Sicherheit zum Zweck des Schutzes von Verbraucherinnen und Verbrauchern unerlässliche Bausteine für die Förderung der IT-Sicherheit in Deutschland.

Eine im Kontext Verbraucherschutz erste konkrete Maßnahme des BSI wird die Vergabe von IT-Sicherheitskennzeichen sein. Gemäß § 9c BSIG kann das BSI Verbraucherinnen und Verbraucher mit diesem IT-Sicherheitskennzeichen über die IT-Sicherheit von Produkten bestimmter vom Bundesamt festgelegter Produktkategorien informieren.

Das Kennzeichen ist zweiteilig aufgebaut: Es besteht aus einer Herstellererklärung über bestimmte IT-Sicherheitsanforderungen und einer Sicherheitsinformation des BSI über sicherheitsrelevante IT-Eigenschaften. Die Kombination dieser Informationen auf einem einheitlichen IT-Sicherheitskennzeichen wird den Verbraucherinnen und Verbrauchern im Rahmen ihrer Kaufentscheidung ermöglichen, transparent, aktuell und unkompliziert den Aspekt der IT-Sicherheit bei Produkten oder auch Dienstleistungen im IT-Bereich mit zu berücksichtigen.

Schutz der Bundesverwaltung verbessert
Auch der Schutz der Bundesverwaltung durch das BSI wird mit den neuen Regelungen des IT-Sicherheitsgesetzes 2.0 deutlich verbessert.

Durch den neuen § 4a BSIG erhält das BSI den Auftrag, die Kommunikationstechnik des Bundes zu kontrollieren. Diese neue Regelung stärkt die Rolle des BSI als zuständige Stelle für IT-Sicherheit innerhalb der Bundesverwaltung. Außerdem ermöglicht sie dem BSI die aktive Förderung eines einheitlich hohen Sicherheitsniveaus bei den IT-Systemen des Bundes.

Ergänzt werden diese Kontrollbefugnisse durch die Aufgabe des BSI, im Benehmen mit den Ministerien, verbindliche Mindeststandards für die Sicherheit der Informationstechnik des Bundes festzulegen. Gemeinsam mit den Ressorts kann so ein grundlegendes und flächendeckend hohes IT-Sicherheitsniveau etabliert werden.

Ergänzend zu diesen präventiven Befugnissen wurden die Möglichkeiten des BSI zur Erkennung und Abwehr von IT-Angriffen auf Regierungsnetze erweitert. Die Angriffsmetoden sind in den letzten Jahren immer

komplexer und vielfältiger geworden. Die Analyse vergangener Angriffe innerhalb der Bundesverwaltung hat gezeigt, dass sich insbesondere spezialisierte Cyber-Angriffe – sog. „Advanced Persistent Threats (APT)“ – über einen mehrjährigen Zeitraum erstrecken können. Um der unterschwelligen Vorgehensweise, die solchen Angriffen immanent ist, effektiv begegnen und später entdeckte Kompromittierungen entfernen zu können, wurde die Speicherdauer der Protokolldaten der Kommunikationstechnik des Bundes auf 18 Monate erweitert. Zudem erhält das BSI eine ergänzende Befugnis zur Verarbeitung behördeninterner Protokollierungsdaten, die ebenfalls zur Erkennung und Analyse laufender und der Rekonstruktion vergangener Angriffe auf die Informations- und Kommunikationstechnik des Bundes von erheblicher Bedeutung sind

Ausbau von Detektionsmaßnahmen und operativer Cyber-Abwehr

Die Analyse von Schadprogrammen und Sicherheitslücken zur Beratung und Warnung der Betroffenen stellt eine elementare Aufgabe des BSI dar. Um die Beratung und Warnung zukünftig effektiver und umfassender gestalten zu können, wurde im BSIG eine Befugnis zur Detektion und Analyse von Schadprogrammen und Angriffsmethoden ergänzt. Das BSI kann zukünftig gemäß § 7b BSIG an den öffentlichen Schnittstellen informationstechnischer Systeme des Bundes, Kritischer Infrastrukturen, digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse Detektionsmaßnahmen zur Suche nach öffentlich bekannten Sicherheitslücken durchführen. Die Ergebnisse dieser Maßnahmen dürfen – der grundlegenden Überzeugung des BSI entsprechend, dass jede Sicherheitslücke unbedingt zu schließen ist – nur zur unverzüglichen Information der Betroffenen verwendet werden.

Zudem erhält das BSI Anordnungsbefugnisse gegenüber Telekommunikations- und Telemedienanbietenden zur Abwehr spezifischer Gefahren für die Informationssicherheit. Bereits vor Inkrafttreten des IT-Sicherheitsgesetzes 2.0 hatten Serviceprovider gemäß § 109a TKG die Befugnis, im Falle einer Störung die Nutzung des Telekommunikationsdienstes einzuschränken, umzuleiten oder zu unterbinden, um hierdurch eine Beeinträchtigung zu beseitigen oder zu verhindern. Durch das IT-Sicherheitsgesetz 2.0 wird dem BSI zur Abwehr besonderer Gefahrenlagen die Möglichkeit eingeräumt, diesen bereits bestehenden Mechanismus zu nutzen, indem es Provider zur Umsetzung der jeweils erforderlichen Maßnahmen auffordert.

Im Hinblick auf Telemedienanbieter hatte das Bundesamt bislang nicht die Befugnis, diese zu Maßnahmen aufzufordern, die die angebotenen Telemediendienste unter Berücksichtigung des jeweiligen Stands der Technik in angemessener Art und Weise absichern. Durch die neue Befugnis aus § 7d BSIG ist das BSI nun in der Lage, den Betreibenden eines Telemediendienstes – z. B. einer Webseite, durch deren unzureichende Sicherung eine erhebliche Gefahr geschaffen wird – zu entsprechenden Absicherungsmaßnahmen aufzufordern. Hierdurch kann das BSI effektiv gegen Gefahren vorgehen, wie z.B. „Drive-by Downloads“ durch schadhafte Onlinewerbung vorgehen.

Erweiterung der KRITIS-Befugnisse

Durch das IT-Sicherheitsgesetz 2.0 wird der neue Adressatenkreis der Unternehmen im besonderen öffentlichen Interesse (UBI) in das BSIG eingeführt. Unter die neuen UBI-Regelungen in § 8f BSIG fallen Unternehmen aus drei unterschiedlichen Kategorien. UBI im Sinne des BSIG sind:

1. Unternehmen, die vom Anwendungsbereich des § 60 Abs. 1 Nr. 1 und 3 AWV erfasst sind (z. B. Rüstungsunternehmen, Hersteller von IT-Produkten für die Verarbeitung von Verschlusssachen).

2. Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten in Deutschland gehören oder für solche Unternehmen wegen ihrer Alleinstellungsmerkmale als Zulieferer von wesentlicher Bedeutung sind.

3. Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-VO oder diesen gleichgestellte.

Aufgrund der Art der jeweils hergestellten Güter und Produkte (Rüstung), des Umgangs mit Materialien, die ein besonders Gefahrenpotential bergen oder der volkswirtschaftlichen Schäden, die durch Cyber-Angriffe oder anderweitige IT-Störungen entstehen können, besteht ein besonderes öffentliches Interesse am Schutz dieser Unternehmen. Während die Zugehörigkeit zu den Kategorien 1 und 3 eindeutig durch den Anwendungsbereich

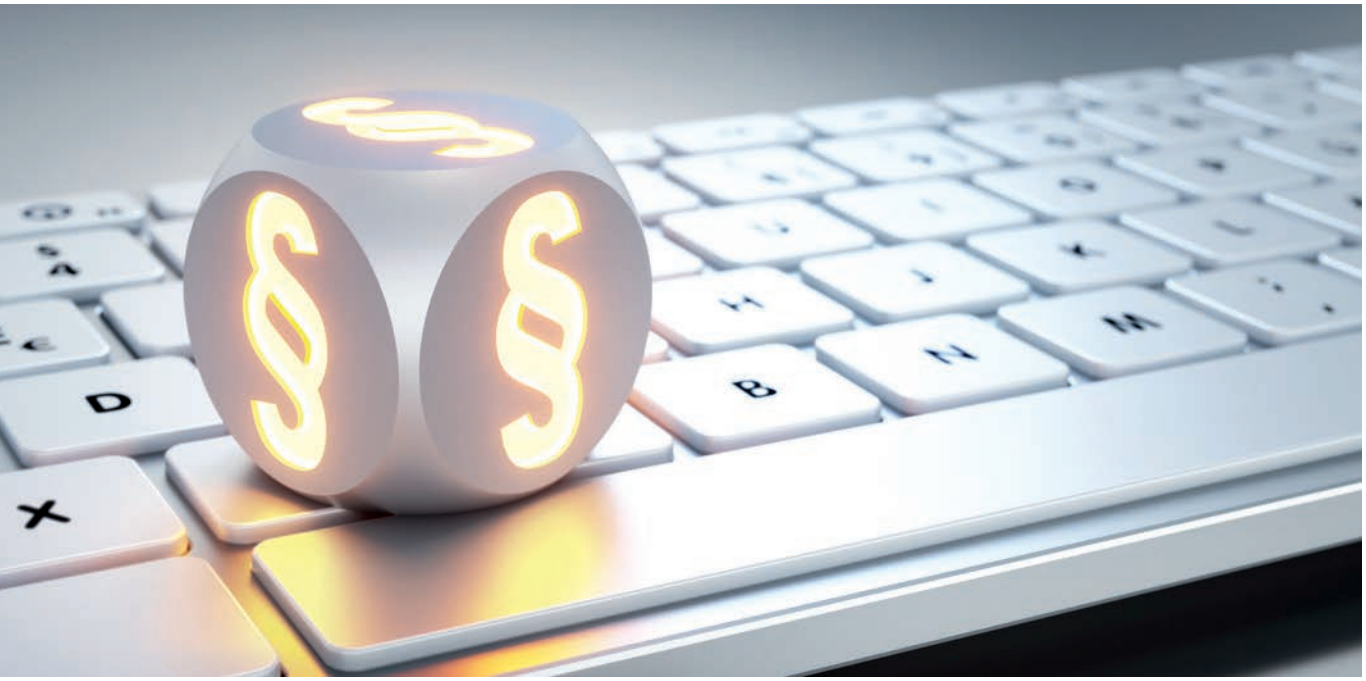
der AWV oder der Störfall-VO festgelegt wird, bedarf es für Kategorie 2 einer weitergehenden Konkretisierung, welche Unternehmen als UBI gelten sollen. Diese Konkretisierung wird durch eine entsprechende Rechtsverordnung – vergleichbar der KRITIS-Verordnung (BSI-KritisV) – umgesetzt.

Abhängig von der Zugehörigkeit zu einer der Kategorien haben die Unternehmen unterschiedliche Pflichten. Unternehmen nach Kategorie 1 und 2 haben dem BSI alle zwei Jahre eine Selbsterklärung zur IT-Sicherheit vorzulegen, aus der unterschiedliche Angaben zu Zertifizierungen im Bereich der IT-Sicherheit, zu sonstigen Sicherheitsaudits oder Prüfungen sowie zu speziellen Schutzmaßnahmen für besonders schützenswerte informationstechnische Systeme, Komponenten und Prozesse hervorgehen. Gleichzeitig müssen sich diese Unternehmen mit Vorlage der ersten Selbsterklärung beim BSI registrieren und eine Kontaktstelle benennen. Für Unternehmen der Kategorie 3 ist diese Registrierung hingegen freiwillig. Eine Meldepflicht in Bezug auf Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme trifft hingegen alle Unternehmen gleichermaßen, jedoch in einer jeweils kategoriespezifischen Ausgestaltung.

Neben der Einführung neuer Regelungen für UBI wurden die Befugnisse des BSI in Bezug auf Kritische Infrastrukturen erweitert. Zum einen wurde die Branche „Siedlungsabfallentsorgung“ als KRITIS-Sektor in das BSIG aufgenommen. Zum anderen wurde das BSI in die Lage versetzt, die Vorlage aller Unterlagen zu verlangen, die für eine Bewertung des KRITIS-Status erforderlich sind. Kommt das BSI bei dieser Untersuchung zu dem Ergebnis, dass ein Betrieb die Kriterien für eine Kritische Infrastruktur erfüllt, kann dieser Betrieb durch das BSI als KRITIS registriert werden. Durch diese neuen Maßnahmen wird das BSI in seiner Aufsichtsfunktion im Bereich Kritischer Infrastrukturen erheblich gestärkt.

Meilenstein auf dem Weg zur Digitalisierung in Deutschland

Das IT-Sicherheitsgesetz 2.0 ist ein wichtiger Meilenstein auf dem Weg zu einer erfolgreichen Digitalisierung in Deutschland, aber kein Schlusspunkt. Der Bundestag hat mit einem Entschließungsantrag zum vorliegenden Gesetz bereits erste Impulse für die Fortentwicklung der IT-Sicherheitsgesetzgebung gegeben. Und auch dem durchaus kontroversen Diskurs, der von Branchenverbänden und anderen zivilgesellschaftlichen Organisationen zu diesem Gesetz geführt wurde, sind wichtige Ansätze für die Weiterentwicklung des BSIG zu entnehmen. Zudem ist mit der NIS-Richtlinie 2.0 bereits ein Regulierungsakt auf europäischer Ebene in Abstimmung, der ebenfalls große Auswirkungen auf die deutsche Gesetzgebung zur IT-Sicherheit, insbesondere das BSIG, haben wird.



So wie die Digitalisierung unser aller Alltag fortwährend verändert, ist es notwendig, das IT-Sicherheitsrecht stetig fortzuentwickeln und an die neuen Aufgaben und Herausforderungen anzupassen. Das BSI steht mit seiner Expertise bereit, diesen andauernden Veränderungsprozess der Digitalisierung, gemeinsam mit den Partnern aus Wirtschaft und Gesellschaft zu gestalten. ■

IT-SICHERHEIT IN DER PRAXIS

Das IT-Sicherheits-kennzeichen

Informationssicherheit gestalten und Transparenz für alle schaffen

von Joshu Wiebe, Referatsleiter Erteilung von IT-Sicherheitskennzeichen

Mit Inkrafttreten des IT-Sicherheitsgesetzes 2.0 am 28. Mai 2021 hat das BSI den Auftrag erhalten, ein freiwilliges IT-Sicherheitskennzeichen einzuführen. Es soll Transparenz für Verbraucherinnen und Verbraucher schaffen, indem es vom Hersteller zugesicherte Sicherheitseigenschaften digitaler Produkte und Dienste auf einen Blick erkennbar macht und zu aktuellen Sicherheitsinformationen, wie beispielsweise Updates und Schwachstellen, informiert.

Wieso braucht der IT-Verbrauchermarkt mehr Transparenz?
Mit dem Internet vernetzte Produkte sollen unser Leben erleichtern und haben längst Einzug in unseren Alltag gehalten, zum Beispiel in Form von smarten Staubsaugern, Uhren oder Sprachassistenten. Sie sind Teil des sogenannten „Internet of Things“ (IoT), dem „Internet der Dinge“. Als selbstverständlicher Bestandteil des Haushaltes vieler Verbraucherinnen und Verbraucher werden dadurch immer mehr Bereiche des täglichen Lebens digitalisiert.

Ganz nebenbei werden dabei Daten gesammelt und mithilfe von Sensoren tiefe Einblicke in unser Privatleben ermöglicht. Normalerweise nutzen die Geräte die gesammelten Informationen nur für den Zweck, dem die Nutzenden auch zugestimmt haben. Damit kein unerwünschter Zugriff auf die Daten und Funktionen der Geräte erfolgt, müssen die Produkte durch den Hersteller mittels geeigneter Sicherheitsfunktionen geschützt und regelmäßig mit Sicherheitsupdates auf den neusten Stand gebracht werden.

Oft ist beim Einkauf von IT für Kundinnen und Kunden nur schwer nachvollziehbar, welche Sicherheitsfunktionen ein IT-Produkt besitzt oder wie lange Sicherheitsupdates zur Verfügung gestellt werden. Tatsächlich wünschen sich Verbraucherinnen und Verbraucher mehr Informationen zum Schutz von Geräten. Bei einer repräsentativen Onlineumfrage des Bundesinnenministeriums und des BSI zum Safer Internet Day 2020 gaben 77,3 % der Teilnehmenden an, dass sie einen Informationsbedarf haben.

Der Bericht zum Digitalen Verbraucherschutz des BSI informiert über die Erkenntnisse einer auf die Sicherheit von IoT-Geräten spezialisierten Firma. Im Dezember 2020 berichtete diese Firma von insgesamt 7.339 Schwachstellen in nur sechs Verbraucherprodukten: einem Smart Speaker, einem Messenger für Kinder, einer Drohne, einem Smart Home-Kamerasystem, einer Haustier-Überwachungskamera sowie einem Streaming-Gerät für Kinder. Durch veraltete Software mit bekannten Sicherheitslücken, unsichere Fernwartungszugänge und mangelhafte Verschlüsselung wurden dabei „nicht einmal grundlegende Sicherheitseigenschaften“ erfüllt.

In dieses Bild passt auch, dass bereits jede vierte Person in Deutschland Opfer von Cyber-Kriminalität geworden ist, was sich in einer vom BSI durchgeführten Befragung von Bürgerinnen und Bürgern zum Digitalbarometer 2020 zeigte. Wenig verwunderlich erscheint dabei die Erkenntnis: Wer mehr Geräte besitzt, wird auch häufiger Opfer von Cyber-Kriminalität.

Mit dem IT-Sicherheitskennzeichen adressiert das BSI diese Problemlage und erhöht die Transparenz auf dem Markt für Verbraucher-IT. Verbraucherinnen und Verbrauchern wird ermöglicht, grundlegende IT-Sicherheitseigenschaften von Produkten leicht zu erkennen und diese während der Kaufentscheidung einzubeziehen.

Wie funktioniert das IT-Sicherheitskennzeichen?
Mit dem freiwilligen IT-Sicherheitskennzeichen haben Hersteller die Möglichkeit die Konformität ihrer Produkte mit IT-Sicherheitsvorgaben zu erklären, die vom BSI für das IT-Sicherheitskennzeichen herausgegeben oder anerkannt wurden. Diese Herstellererklärung umfasst die Zusicherung, dass die Produkte nach dem zugrundeliegenden Standard geprüft wurden und dessen Anforderungen erfüllen.

Das BSI führt bei der Freigabe des IT-Sicherheitskennzeichens eine Plausibilitätsprüfung des Antrages und der Herstellererklärung durch. Dabei verschafft sich das BSI einen Eindruck darüber, ob die Angaben des Herstellers sowie dessen dargestellte Prüfverfahren und -maßnahmen nachvollziehbar und plausibel erscheinen. Soweit vorhanden, kann das BSI auch bereits bekannte Probleme mit dem Produkt (z.B. Sicherheitslücken) oder vorheriges Fehlverhalten des Herstellers (z.B. Warnungen vor Produkten) bei der Freigabe einbeziehen. Das BSI kann die Freigabe der Nutzung auch dann verweigern, wenn der Freigabe, unabhängig von den eingereichten Unterlagen, ernstliche Zweifel an der Herstellererklärung entgegenstehen.

Wichtig ist: Anders als bei einer Zertifizierung prüft das BSI im Rahmen der Freigabe des IT-Sicherheitskennzeichens zunächst nicht, ob das Produkt die zugesicherten Anforderungen auch erfüllt. Diese Prüfung erfolgt in einem der Freigabe nachgelagerten Prozess, der Marktaufsicht.

Die Marktaufsicht kann dabei „anlasslos“ und „anlassbezogen“ erfolgen. Bei der anlasslosen Marktaufsicht prüft das BSI nach einem systematischen Überwachungskonzept (z.B. durch Stichproben), ob die Anforderungen an das IT-Sicherheitskennzeichen tatsächlich eingehalten werden.

Die anlassbezogene Marktaufsicht erfolgt beispielsweise dann, wenn dem BSI Informationen über Schwachstellen oder andere Sachverhalte bekannt werden, die darauf hinweisen, dass ein Produkt die Anforderungen des IT-Sicherheitskennzeichens nicht mehr erfüllt. Das BSI kann aber auch eigene technische Prüfungen durchführen oder tiefergehende Nachweise vom Hersteller einfordern.

Eine fortlaufende Marktaufsicht im Nachgang zur Erteilung ist sinnvoll, da IT-Produkte im Laufe der Zeit durch Bekanntwerden neuer Schwachstellen angegreifbarer werden können.

Auf Basis der Erkenntnisse der Markaufsicht stellt das BSI Sicherheitsinformationen zu den gekennzeichneten Produkten zur Verfügung. Die Sicherheitsinformation ist ein zentrales Element des IT-Sicherheitskennzeichens und wird auf einer Informationsseite des BSI zum jeweiligen Produkt eingebettet. Der Link zur Sicherheitsinformation des jeweiligen Produktes ist direkt auf dem produktspezifischen Etikett des IT-Sicherheitskennzeichens per Text und QR-Code abgebildet. Damit ist es für Verbraucherinnen und Verbraucher leicht möglich, die Sicherheitsinformation bei der Kaufentscheidung zu berücksichtigen. So wird zentral und leicht zugänglich dargestellt, ob der Marktaufsicht Informationen über Schwachstellen oder Sicherheitsupdates zur Verfügung stehen. Die Inhalte der Sicherheitsinformation werden je nach Erkenntnislage des BSI aktualisiert.

Durch die mit dem jeweiligen Produkt verbundene und leicht abrufbare Sicherheitsinformation informiert das BSI über die vom Hersteller zugesicherte Sicherheitsfunktionen. Zusätzlich werden aktuelle und sicherheitsrelevante Informationen wie zum Beispiel Schwachstellen und Sicherheitsupdates bereitgestellt. Damit trägt das IT-Sicherheitskennzeichen dazu bei, die Sicherheit von Vebraucher- und Verbraucherinnen-IT transparenter zu machen. ■

Weitere Informationen:

www.bsi.bund.de/IT-SIK.

Bericht zum Digitalen Verbraucherschutz

Die IT-Sicherheit des digitalen Verbrauchermarktes unter der Lupe

von Stephanie Hartmann, Referat Sichere Verbraucherprodukte und -dienste und Marktbeobachtung und Jörg Hübner, Referat Grundsatzfragen des Digitalen Verbraucherschutzes und Kooperationen

Mit dem „Bericht zum Digitalen Verbraucherschutz“ setzt das Bundesamt für Sicherheit in der Informationstechnik (BSI) neue Akzente. Es ist die erste Publikation in Deutschland, die systematisch und fortan jährlich eine Einschätzung zur Informationssicherheit am Verbrauchermarkt gibt, Themenschwerpunkte und aktuelle Entwicklungen näher beleuchtet sowie Handlungsfelder skizziert, um Verbraucherinnen und Verbraucher im digitalen Alltag besser zu schützen. Für das Berichtsjahr 2020 und mit Blick auf die fortwährende Pandemie wurde zudem das Thema der Cyber-Sicherheit im Gesundheitswesen als Themenschwerpunkt eingehender betrachtet.

Mitte dieses Jahres ist der „Bericht zum Digitalen Verbraucherschutz 2020“ auch mit dem Ziel erschienen, vor allem institutionelle Multiplikatorinnen und Multiplikatoren des Verbraucherschutzes anzusprechen. Hierzu zählen unter anderem Verbraucherzentralen, Vereine und Verbände, aber auch Behörden, die auf die Herausforderungen des digitalen Verbraucherschutzes aufmerksam gemacht und mit denen gemeinsame Handlungsfelder aktiv erschlossen werden sollen.

Um sich dem Verbraucherschutzjahr 2020 anzunähern, wurden eine systematische Fachliteratur- und Medienrecherche sowie weitere empirische Analysen durchgeführt. Dabei haben Expertinnen und Experten IT-Sicherheitsvorfälle mit Verbraucherschutzbezug und weitere Trendverläufe gesichtet und bewertet. Eine tiefergehende Untersuchung von Gesundheits-Apps ergänzt die inhaltliche Aufbereitung und ist Herzstück des Themenschwerpunktes.

„Es erfordert nur minimalen Rechercheaufwand, um hinsichtlich der Bedrohungslage im digitalen Raum für Verbraucherinnen und Verbraucher im Jahr 2020 fündig zu werden.“ Diese Aussage des Berichtes verdeutlicht, wie häufig und zugleich vielfältig die IT-Sicherheitsrisiken sind, denen Verbraucherinnen und Verbraucher im digitalen Alltag ausgesetzt sind. Was sind die wesentlichen Erkenntnisse des Berichtes?

Schwerpunktthema: Gesundheit

Das vergangene Jahr war von gesamtgesellschaftlichen Herausforderungen geprägt, die mit enormer Dynamik und nachhaltiger Wirkung die digitale Lebenswelt beeinflusst haben. Ob die smarte Information bzw. Interaktion im Gesundheitsbereich, die Fokussierung auf E-Learning im Bildungsbereich oder das vernetzte Homeoffice als neuer Schwerpunkt im Arbeitsalltag – die globale Corona-Pandemie war und hat zweifelsohne eine Entwicklung beschleunigt, die mit der fortwährenden Digitalisierung stetig neue Angriffsflächen eröffnet. Viele Verbraucherinnen und Verbraucher hatten vor allem zu Beginn der Pandemie ein erhöhtes Informationsbedürfnis, welches Cyber-Kriminelle für sich nutzten. Allein in Nordrhein-Westfalen gingen bis Mitte September 2020 mehr als 1.200 Strafanzeigen in diesem Zusammenhang ein: Kriminelle gaben sich zum Beispiel als medizinische Fachkräfte, Virologinnen und Virologen oder Dienstleistende aus und brachten gefälschte Webseiten und E-Mails in Umlauf. Das Öffnen von E-Mail-Anhängen oder das Anklicken bestimmter Schaltflächen auf den Webseiten führte dabei zu einer Infektion des vernetzten Endgeräts mit entsprechender Schadsoftware.

Ganz unabhängig von Corona stellt der Gesundheitsbereich an sich ein großes Anwendungsfeld für digitale Produkte und Dienstleistungen dar. So sind vor allem mobile Gesundheitsanwendungen in den letzten Jahren zu einem Trendthema des digitalen Verbrauchermarktes

avanciert. Die Verbreitung von Wearables, wie Fitnesstrackern und Smartwatches, haben diese Entwicklung begünstigt. Mit hohen IT-sicherheitstechnischen Anforderungen gilt es die Vertraulichkeit, Verfügbarkeit und Integrität der Daten und des Systems sicherzustellen, da personenbezogene Gesundheits- und Körperdaten einem erhöhten Schutzbedarf unterliegen.

Das BSI hat mit seiner Marktbeobachtung im Digitalen Verbraucherschutz ausgewählte Apps im Gesundheitsbereich, die kein Medizinprodukt sind bzw. nicht im „Verzeichnis der Digitalen Gesundheitsanwendungen (DiGA)“ gelistet werden, in einer Studie näher untersucht, die im aktuellen Bericht näher vorgestellt wird. Der Markt für Gesundheits-Apps stellt sich dabei sowohl intransparent als auch hochdynamisch dar. Eine Anbieterbefragung machte jedoch deutlich, dass bei der Entwicklung und Vermarktung solcher Apps wesentliche IT-Sicherheitsgrundsätze wie „Security by Design“, verbindliche Update-Regelungen und Prozesse zum Umgang mit Schwachstellen nur unzureichend betrachtet werden. Technische Analysen ausgewählter Apps zeigten unter anderem auf, dass ein Abfangen, Auslesen oder Manipulieren der Kommunikation möglich war, beispielsweise durch fehlendes „Certificate Pinning“ oder die Übermittlung von Passwörtern in nicht gehashter Form.

Handlungsfelder

Über die Gesundheits-Apps hinaus wird im aktuellen Bericht skizziert, dass generell eine Vielzahl an Diensten und Produkten im Umgang mit sensiblen Daten meist unzureichende IT-Sicherheitsvorkehrungen vorweist. So wurden im betrachteten Zeitraum mehrere Vorfälle bekannt, in denen Verbraucherinnen und Verbraucher erheblichen Sicherheitsrisiken ausgesetzt waren: IoT-Geräte (Internet of Things), insbesondere Smart Home-Technologien, spielen hier eine große Rolle. Die leicht zugänglichen Produkte, welche meist durch smarte Bedienelemente bei Nutzerinnen und Nutzern punkten, verfügen häufig über veraltete, nicht geschlossene Sicherheitslücken sowie mangelhafte Sicherheitseigenschaften im Produktdesign. Beispielsweise wurden in der Analyse eines auf IoT-Sicherheit spezialisierten Unternehmens allein in sechs ausgewählten Produkten über 7.000 Schwachstellen festgestellt.

Unsichere (Kunden-)Datenbanken stellen eine weitere Gefahrenquelle dar – dem potenziellen Datenabfluss sind Verbraucherinnen und Verbraucher hilflos ausgesetzt. Beinahe täglich werden diese Datenleaks öffentlich bekannt. Hier richtet sich der Appell an die Anbietenden, entsprechende technische und organisatorische Vorkehrungen vorzunehmen, um mehr Informationssicherheit zu schaffen und zugleich das Risiko zu minimieren, dass Daten von Kundinnen und Kunden in die Hände von Kriminellen geraten.

Vorgehensweisen

In vielen Fällen genügen schon einfachste Maßnahmen, um Sicherheitsrisiken zu minimieren – das BSI rät Unternehmen und Herstellern fortlaufend dazu, sich mit den wesentlichen Grundlagen von IT-Sicherheitsmaßnahmen auseinanderzusetzen und konsequent umzusetzen. Hersteller sollten sich bereits ab dem Zeitpunkt der Gestaltung von Produkten und Diensten am Konzept des „Security by Design“ orientieren, um sichere Verbraucherprodukte und -dienste am Markt zu etablieren. Zudem tragen angemessenes IT-Sicherheitsmanagement und die Umsetzung des IT-Grundschutzes dazu bei, sowohl die Daten von Unternehmen als auch von ihren Kundinnen und Kunden zu schützen. Eine Vielzahl weiterer Maßnahmen, wie die Umsetzung von technischen Richtlinien und Normen, welche wichtige Sicherheitseigenschaften und Schutzmechanismen als Standard etablieren, sind bei der Produktentwicklung die Basis, um Informationssicherheit „ab Werk“ bieten zu können. Nicht zu vergessen ist die Analyse und entsprechende zielgruppengerechte Aufarbeitung von Verbraucherbedarfen nicht nur durch die Anbietenden selbst, sondern auch durch weitere Stakeholder wie Verbände, Vereine und staatliche Institutionen, um durch ganzheitliche Ansätze die sichere Nutzung von digitalen Produkten und Diensten zu ermöglichen.

Novum in Deutschland: Der „Bericht zum Digitalen Verbraucherschutz“ beleuchtet fortan jährlich die Informationssicherheit im digitalen, privaten Alltag. (Titelbild)

Abbildung: Handlungsfelder und Vorgehensweisen

Ausblick

Die Digitalisierung bietet den Verbraucherinnen und Verbrauchern enorme Chancen, um den Alltag einfacher und komfortabler zu gestalten. Dabei sind Digitalisierung und Informationssicherheit zwei Seiten einer Medaille. Das heißt, die Informationstechnik und damit die verbundenen Sicherheitsrisiken am digitalen Verbrauchermarkt und im Verbraucherumfeld müssen an jedem Punkt des Entwicklungs-, Vermarktungs- und Verbrauchsprozesses mitgedacht werden. Verbraucherinnen und Verbraucher, wirtschaftliche, staatliche und zivilgesellschaftliche Akteure und Akteurinnen stehen gemeinsam in der Verantwortung.

Der „Bericht zum Digitalen Verbraucherschutz“ für das kommende Berichtsjahr 2021 wird abermals die aktuellen IT-Sicherheitsvorfälle aufgreifen und bereits aufgeführte IT-Sicherheitsrisiken für Verbraucherinnen und Verbraucher in ihrer Entwicklung weiter beobachten, um unter anderem auch Aktivitäten für das BSI abzuleiten. Gleichermaßen sollen neue Sicherheitsthemen und Trends am digitalen Verbrauchermarkt fokussiert werden. Zudem untersucht das BSI fortlaufend die Bedürfnisse, Kompetenzen und Erwartungen von digitalen Verbraucherinnen und Verbrauchern, um Erkenntnisse für einen ganzheitlichen digitalen Verbraucherschutz gewinnen und teilen zu können. ■

Der „Bericht zum Digitalen Verbraucherschutz 2020“ zum Download und Informationen für eine postalische Bestellung unter:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/lageberichte_node.html

Gut vorbereitet auf den nächsten Notfall

IT-Grundschutz ergänzt BSI-Standard 200-4 um zahlreiche Hilfsmittel

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

Egal, ob Cyber-Angriff, Corona-Pandemie oder Naturkatastrophe – Unternehmen und Behörden sind permanent Risiken ausgesetzt, die zu einer Unterbrechung ihres Geschäftsbetriebs führen können. Auf einmal stehen zeitkritische Geschäftsprozesse still und niemand weiß, was zu tun ist. Das BSI bietet mit dem BSI-Standard 200-4 und neuen Hilfsmitteln eine praxisnahe, fortschrittliche Anleitung, um ein Business-Continuity Management-System (BCMS) zur Geschäftsfortführung zu etablieren. Dieser Artikel gibt eine kurze Übersicht über die vom BSI zur Verfügung gestellten BCM-Hilfsmittel.

„In der Not ist guter Rat teuer“

So heißt es in einem altbekannten deutschen Sprichwort. Und in der Tat lässt sich nicht von der Hand weisen, dass eine Unterbrechung zeitkritischer Geschäftsprozesse zu erheblichen Schäden bis hin zur Geschäftsaufgabe führen kann. Um sich vor diesem Risiko zu schützen, haben sich sogenannte Business Continuity Management Systeme (BCMS) etabliert. Ein BCMS senkt einerseits präventiv die Eintrittsrisiken, sodass eine derartige Notlage gar nicht erst eintreten kann. Andererseits bereitet es eine Institution darauf vor, auf ein solches Schadensereignis bestmöglich reagieren zu können und im Notfall bzw. in der Krise handlungsfähig zu bleiben.

Eine große Herausforderung besteht hierbei häufig in der Fragestellung, wie viele Ressourcen für ein BCMS aufgewendet werden. Gerade in Unternehmen ist das oftmals eine sehr harte Kosten-Nutzen-Rechnung, denn die beste Absicherung nützt nichts, wenn die damit einhergehenden Kosten einen wirtschaftlichen Betrieb unmöglich machen. Gleichzeitig sind auch in Behörden die Ressourcen begrenzt. Hier sollte ein BCMS ebenfalls möglichst ökonomisch umgesetzt werden.

Einfacher Einstieg in das BCM

Ein Hauptziel bei der Modernisierung des BSI-Standards 100-4 zum BSI-Standard 200-4 war daher, eine praxisnahe Umsetzungsanleitung zu formulieren. Der neue Standard richtet sich an weniger erfahrene Anwenderinnen und Anwender und soll diesen einen einfachen Einstieg in das Thema BCM ermöglichen. Aber auch BCM-Profis werden adressiert. Diesen steht unter anderem demnächst ein Anforderungskatalog in den Hilfsmitteln zur Verfügung, der einen schnellen und effektiven Abgleich aller Anforderungen aus dem BSI-Standard 200-4 ermöglicht.

Die BCM-Hilfsmittel sind eine wesentliche Arbeitserleichterung für die Arbeit mit dem BSI-Standard 200-4. Sie führen die Hilfsmittel aus dem Umsetzungsrahmenwerk (UMRA) zum BSI-Standard 100-4 fort und lassen sich in die folgenden drei Kategorien einteilen:

- Normativer Anhang (Anforderungskatalog und Glossar)
- Dokumentvorlagen für wesentliche, im BSI-Standard 200-4 geforderte Dokumente
- Weiterführende Informationen

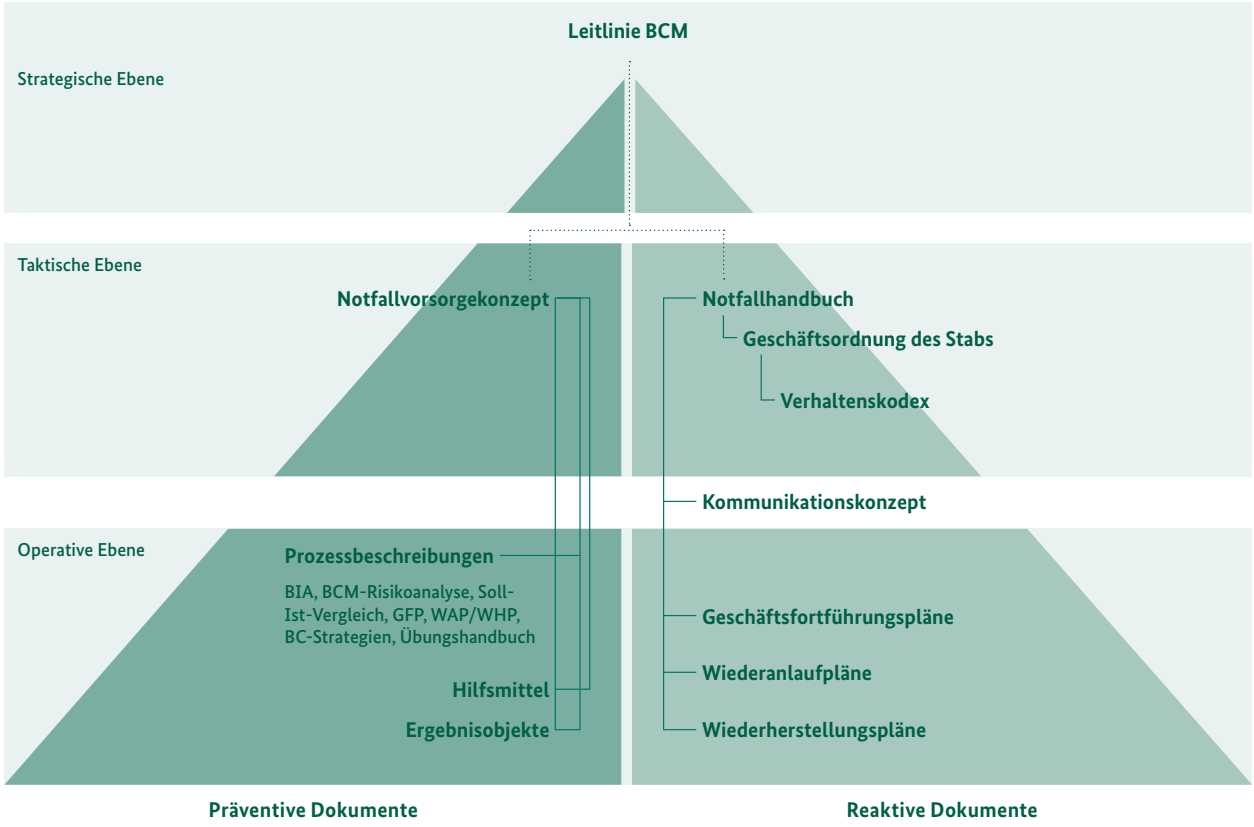


Abbildung 1: Leitlinie BCM

Dokumentvorlagen für Orientierung und Struktur
Der BSI-Standard 200-4 konkretisiert die Vorgaben aus der ISO 22301:2019 und empfiehlt eine konkrete Dokumentenstruktur (siehe Abbildung 1). Diese stellt den Anwenderinnen und Anwendern eine konkrete Orientierungshilfe zur Verfügung. Das BSI bietet zur Unterstützung zu vielen Dokumenten aus der Dokumentenstruktur zusätzlich Dokumentvorlagen an, die bereits mit Beispieltexten angereichert sind. Anwenderinnen und Anwender können die Vorlagen an die Gegebenheiten der eigenen Institution anpassen und erfüllen damit automatisch zahlreiche Anforderungen des BSI-Standard 200-4. Der Vorteil ist ein deutlich geringerer Dokumentationsaufwand.

Feedback an das IT-Grundschutz-Team
Die Hilfsmittel zum BSI-Standard 200-4 werden als sogenannte „Community Drafts" veröffentlicht und fortlaufend ergänzt und aktualisiert. Kommentare und Anregungen zu den Hilfsmitteln und zum BSI-Standard 200-4 können an grundschutz@bsi.bund.de gesendet werden.

Weiterführende Informationen
Da der Umfang eines Standardwerks begrenzt ist, hat das BSI in den Hilfsmitteln zum Standard 200-4 ergänzende Aspekte veröffentlicht. In den weitergehenden Informationen gibt es Hinweise zu BCM-Tools, Vorschläge für BC-Strategien, Weitergehende Aspekte zur Bewältigung (siehe „Exkurs um Krisenmanagement: Analoge Krisen vs. IT-Krisen") und viele weitere, hilfreiche Veröffentlichungen. Beispielsweise sind im Dokument „Vorschläge für BC-Strategien" konkrete Ideen dazu erläutert, wie Anwenderinnen und Anwender erfolgreiche Strategien und Lösungen ausgestalten können. ■

Exkurs zum Krisenmanagement: Analoge Krisen vs. IT-Krisen

Das Krisenmanagement ist ein umfangreiches und komplexes Thema, das im BSI-Standard 200-4 nicht vollständig abgedeckt werden kann, da hierfür ein eigenes Krisenmanagementsystem erforderlich ist. Jedoch werden Institutionen durch den BSI-Standard 200-4 grundlegend dazu befähigt, mit ihrer besonderen Aufbauorganisation, Krisen, die aus der Unterbrechung zeitkritischer Geschäftsprozesse entstehen, zu bewältigen.

Weitergehende Informationen zum Krisenmanagement sind in dem Hilfsmittel „Weiterführende Aspekte zur Bewältigung" beschrieben. Neben beispielhaften Vorschlägen für den Aufbau von Notfall- und Krisenstäben werden auch die Besonderheiten von IT-Krisen aufgegriffen. IT-Krisen, und hierbei insbesondere Cyber-Angriffslagen, unterscheiden sich erheblich von herkömmlichen analogen Krisen (siehe Abbildung 2). Sie sind in der Regel nicht örtlich begrenzt, entwickeln und breiten sich schneller und dynamischer aus, sind nicht immer direkt als solche ersichtlich und sind durch Angriffsszenarien geprägt (z.B. gezielte Cyber-Attacken), die in vergleichbarer Form im analogen Umfeld erheblich seltener vorkommen.

Wesentliche Unterschiede zwischen analogen Krisen und IT-Krisen

Abbildung 2: Analoge Krisen vs. IT-Krisen

BSI INTERNATIONAL

Die digitale Souveränität Europas stärken

Das Europäische Kompetenzzentrum, die Nationalen Koordinierungszentren und die Cyber-Sicherheits-Community

von Sirko Höer und Heiko Siebel, Referat Technologie- und Forschungsstrategie

Je mehr der Alltag der Menschen und die Geschäftsprozesse in Organisationen mit digitalen Technologien verwoben sind, umso wichtiger ist der Ausbau der Fähigkeiten, Cyber-Sicherheitsvorfälle abzuwehren. Ziel der Europäischen Union ist es, dabei international eine Führungsrolle einzunehmen und die eigene digitale Souveränität zu stärken.

Bereits heute gibt es in der EU umfangreiche Aktivitäten hinsichtlich Forschung, Technologien und industrieller Entwicklung im Bereich der Cyber-Sicherheit. Oft beschränken sich diese Aktivitäten allerdings auf bestimmte Regionen, Unternehmensgrößen, Branchen oder Gesellschaftsbereiche. Diese Aktivitäten sollen künftig innerhalb der EU enger abgestimmt werden, um Ressourcen zu bündeln, Synergien zu schaffen und ein ausgeglichenes sowie wettbewerbsfähiges Cyber-Sicherheitsniveau herzustellen.

Das Europäische Kompetenzzentrum für Cybersicherheit

Hierzu hat die Europäische Kommission mit der Verordnung 2021/887 die Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung (ECCC, im Folgenden „Kompetenzzentrum“) beschlossen. Zusätzlich wird ein Netz von Nationalen Koordinierungszentren (NCC) in den EU-Mitgliedstaaten etabliert. Das Kompetenzzentrum hat seinen Sitz in Bukarest und wird zum wichtigsten Instrument der EU für die Bündelung von Investitionen in Forschung, Technologie und industrieller Entwicklung im Bereich der Cyber-Sicherheit. Dazu gehört unter anderem auch die Realisierung von Cyber-Sicherheitsprodukten, -diensten und -verfahren. Insbesondere die Planungen der europäischen Förderprogramme „Horizont Europa“ und „Digitales Europa“ im Bereich Cyber-Sicherheit werden damit besser aufeinander abgestimmt. Bei diesen Aktivitäten sind vor allem auch die Belange von kleinen und mittelständischen Unternehmen (KMU) sowie von Start-ups zu berücksichtigen.

Das Kompetenzzentrum wird durch die Mitgliedstaaten und die Europäische Kommission verwaltet. Dafür ist ein Verwaltungsrat (engl. „Governing Board“) eingerichtet worden, der aus Mitgliedern der Kommission und Vertreterinnen und Vertretern der Mitgliedstaaten besteht. Das BSI repräsentiert Deutschland im Verwaltungsrat. Der Verwaltungsrat steuert die strategische Ausrichtung der Tätigkeiten des Kompetenzzentrums und stellt den Einklang der Aufgaben mit der Verordnung sicher.

In Abgrenzung zu Computernotfallteams (engl. „Computer Security Incident Response Team“, CSIRT) und deren CSIRT-Netzwerken soll das Kompetenzzentrum keine operativen Cyber-Sicherheitsaufgaben wie Detektion und Bewältigung von Vorfällen wahrnehmen. Das Zentrum sollte jedoch in der Lage sein, die Entwicklung

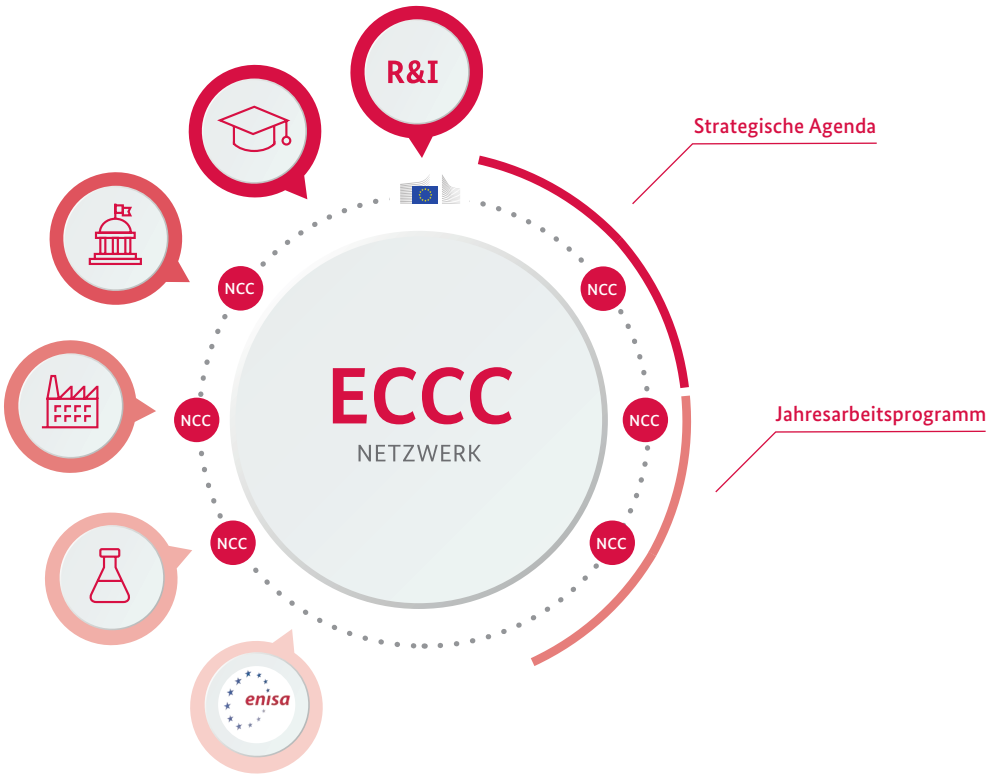


Abbildung: ECCC

von digitalen Infrastrukturen im Dienste der Wirtschaft, insbesondere der KMU, der Forschungsgemeinschaften, der Zivilgesellschaft und des öffentlichen Sektors orientiert am Auftrag und den Zielen der Verordnung zu erleichtern.

Ziele und Visionen

Zu den zentralen Zielen des Kompetenzzentrums gehört die Stärkung der Führungsrolle und strategischen Autonomie der Union. Dies erfolgt durch die Wahrung und Weiterentwicklung der Kapazitäten und Fähigkeiten im Bereich der Cyber-Sicherheit. Des Weiteren fokussiert sich das Kompetenzzentrum auf die Steigerung der globalen Wettbewerbsfähigkeit der Cyber-Sicherheitsbranche und die Gewährleistung hoher Cyber-Sicherheitsstandards.

Das europäische Netzwerk der Nationalen Koordinierungszentren (NCCs) wird dabei den Austausch zwischen den Mitgliedstaaten intensivieren, damit mögliche internationale Projektpartnerschaften besser und schneller gefunden und geschlossen werden können. Die Nationalen Koordinierungszentren werden den Austausch zwischen relevanten nationalen Stellen im Forschungs- und Wirtschaftssektor im Bereich Cyber-Sicherheit und Cyber-Verteidigung innerhalb der Mitgliedstaaten fördern. Dadurch wird der Informationsfluss zum Kompetenzzentrum gebündelt, um die jeweiligen nationalen Cyber-Sicherheits-Communities bestmöglich zu unterstützen. Ein weiteres Ziel der Nationalen Koordinierungszentren ist die Förderung und Verbreitung von Bildungsprogrammen im Bereich der Cyber-Sicherheit.

Beteiligt ist zudem die Agentur der Europäischen Union für Cybersicherheit (ENISA), die dem Kompetenzzentrum sowie den Nationalen Koordinierungszentren beratend zur Seite steht.

Das Nationale Koordinierungszentrum für Deutschland

Das deutsche Nationale Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung (NKCS, das deutsche NCC) ist eine gemeinsame, virtuelle Institution des Bundesinnenministeriums, des Bundesministeriums für Bildung und Forschung, des Bundeswirtschaftsministeriums und des Bundesverteidigungsministeriums sowie einzelner nachgeordneten Bereichen. Dabei wird das BSI die Rolle als Kopfstelle und „Single Point of Contact“ wahrnehmen.

Ziel des NKCS ist es, eine nationale Informationsplattform für alle Interessierten bereitzustellen, die Vernetzung innerhalb der deutschen Cyber-Sicherheits-Community zu fördern sowie eine initiale Beratung zu Themen der Cyber-Sicherheitsforschung und -entwicklung inklusive Projektvorhaben mit einer europäischen Perspektive anzubieten. ■

Weitere Informationen:

EU-Verordnung 2021/887
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0887&qid=1623142941122

Horizont Europa
https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

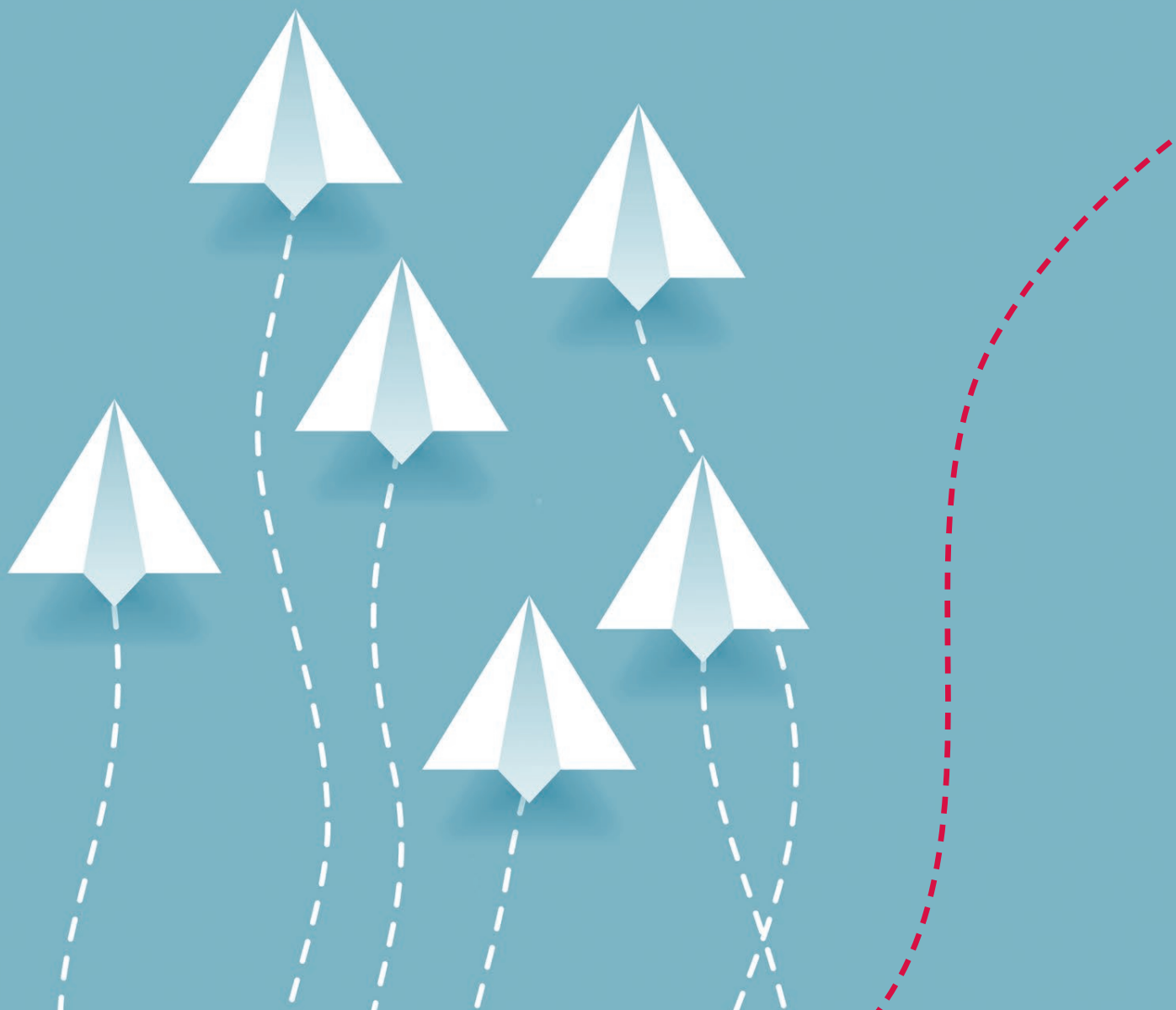
Digitales Europa
https://digital-strategy.ec.europa.eu/en/activities/digital-programme

Die Europäische Bürgerinitiative

Online-Sammelsysteme für Unterstützungsbekundungen europäischer Bürger und Bürgerinnen

von Yona Raekow, Referatsleiterin Zertifizierung nach Technischen Richtlinien

Die Europäische Bürgerinitiative (EBI) ist seit dem 01. April 2012 ein wichtiges Instrument der partizipativen Demokratie in der EU. Dieses Instrument und die Beteiligung von einer Million EU-Bürgerinnen und Bürger, die in einem Viertel (mind. sieben) der Mitgliedstaaten wohnen, verschafft sich in Brüssel Gehör: EU-Bürgerinnen und Bürger können die Europäische Kommission auffordern, einen Rechtsakt vorzuschlagen. Das Recht auf die Vorlage einer EBI ist grundsätzlich mit dem Initiativrecht des Parlaments und des Rates vergleichbar. Um eine EBI durchzuführen müssen folgende Phasen durchlaufen werden:



1 Bürgerausschuss
Die Einleitung einer EBI beginnt mit der Gründung einer Organisationsgruppe, dem „Bürgerausschuss". Diesem Ausschuss müssen mindestens sieben Personen angehören, die in mindestens sieben verschiedenen Mitgliedstaaten ansässig sind. Der Ausschuss dient als Ansprechpartner der Kommission zur EBI.

2 Registrierung
Zunächst muss die EBI bei der Kommission registriert werden. Die Kommission entscheidet innerhalb von zwei Monaten über die Registrierung. Eine Registrierung wird abgelehnt, wenn die Verfahrenserfordernisse nicht erfüllt sind oder die Initiative außerhalb des Rahmens liegt, in dem die Kommission befugt ist, einen Vorschlag für einen Rechtsakt vorzulegen. Sie wird ebenfalls abgelehnt, wenn die Initiative offenkundig unseriös, missbräuchlich oder böswillig ist oder den Werten der EU entgegensteht. Registrierte Initiativen werden auf dem Internetportal der Kommission veröffentlicht.

3 Sammlung von Unterstützungsbekundungen
Sobald die EBI registriert worden ist, können die Organisatorinnen und Organisatoren mit der Sammlung von Unterstützungsbekundungen beginnen. Dazu haben sie zwölf Monate Zeit. Unterstützungsbekundungen können in Papierform oder elektronisch gesammelt werden.

Für die Onlinesammlung stellt die Kommission seit 2020 ein zentrales Online-Sammelsystem (OCS) bereit, das die Organisatoren Europäischer Bürgerinitiativen kostenfrei nutzen können. Als Alternative zum zentralen OCS besteht zusätzlich auch die Möglichkeit, Unterstützungsbekundungen über individuelle, eigenentwickelte OCS zu sammeln. Diese müssen jedoch vor ihrem Einsatz durch die zuständige Behörde des Mitgliedsstaates, in dem das System betrieben wird, zertifiziert werden. In Deutschland ist die zuständige Behörde zur Zertifizierung von individuellen OCS das BSI.

4 Überprüfung der Unterschriften
Sobald die Organisatorinnen und Organisatoren die erforderliche Mindestanzahl von insgesamt über 1 Mill. Unterstützungsbekundungen in sieben Mitgliedstaaten gesammelt haben, müssen sie diese bei den zuständigen nationalen Behörden – in Deutschland ist es das Bundesverwaltungsamt – einreichen. Ihre Aufgabe ist es, die Unterstützungsbekundungen zu validieren und die Anzahl der gültigen Bekundungen zu bescheinigen.

5 Vorlage und Prüfung
In dieser Phase müssen die Organisatorinnen und Organisatoren die entsprechenden Bescheinigungen der nationalen Behörden einreichen.

Abbildung: Phasen der EBI

6 Antwort erhalten

Ist die Unterschriftensammlung erfolgreich, muss die Kommission sie unverzüglich in einem Register veröffentlichen und sich auf angemessener Ebene mit den Organisatorinnen und Organisatoren treffen, damit diese die Einzelheiten ihres Antrags erläutern können. Nach einem Meinungsaustausch mit der Kommission erhalten die Organisatorinnen und Organisatoren die Gelegenheit, die Initiative bei einer öffentlichen Anhörung im Parlament vorzustellen. Die Anhörung wird von dem Ausschuss organisiert, der für den Gegenstand der Bürgerinitiative zuständig ist. Im Idealfall folgt dann eine Gesetzesinitiative der Kommission.

Aufgabe des BSI

Aufgabe des BSI ist die Bescheinigung der Konformität von individuellen OCS. Ein individuelles OCS umfasst sowohl bei den EBI-Organisatorinnen und Organisatoren als auch beim Hosting-Provider und Auftragsdatenverarbeiter:

- die technische Plattform (Hardware, Software, Hosting-Umgebung)
- Geschäftsprozesse
- Personal und
- Infrastruktur

Die erforderlichen Nachweise über die Übereinstimmung eines individuellen OCS mit der EBI-VO sind von der Antragstellerin bzw. vom Antragsteller für sämtliche Bestandteile des Systems zu erbringen.

Das BSI prüft die eingereichten Nachweise zunächst auf Vollständigkeit – d. h. ob sämtliche Anforderungen durch geeignete Nachweise belegt wurden – und führt anschließend eine inhaltliche Prüfung auf Grundlage von Spezifikationen der EU Kommission durch.

Falls erforderlich ist das BSI berechtigt, zusätzliche Unterlagen, Ergänzungen oder Nachbesserungen einzufordern. Das BSI kann bei Bedarf zusätzlich Vor-Ort-Audits bei der Antragstellerin bzw. beim Antragsteller oder dem Hosting-Provider ansetzen und praktische Tests mit dem OCS (z. B. Schwachstellen-/Penetrationstests) durchführen. Bei positivem Abschluss erteilt das BSI die beantragte Bescheinigung.

Anhängige Initiativen

Bislang haben sechs Initiativen die erforderliche Anzahl an Unterschriften erreicht („Wasser ist ein Menschenrecht“, „Einer von uns“, „Stop Vivisection“, „Verbietet Glyphosat“, „Minority SafePack – One Million Signatures for Diversity in Europe“ und „Schluss mit der Käfighaltung“) und sind der Kommission vorgelegt worden. Seit der Einführung der EBI wurden Stand August 2021, 107 Registrierungsanträge gestellt, von denen die Kommission insgesamt 82 Initiativen registriert hat. Für 20 dieser 82 Initiativen bescheinigte das BSI die Konformität des verwendeten OCS. ■

Weitere Informationen:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Leistungen-und-Kooperationen/Europaeische-Buergerinitiative/Europaeische_Buergerinitiative/europaeische_buergerinitiative_node.html

https://europa.eu/citizens-initiative/_de

Frischer Wind zur Stärkung des digitalen Binnenmarktes

Aktuelle Entwicklungen zur europäischen Cyber-Sicherheitszertifizierung

von Diana-Victoria Menzel und Patrick Seidel, Referat Fachgremienarbeit für Prüf- und Zertifizierungsverfahren, Qualitätsmanagement

Seit 2019 wird ein gemeinsamer europäischer Rahmen für Cyber-Sicherheitszertifizierungen aufgebaut, um den digitalen Binnenmarkt zu stärken. Das BSI ist maßgeblich beteiligt, muss aber auch einige organisatorische Neuerungen zuwege bringen.

Die Zertifizierung von Cyber-Sicherheit ist seit jeher ein Themenbereich, über den unterschiedliche Interessen abgebildet werden. Zum einen werden über die Zertifizierung die Interessen der Hersteller in den Blick genommen, damit diese mit ihren Produkten am Markt wettbewerbsfähig bleiben. Zum anderen werden die Interessen des Gesetzgebers, welcher die notwendigen Rahmenbedingungen geschaffen hat, konkretisiert. Und nicht zuletzt werden die Interessen der Verbraucherinnen und Verbraucher hervorgehoben, die mithilfe der unabhängigen Zertifizierung am Markt verfügbare Produkte besser beurteilen können.

Die Europäische Kommission hat diese vielfältigen Interessen in den Blick genommen, um den digitalen Binnenmarkt der Europäischen Union für die Herausforderungen der kommenden Jahrzehnte zu wappnen. Die Basis zur Umsetzung dieses Ziels ist die EU-Verordnung 2019/881, die im Sommer 2019 in Kraft trat, der sogenannte Cybersecurity Act (CSA). Dieser ermöglicht die gemeinsame Entwicklung und Anerkennung des europäischen Rahmenwerks zur Cyber-Sicherheitszertifizierung und stärkt nicht nur das Vertrauen untereinander, sondern auch den digitalen Binnenmarkt.

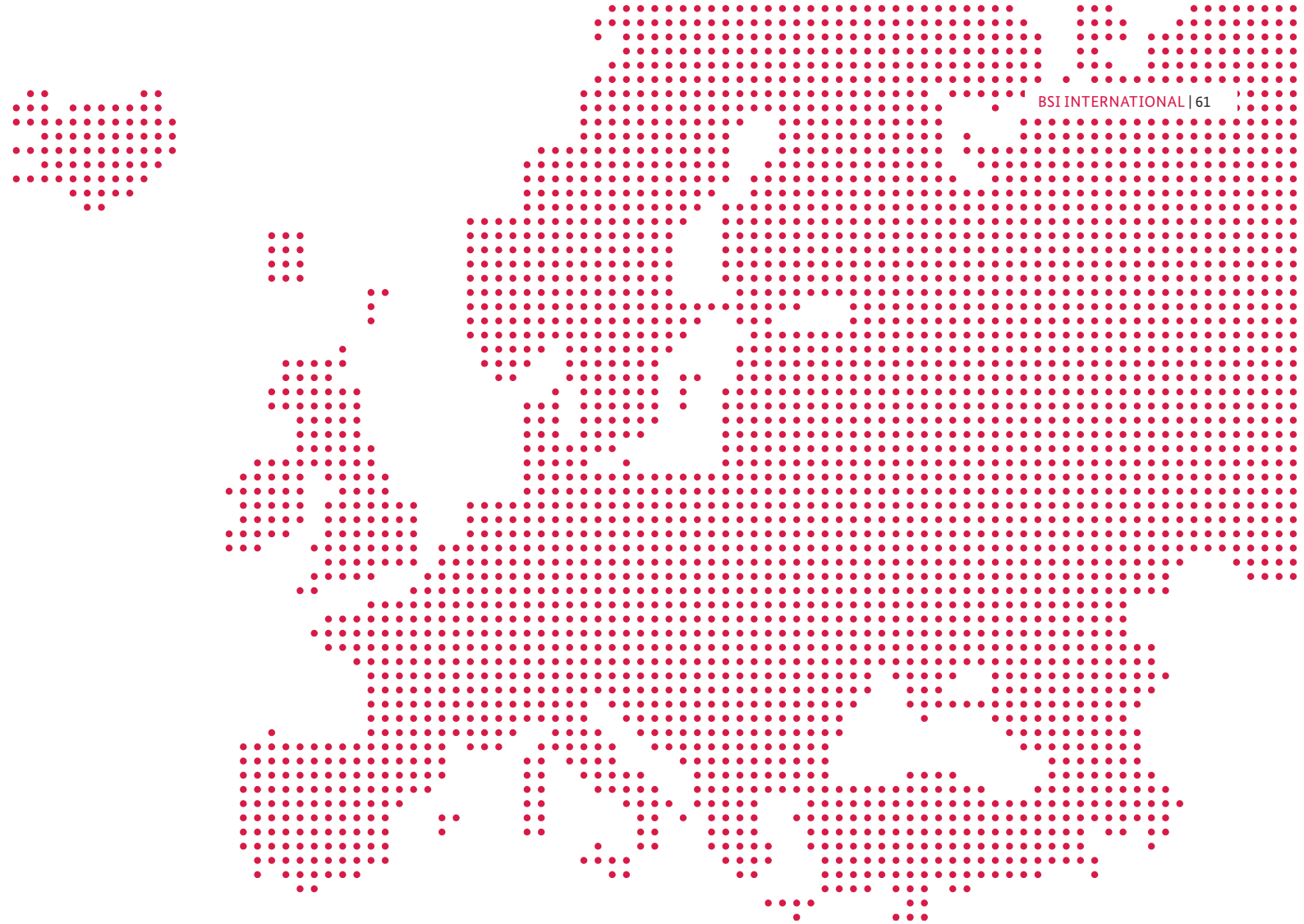
Aufgabenteilung nach Maßgabe des CSA

Der CSA legt fest, dass alle europäischen Mitgliedstaaten eine nationale Behörde für Cyber-Sicherheitszertifizierung (engl. „National Cybersecurity Certification Authority“, NCCA) benennen sollen. Im Mai 2021 hat der Bundestag mit der Verabschiedung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) durch den neuen Paragrafen 9a BSIG als deutsche NCCA ernannt. Dabei gliedert sich die NCCA innerhalb des BSI in zwei Aufgabenbereiche: Zertifizierung und Aufsicht.

Als zertifizierende NCCA erteilt das BSI gemäß IT-Sicherheitsgesetz 2.0 und CSA als alleinige Stelle in Deutschland Cyber-Sicherheitszertifikate für die Vertrauenswürdigkeitsstufe „hoch“, sofern diese Vertrauensstufe im Rahmen eines europäischen Zertifizierungsschemas festgelegt wurde. Zur Erfüllung dieser Aufgabe profitiert das BSI von seiner langen und international anerkannten Zertifizierungserfahrung. Das erste gemeinsame europäische Cyber-Sicherheitsschema, das EUCC, basiert auf der Common Criteria-Zertifizierung, mit der das BSI sich über die letzten Jahrzehnte Vertrauen zu Qualität und Unabhängigkeit seiner Zertifikate über nationale Grenzen hinaus aufbauen konnte. Auch die neuen europäischen Anforderungen wurden maßgeblich durch das BSI mitgestaltet.

Kontrolle über Aufsichtsführung

Der weitere wichtige Aufgabenbereich der NCCA betrifft die Aufsichtsführung, die künftig sicherstellt, dass die im jeweiligen europäischen Schema für die Cyber-Sicherheitszertifizierung festgelegten Anforderungen, von der



Herstellerselbsterklärung (Vertrauenswürdigkeitstufe: „niedrig“) über die privaten Zertifizierungsstellen (Vertrauenswürdigkeitsstufe: „mittel“) bis hin zur zertifizierenden NCCA des BSI (Vertrauenswürdigkeitsstufe: „hoch“), eingehalten werden.

Künftig können Beschwerden an die aufsichtsführende NCCA gerichtet werden, wenn die Vermutung besteht, dass gegen den CSA bzw. die im jeweiligen europäischen Schema für die Cyber-Sicherheitszertifizierung festgelegten Regeln verstoßen wurde. Sollte die NCCA feststellen, dass ein solcher Verstoß vorliegt, ist sie befugt, entsprechende Sanktionen, beispielsweise in Form von Bußgeldern, zu verhängen. Ebenfalls gesetzlich festgelegt wurde, dass das BSI den Konformitätsbewertungsstellen die Befugnis erteilt, entsprechend der europäischen Cyber-Sicherheitszertifizierung tätig zu werden.

Seit Beginn des Jahres 2021 findet im BSI der Aufbau der NCCA statt. Dabei spielt der BSI-Standort in Freital eine besondere Rolle, denn hier ist ein großer Teil der im CSA benannten Aufgaben verortet. Dies erfordert sowohl organisatorische Neuerungen als auch personellen Aufwuchs.

Zusammenarbeit in Europa

Eine weitere wichtige Aufgabe der NCCA ist die enge Zusammenarbeit auf europäischer Ebene bedingt durch die Mitgliedschaft in der Europäischen Gruppe für die Cyber-Sicherheitszertifizierung (ECCG). Hier wird vor allem die Weiterentwicklung des europäischen Zertifizierungsrahmens gestaltet sowie der Austausch der NCCAs untereinander gewährleistet. Ferner sind der Europäischen Kommission und der Europäischen Agentur für Cybersicherheit (ENISA) die Konformitätsbewertungsstellen für jedes europäische Schema der Cyber-Sicherheitszertifizierung zu melden. Neben der Befugnis zur Erteilung von Zertifikaten werden dort auch Widerrufe durch die aufsichtsführende NCCA gemeldet und veröffentlicht. Dies gewährleistet, dass die zertifizierenden Stellen der Mitgliedstaaten die anspruchsvollen Anforderungen des europäischen Zertifizierungsrahmens einhalten. ■

Weitere Informationen:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/NCCA/ncca_node.html

https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html

DIGITALE GESELLSCHAFT

Crashtest für Cyber-Sicherheit

Wie IT-Sicherheit die Mobilitätswende voranbringt und Wachstum in Deutschlands wichtigsten Industrien unterstützt

Die Automobilbranche ist die größte Branche des verarbeitenden Gewerbes und gemessen am Umsatz der mit Abstand bedeutendste Industriezweig in Deutschland. Angesichts der Herausforderungen des Klimawandels und der notwendigen Mobilitätswende, befindet sich die Branche in einem rasanten Wandel. Dabei spielen nicht nur der Umstieg auf alternative Antriebe und Elektromobilität eine Rolle, sondern auch der zunehmende Einsatz von Informationstechnologie.

Moderne Fahrzeugmodelle entwickeln sich zu vollvernetzten Plattformen. Hersteller entwickeln eigene Cloud-Infrastrukturen. Technologien wie die Fahrzeug-zu-Fahrzeug-Kommunikation und 5G sollen das Autofahren sicherer und komfortabler machen. Durch die Digitalisierung werden neue Dienstleistungen und Funktionen im Fahrzeug ermöglicht. Das automatisierte Fahren ist nur ein Aspekt dieser Entwicklung. Künstliche Intelligenz (KI) soll künftig eine ganze Reihe von Funktionen übernehmen und eine vernetzte und ressourcenschonende Mobilität ermöglichen.

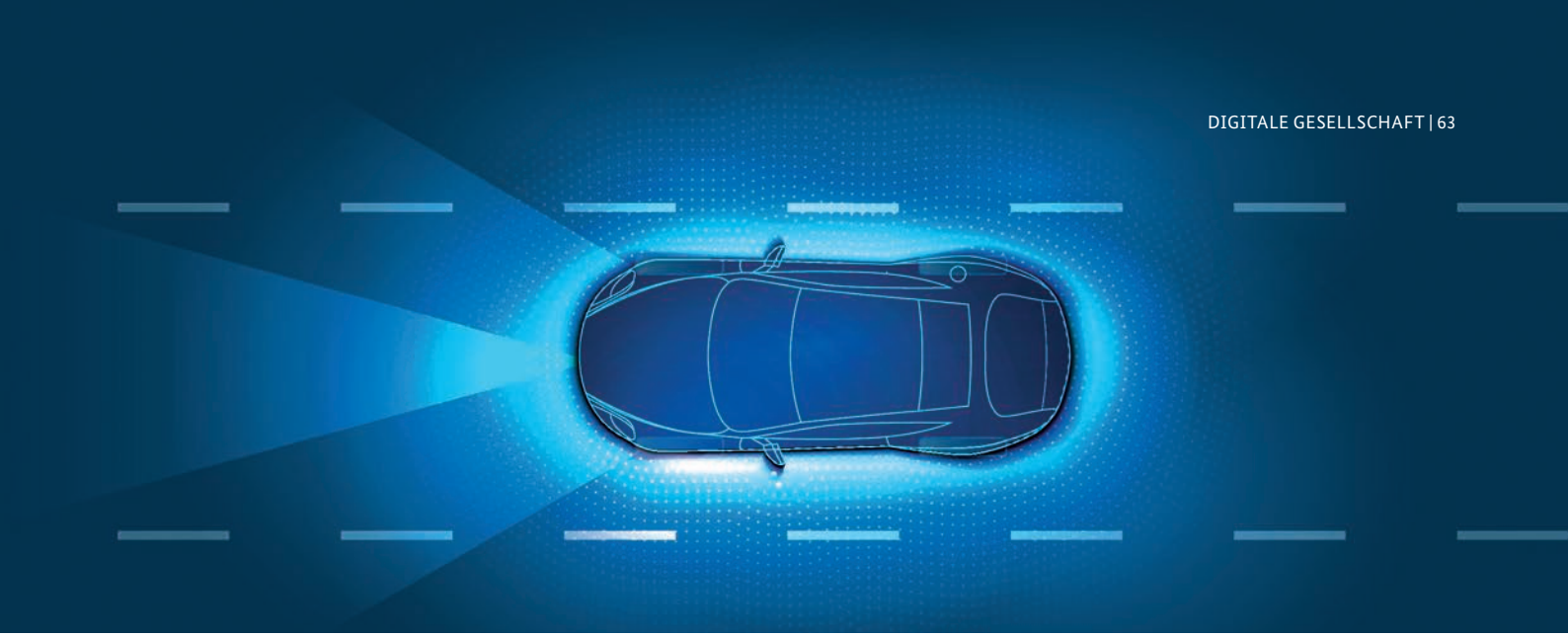
Neue Herausforderungen für die Cyber-Sicherheit

In dem Maße, in dem Fahrzeuge mit der Außenwelt vernetzt sind, nimmt auch die Angriffsfläche und damit die Bedeutung von IT-Sicherheit in der Automobilbranche zu. Dies gilt in der kompletten Wertschöpfungskette ebenso wie für die Fahrzeuge selbst. Cyber-Sicherheit muss deshalb in allen Bereichen und bei allen Digitalisierungsvorhaben einen Schwerpunkt bilden und von Anfang an umgesetzt werden. Die gilt insbesondere deshalb, weil Cyber-Angriffe immer ausgefeilter werden.

Welch gravierende Auswirkungen die Angreifbarkeit durch Cyber-Kriminelle haben kann, zeigen Beispiele aus der jüngsten Zeit: Automobilhersteller und ihre Zulieferer wurden Opfer von gezielten Cyber-Angriffen. 2017 kam es bei einem französischen Automobilhersteller zu einem Stillstand der kompletten Produktion, ausgelöst durch die Schadsoftware „WannaCry“. Auch dessen Zulieferer waren durch die Auswirkungen betroffen und konnten keine Teile liefern. 2020 wurden die Systeme eines deutschen Zulieferers und Dienstleisters für die Automobilhersteller verschlüsselt und mehrere Gigabyte Daten flossen ab. 2021 waren zwei Zulieferer von einem Ransomware-Angriff betroffen.

Einsatz neuer Technologien: Chance und Risiko zugleich

Die wachsende Bedeutung der IT in Fahrzeugen führt zu einem steigenden Einfluss der IT-Sicherheit auf die Gesamt-Sicherheit von Kraftfahrzeugen und stellt auch die Zulassung vor ganz neue Herausforderungen. Dies gilt insbesondere für Systeme, die auf Künstliche Intelligenz setzen. Die Funktionsweise von KI-Systemen ist komplex und schwer interpretierbar. Die starke Vernetzung von IT-Komponenten innerhalb eines Fahrzeugs und mit externen IT-Systemen erhöht die Komplexität des Gesamtsystems massiv. Zudem verändert sich die IT über den Lebenszyklus des Fahrzeugs, zum Beispiel durch Softwareupdates. Für eine effektive Bewertung der Sicherheitseigenschaften werden somit qualitativ neue Methoden und Werkzeuge benötigt.



Die Robustheit von KI-Systemen zu fördern, dient nicht nur der Prävention von Hackerangriffen, sondern reduziert zugleich die Fehleranfälligkeit im Normalbetrieb. Bei sogenannten adversarialen Angriffen beispielsweise können KI-Systeme mit optischen Störungen (z.B. Aufkleber auf Straßenschildern) in die Irre geführt werden. Methoden, die die Robustheit von KI-Systemen gegen solche Manipulationen erhöhen, helfen auch, diese weniger anfällig gegen andere optische Störungen wie beispielsweise Schmutz oder Schnee auf Schildern zu machen.

Gemeinsam für mehr Cyber-Sicherheit: Aktivitäten des BSI

Das BSI fördert gezielt Vernetzung und Austausch mit den relevanten Akteuren der Branche, um die IT-Sicherheit im Automobilbereich zu verbessern. Mit Herstellern und Zulieferern arbeitet das BSI über den Verband der Automobilindustrie (VDA) zu sicherheitsrelevanten Themen. Gemeinsame Forschungsvorhaben wurden in Deutschland und international angestoßen.

Darüber hinaus entwickelt das BSI die Standards, um die Sicherheit von IT-Systemen im Automobilbereich zu testen – gemeinsam mit Partnern in Deutschland und Europa. Mit dem Kraftfahrt-Bundesamt (KBA) arbeitet das BSI an der Umsetzung der neuen UNECE-Regeln (UNECE: Wirtschaftskommission der Vereinten Nationen für Europa) zur Cyber-Sicherheit in der Typgenehmigung und Marktüberwachung. Die ersten Verfahren zur Zertifizierung der Cyber Security Management Systeme (CSMS) und Software Update Management Systeme (SUMS) bei den Herstellern nach UNECE R155 und R156 werden derzeit vom BSI begleitet.

Mit dem TÜV-Verband e. V. erarbeitet das BSI Konzepte zur Prüfung und Bewertung von KI-basierten Komponenten und Funktionen. Auf europäischer Ebene arbeitet das BSI intensiv an der europaweiten Entwicklung und Koordination gemeinsamer Standards mit. Auf der IAA Mobility 2021 hat das BSI erstmals ein Branchenlagebild Automotive vorgestellt. Dieses beleuchtet die Cyber-Sicherheitslage der IT im Auto selbst und der Lieferkette im Herstellungsprozess. Das BSI wird des Weiteren zwei Technische Richtlinien (TR-03164-1 und -2) zur IT-Sicherheit in sogenannten „Cooperative Intelligent Transport Systems“ (C-ITS) veröffentlichen. Derzeit entwickelt das BSI zudem im Rahmen eines Projektes zu Hard- und Softwareanalysen einen Leitfaden für Penetrationstests für vernetzte Fahrzeuge, der von Behörden, Prüfstellen und Unternehmen genutzt werden kann. Es sollen darin u.a. organisatorische und technische Voraussetzungen für die Durchführung beschrieben und die typischen drahtlosen und drahtgebundenen Schnittstellen eines vernetzten Fahrzeuges abgedeckt werden. Der Leitfaden soll 2022 fertiggestellt werden.

IT-Sicherheit als Schlüssel für Vertrauen in neue Technologien

Mehr (IT-)Sicherheit schafft einen entscheidenden Rahmen für die Akzeptanz und Nutzung neuer Technologien gerade im Mobilitätssektor: Niemand will sein Leben riskieren, wenn er fliegt, in die Bahn, auf ein Schiff oder ins Auto steigt. BSI-Präsident Arne Schönbohm beschrieb die Herausforderung bei der Vorstellung des Branchenagebildes so: „Computer sind das Hirn jedes modernen Fahrzeugs und übernehmen längst zentrale Steuerungsfunktionen. Wenn Autos mit anderen Autos oder mit der Straßeninfrastruktur vernetzt sind, müssen wir sichergehen können, dass wir beim Fahren vor Manipulationsversuchen Dritter geschützt sind. Cyber-Sicherheit wird dabei genauso wichtig wie funktionierende Bremsen. Wir brauchen einen Crashtest für Cyber-Sicherheit!“ Dieser Herausforderung stellt sich das BSI als die Cyber-Sicherheitsbehörde des Bundes. Für eine sichere und vernetzte Mobilität. ■

Weitere Informationen:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive.html

Nächste Stufe für das Smart-Meter-Gateway

Wie die Digitalisierung der Energiewende voranschreitet

von Michael Brehm und Thomas Joachim, Referat Cyber-Sicherheit für die Digitalisierung der Energiewirtschaft

Der Rollout des Smart-Meter-Gateways (SMGW) läuft: Der Grundstein, um das Smart Grid der Zukunft sicher zu gestalten ist gelegt. Darauf aufbauend gilt es jetzt, die Standards für zukünftige energiewirtschaftliche Anwendungsfälle im Kontext des intelligenten Messsystems gemeinsam mit dem Bundeswirtschaftsministerium (BMWi) und den Marktakteurinnen und -akteuren zu gestalten und somit zum Gelingen der Digitalisierung der Energiewende beizutragen.

Die mit der rasanten Technologieentwicklung einhergehende Digitalisierung aller gesellschaftlichen Lebensbereiche stellt Staat, Wirtschaft und Gesellschaft vor große Herausforderungen. Anstelle von wenigen Großkraftwerken muss künftig eine Vielzahl von dezentralen Erzeugungsanlagen (z. B. Photovoltaik-Anlagen) in das intelligente Energienetz (Smart Grid) integriert werden. Auf der Seite der Verbraucherinnen und Verbraucher bedingt die wachsende Zahl von Verbrauchseinrichtungen, wie Wallboxen und Wärmepumpen, ein sicheres und intelligentes Lastmanagement. Flexibilität im zukünftigen Smart Grid ist nötig, um Erzeugung und Verbrauch im Sinne der Netzstabilität aufeinander abzustimmen.

Durch die Verwendung von intelligenten Messsystemen (iMSys) und der damit einhergehenden Verwendung von zertifizierten SMGW werden wichtige Systeme des Energienetzes über eine sichere Kommunikationsinfrastruktur vernetzt. Zudem können durch den Einsatz von iMSys Netzzustandsdaten erhoben werden, was mehr Transparenz über die Leistungsflüsse im Verteilnetz zur Folge hat. Ferner sollen flexible Verbrauchseinrichtungen und dezentrale Erzeugungsanlagen zukünftig über das iMSys gesteuert und somit netz- und marktdienlich eingesetzt werden.

Stufen der Digitalisierung - Der Rollout seit 2020

Durch den Start des Rollouts 2020 wird das Potential der sicheren Gateway-Kommunikationsplattform bereits umfangreich genutzt. Damit werden wertvolle Erfahrungen für die Weiterentwicklung der technischen Standards gesammelt. Gemeinsam mit dem BMWi hat das BSI eine Standardisierungsstrategie zur sektorübergreifenden Digitalisierung der Energiewende erarbeitet und veröffentlicht (sog. BMWi-BSI-Roadmap). Auf der Basis dieser Strategie werden gemeinsam mit den Partnerbehörden, Verbänden und Unternehmen der Energiewirtschaft die wesentlichen Technischen Eckpunkte und die daraus resultierenden Anforderungen für ein sicheres Smart Grid der Zukunft festgelegt.

Mögliche Einbau- und Anwendungsfälle in der Niederspannung*	Stand 2021	Prognose (2030)
Verbraucher > 6.000 bis 100.000 kWh Jahresstromverbrauch	3,7 Mio.	4,1 Mio.
Verbraucher 4.000 bis 6.000 kWh/a mit dynamischem Tarif	-	0,4 Mio.
Verbraucher im Liegenschaftsmodell und Submetering-System	-	> 1,8 Mio.
Flexible Verbraucher	1,0 Mio.	> 5,2 Mio.
EEG/KWKG-Erzeuger 7 bis 100 kW	1,2 Mio.	2,2 Mio.
Prosumer mit PV 1 bis 7 kW und Steuerbarer Verbrauchseinrichtung	0,6 Mio.	1,2 Mio.
Öffentliche Ladeinfrastruktur für Elektrofahrzeuge	0,1 Mio.	> 0,5 Mio.
Summe	**6,6 Mio.**	**> 15,4 Mio.**

*Abbildung 1: Einsatz- und Absatzpotential für das iMSys – Jetzt und in Zukunft (*Quelle: Technische Eckpunkte)*

Die im Mai 2021 veröffentlichten Technischen Eckpunkte enthalten Leitplanken für die nächsten Schritte zur Weiterentwicklung der Standards für die Digitalisierung der Energiewende. Die Beschreibung der entsprechenden Entwicklungsstufen des iMSys erfolgte mit der Veröffentlichung des Stufenmodells (Version 2.0) im Juni.

Während Stufe 2 bereits erreicht ist, enthalten die darauf aufbauenden Entwicklungsstufen weitere funktionale und systemtechnische Erweiterungen für das iMSys, insbesondere für das SMGW: Stufe 3 fokussiert sich auf die Erweiterung der Monitoring-Möglichkeiten im intelligenten Energienetz für Kundinnen und Kunden sowie Betreiber (z.B. freiwillige hochfrequente Messdatenerfassung, Netzzustandsdatenversand) sowie der sicheren Steuerung von flexiblen Verbrauchs- und Erzeugungsanlagen. Zudem werden einheitliche Standards zur Anbindung weiterer Systemeinheiten geschaffen, um einen stufenweisen Rollout für weitere Einbaufälle auf der Basis bereits verfügbarer zertifizierter Technik zu ermöglichen.

Weiterentwicklung der Technischen Standards des BSI

Die Beschreibung der technischen Standards erfolgt in Schutzprofilen und Technischen Richtlinien des BSI. Anfang dieses Jahres hat das BSI gemeinsam mit den Partnerbehörden und den wesentlichen Stakeholdern der Energiewirtschaft die Technische Richtlinie BSI-TR-03109-1 für das SMGW grundlegend überarbeitet. Der nunmehr verabschiedete Stand gibt die Anforderungen der Stufe 2 vollständig wieder und legt die Basis für das nach Messstellenbetriebsgesetz notwendige Konformitätsbewertungsverfahren zum Nachweis der Interoperabilität. Zur weiteren Beschleunigung der Zertifizierungsverfahren sollen künftig Synergieeffekte zwischen den notwendigen eichrechtlichen (Bauartzulassung), funktionalen (TR) sowie IT-Sicherheitsbezogenen (Common Criteria) Zertifizierungen realisiert werden.

Die Re-Zertifizierung des dritten SMGW-Herstellers nach Common Criteria, dessen Geräte damit den Funktionsumfang der Stufe 2 erreichen, zeigt, dass der geplante Ausbaupfad mit funktionalen Software-Updates auf bestehenden SMGW realisierbar ist und die Technik den gesetzten Erwartungen gerecht wird.

Entwicklungsperspektiven des intelligenten Messsystems

Das Einsatzpotential des iMSys als Schlüsseltechnologie für die Digitalisierung der Energiewende ist enorm und entwickelt sich dynamisch weiter (vgl. Abbildung 1). Die Weiterentwicklungsmotoren sind die Dialogplattformen des BMWi und des BSI im Rahmen des Roadmap-Prozesses: Die Task-Forces zu einzelnen Themen wie Metering, Grid oder E-Mobilität sowie die AG Gateway-Standardisierung.

Zukünftig sollen weitere Mehrwerte für vielfältige energiewenderelevante Anwendungen auf Basis des iMSys etabliert werden. Bereits Ende 2021 sollen die technischen Standards für weitere Systemeinheiten der Stufe 3 (zur Steuerung, zur Einbindung des Submeterings sowie zur vereinfachten Anbindung weiterer Anlagen) beschrieben sein, sodass in der Folge entsprechende Zertifizierungen dieser Systemeinheiten möglich werden. ■

Weitere Informationen:
u.a. BMWi-/BSI-Roadmap, Technische Eckpunkte, Technische Richtlinien und Schutzprofile

https://bsi.bund.de/SmartMeter

Smart-eID

Mit der mobilen Identität in die Zukunft

von Philipp Zimmermann und Christopher Boysen, Referat Technische Anforderungen an eID-Komponenten und hoheitliche Dokumente

Der Einsatz mobiler Identitäten (Smart-eID) ist ein wichtiger Schritt zur Unterstützung der voranschreitenden Digitalisierung. Diese ermöglicht die sichere Speicherung einer digitalen Identität im Smartphone, sodass die Nutzung der Online-Ausweisfunktion auch ohne physisches Ausweisdokument möglich ist.

Mit der Einführung des neuen Personalausweises, des Aufenthaltstitels mit der Online-Ausweisfunktion und der eID-Karte für Unionsbürgerinnen und Unionsbürger wurde die Möglichkeit der gegenseitigen Authentifizierung von Ausweisinhaber und Diensteanbietern im Rahmen von E-Business- und E-Government-Anwendungen geschaffen. Im Zuge der digitalen Transformation von Geschäftsprozessen soll dieser Vorgang nun vereinfacht werden. Nutzerinnen und Nutzer sollen zukünftig die Online-Ausweisfunktion allein mit ihren Smartphones und ohne ein physisches Ausweisdokument nutzen können.

Der Beauftragte der Bunderegierung für Informationstechnik und Staatssekretär des Bundesinnenministeriums Dr. Markus Richter brachte das Projekt im Rahmen seines Neun-Punkte-Plans für ein digitales Deutschland auf den Weg. Die Zusammenarbeit zwischen dem Bundesministerium des Inneren, für Bau und Heimat und dem Bundesamt für Sicherheit in der Informationstechnik treibt die Umsetzung aktuell voran. Dabei übernimmt das BSI die technische Leitung sowie die technische Koordinierung des Projektes mit verschiedenen Auftragnehmern aus der Privatwirtschaft und integriert die Smart-eID in die bereits bestehende eID-Infrastruktur.

Einführung der Smart-eID

Die Einführung der Smart-eID ermöglicht das Ableiten von Identitätsdaten von einem Personalausweis, einem elektronischen Aufenthaltstitel oder der seit Januar 2021 neu eingeführten Unionsbürgerkarte auf das Smartphone. Dazu werden mithilfe der AusweisApp2, dem eID-Client des Bundes, die Identitätsdaten des Nutzers einmalig über die NFC-Schnittstelle von einem der genannten Dokumente ausgelesen und mithilfe eines Personalisierungsdienstes sicher im Smartphone gespeichert. Der Zugriff auf die gespeicherten Identitätsdaten wird durch eine sechsstellige Nutzer-PIN sichergestellt. Verfügt das Smartphone über ein verbautes Secure Element werden Zugriffschutz und Sicherheit der Daten erweitert. Der Hardwaresicherheitschip verfügt über kryptografische Funktionen und ermöglicht die sichere Speicherung und Verwendung von Schlüsselmaterial in der Hardware auf dem mobilen Gerät. Der Zugriff auf diese Funktionen kann durch einen Cryptographic Service Provider (CSP) gekapselt sein, der eine einheitliche Schnittstelle darstellt.

Zur Einführung der Smart-eID werden zunächst Smartphones mit Secure Element und CSP, wie zum Beispiel das Samsung S20, unterstützt. Weitere Geräte mit Secure Element und CSP oder mit Secure Element aber ohne CSP, Smartphones ohne Secure Element oder Geräte ohne Zugriffsmöglichkeit auf ein vorhandenes Secure Element sollen schnellstmöglich folgen, um möglichst vielen Nutzerinnen und Nutzern den Zugang zur Smart-eID zu ermöglichen.

Kontrolle über die eigenen Identitätsdaten

Nutzerinnen und Nutzer verfügen zu jedem Zeitpunkt über die volle Kontrolle ihrer Identitätsdaten, da diese ausschließlich lokal im eigenen Smartphone gespeichert werden. Jederzeit kann die Smart-eID über die AusweisApp2 gelöscht werden. Bei Verlust des Smartphones kann die Smart-eID entweder über die Fernlöschfunktion des Mobilbetriebssystems oder über den Sperr-Notruf (Tel.-Nr.: 116 116) mithilfe des Sperrkennworts gesperrt und somit unbrauchbar gemacht werden. Das Sperrkennwort wird der Nutzerin bzw. dem Nutzer einmalig beim Einrichtungsprozess der Smart-eID angezeigt und per Brief an die im Personalausweis hinterlegte Adresse gesendet.

Verfügt die Nutzerin bzw. der Nutzer über mehre Smartphones, kann für jedes Smartphone eine Smart-eID abgeleitet und eingerichtet werden. Eine Übersicht über sämtliche Smart-eIDs kann über den Auskunftservice des Ausweisherstellers abgefragt werden. Neben Typ und Hersteller des Smartphones werden auch das Erstellungsdatum und Ablaufdatum sowie das Sperrkennwort für die jeweilig Smart-eID angezeigt. Identitätsdaten der Nutzerinnen und Nutzer werden von diesem Dienst nicht verarbeitet oder erfasst.

Eine Selbstauskunft über die gespeicherten Identitätsdaten der Smart-eID ist mittels Online-Ausweisfunktion und der AusweisApp2 möglich. Wie bei der Selbstauskunft anderer Ausweisdokumente werden hierbei die gespeicherten Daten sicher entschlüsselt und der Nutzerin bzw. dem Nutzer angezeigt.

Die Entscheidungsfreiheit, ob die herkömmliche Online-Ausweisfunktion durch Nutzung eines physischen Ausweisdokumentes oder die Smart-eID verwendet wird, obliegt den Nutzerinnen und Nutzern und kann lediglich durch den Dienstanbieter auf den physischen Ausweis eingeschränkt werden, wenn dieser besondere Anforderungen an das Vertrauensniveau stellt.

Die Smart-eID stellt einen Meilenstein auf dem Weg in ein digitales Deutschland dar. Das BSI hat einen wichtigen Beitrag dazu geleistet, die Sicherheit und Zuverlässigkeit der Smart-eID für die Bürgerinnen und Bürger zu gewährleisten. ■

Gut abgesichert: die Bundestagswahl 2021

Interview mit Dr. Georg Thiel, Präsident des Statistischen Bundesamts und Bundeswahlleiter

Die Bundesrepublik hat gewählt – unter Beobachtung von Bundeswahlleiter Dr. Georg Thiel und seinem Team. Zahlreiche Maßnahmen hatten die Behörden im Vorfeld ergriffen, um eine sichere Durchführung der Wahl zu gewährleisten – darunter etliche zur informationstechnischen Absicherung der Wahl. Mit Erfolg: Zu größeren Zwischenfällen kam es nicht. Am 27. September 2021 um 6 Uhr morgens morgens war es dann so weit: Thiel konnte das vorläufige amtliche Ergebnis der Wahl zum 20. Deutschen Bundestag bekannt geben.

Herr Dr. Thiel, würden Sie für die Leserinnen und Leser Ihre Aufgabe am Wahlabend und Ihre Wahrnehmung des Verlaufs beschreiben?

Am Wahltag war ich mit meinem Team im Reichstagsgebäude in Berlin und hatte den Ablauf der Wahl im Blick. Ab 18 Uhr wurden die Stimmen in den Wahllokalen ausgezählt. Die Ergebnisse wurden als Schnellmeldungen über die Kreis- und Landeswahlleitungen bis zu mir weitergereicht und von meinem Team auf Plausibilität geprüft. Nach Vorliegen aller Wahlkreisergebnisse haben wir das vorläufige amtliche Wahlergebnis berechnet und um 6 Uhr am Montagmorgen bekannt gegeben.

„Wir waren gut vorbereitet – auch dank der Unterstützung des BSI.“

Insgesamt wurde die Bundestagswahl ordnungsgemäß durchgeführt. Die Probleme in vielen Berliner Wahllokalen haben uns natürlich im Nachgang der Wahl beschäftigt und wir mussten für eine transparente Aufarbeitung sorgen, aber davon abgesehen gab es keine größeren Zwischenfälle. Auch die Informationstechnik und deren Sicherheit haben uns keine wesentlichen Probleme bereitet. Hier waren wir gut vorbereitet – auch dank der Unterstützung des BSI. Unsere gemeinsame Arbeit hat sich ausgezahlt!

Nach einem Austausch mit mehreren Sicherheitsbehörden hat das BSI im Vorfeld der Wahl als mögliche Bedrohungsszenarien sowohl Cyber-Stalking/Mobbing, Informationsoperationen als auch ungezielte Angriffe wie bspw. Ransomware benannt. Was ist aus Ihrer Sicht die größte Bedrohung bei der Durchführung der Bundestagswahl?

Im Vorfeld der Wahl und auch am Wahltag gab es falsche und irreführende Informationen, die Wählerinnen und Wähler beeinflussen und Misstrauen gegenüber der Wahl und dem Wahlergebnis provozieren sollten. Daher haben wir einerseits die Lage in den klassischen und sozialen Medien beobachtet und andererseits von Seiten des Bundeswahlleiters proaktiv, umfassend und seriös informiert.

Daneben haben wir zusammen mit dem BSI die Informationstechnik abgesichert, die für die Übermittlung der vorläufigen Ergebnisse in der Wahlnacht eingesetzt wird. So gab es Schulungen für die Kommunen zur IT-Sicherheit und eine Handreichung für die Wahlorgane. Die Sicherheitsvorkehrungen wurden ständig überprüft und angepasst. Schnell identifizierte Angriffsversuche im Vorfeld der Wahl haben gezeigt, dass diese Sicherheitssysteme funktionieren.

In zahlreichen Medienberichten wurde im Vorfeld die Sicherheit der Briefwahl im Vergleich zur klassischen Urnenwahl angezweifelt. Können Sie sich erklären, warum es regelmäßig zu diesen Unsicherheiten kommt?

Bei der Briefwahl kann nicht in gleicher Weise wie im Wahllokal sichergestellt werden, dass die Wählerin bzw. der Wähler den Stimmzettel selbst und unbeobachtet ausgefüllt hat. Die Briefwahl beeinflusst damit die Prinzipien der freien und geheimen Wahl. Diese Grundsätze sicherzustellen, ist bei der Briefwahl Sache der Wählerinnen und Wähler selbst.

Auf der anderen Seite verfolgt der Gesetzgeber mit der Briefwahl das Ziel, den Grundsatz der allgemeinen Wahl zu gewährleisten, also möglichst allen Wählerinnen und Wählern – gerade in Pandemiezeiten – die Teilnahme an der Wahl zu ermöglichen. Das Bundesverfassungsgericht hat die 1957 eingeführte Briefwahl in mehreren Entscheidungen als verfassungskonform beurteilt.

Wie schätzen Sie den zukünftigen Einfluss der Digitalisierung auf den Wahlprozess ein? Der Einsatz welcher Art von wahlunterstützender Software wird für die nächsten Bundestagswahlen avisiert?

Für die Wahlvorbereitung ist die Ausweitung digitaler Angebote sinnvoll, um sie zu vereinfachen und Verfahren zu beschleunigen. Schon jetzt können Wahlberechtigte in vielen Gemeinden Briefwahlunterlagen über einen auf die Wahlbenachrichtigung gedruckten QR-Code beantragen. Ich setze mich auch dafür ein, dass Auslandsdeutsche ihren Antrag auf Eintragung ins Wählerverzeichnis zukünftig digital stellen können, um Probleme durch zu lange Postlaufzeiten zu reduzieren.

Für die Stimmabgabe selbst dürfte ein digitales Verfahren in der nächsten Zukunft wenig realistisch sein. Das Bundesverfassungsgericht hat für den Einsatz elektronischer Wahlgeräte hohe Hürden gesetzt: Die Stimmabgabe muss geheim erfolgen, aber die Auszählung aller abgegebenen Stimmen ist öffentlich und lässt sich wiederholen. Die Ermittlung des Wahlergebnisses ist transparent und für jeden nachvollziehbar. All das bieten kein Wahlcomputer und keine Online-Wahl.

Für die Auszählung ist eine Software-Unterstützung im Wahllokal nicht notwendig, zumal eine mögliche Ungültigkeit eines Stimmzettels nur individuell überprüft werden kann. Für die Zusammenführung der Ergebnisse aus allen 299 Wahlkreisen und die Ermittlung der Sitzverteilung nutzen wir natürlich eine Software. Auf unserer Webseite zeigen wir aber auch Schritt für Schritt die Berechnungen und die so ermittelte Verteilung: Es ist wichtig, dass diese immer auch ohne Nutzung der Software nachvollziehbar ist – diese Überprüfbarkeit und Transparenz ist ein wichtiger Grundsatz unseres Wahlsystems.

Am Wahltag waren außer dem Team des Bundeswahlleiters und des BSIs noch Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, das Informationstechnikzentrum Bund sowie der IT-Dienstleister elect-IT vor Ort. Welche Zusammenarbeit würden Sie in der Absicherung der Wahl gern ausbauen?

Keine Behörde und kein Wahlorgan allein könnten dies bewerkstelligen. Außer den genannten Akteuren arbeiten wir z. B. mit der Bundeszentrale für politische Bildung und dem Bundespresseamt zusammen, um über den Wahlablauf zu informieren und Falschinformationen vorzubeugen. Das Bundesinnenministerium und weitere Sicherheitsbehörden beobachten und analysieren fortlaufend die Sicherheitslage, um eine sichere Wahl für alle Bürgerinnen und Bürger zu gewährleisten.

Diese Zusammenarbeit vieler Expertinnen und Experten für die verschiedenen Aufgaben möchten wir auch bei zukünftigen Wahlen weiterentwickeln. ■

Der Bundeswahlleiter ist als unabhängiges Wahlorgan für die Durchführung von Bundestags- und Europawahlen verantwortlich. Mit dem Amt des Bundeswahlleiters wird nach ständiger Staatspraxis der Präsident des Statistischen Bundesamtes betraut. Dr. Georg Thiel hat beide Ämter seit dem 1. November 2017 inne.

BSI Basis-Tipp

Von überall Zugriff auf Ihre Daten

Fotos, Videos, Dokumente, Anwendungen und sogar Gesundheitsdaten werden zunehmend in der Cloud gespeichert. Cloud Computing kann als „Rechenleistung aus der Wolke“ verstanden werden. Die Wolke ist dabei ein bildlicher Ausdruck für Rechenzentren, die mit dem Internet verbunden sind. Ein Cloud-Dienst ist ein Onlinedienst, auf den Nutzerinnen und Nutzer über das Internet jederzeit zugreifen können – egal, mit welchem Endgerät. Dies kann beispielsweise ein PC, ein Smartphone oder ein internetfähiger Fernseher sein. Daten und Anwendungen werden nicht auf dem Gerät gespeichert, sondern auf entfernte Server ausgelagert. Die Vorteile liegen auf der Hand: Dokumente können von verschiedenen Personen bearbeitet, Fotos mit Freunden und Familie geteilt und Videos von überall gestreamt werden.

Beispiele für Cloud-Dienste

- Online-Speicher für Daten
- Web-Mail
- Smartwatch und Fitnesstracker
- Streaming-Plattformen
- Online-Programme zur Text- und Grafikbearbeitung

Weitere Informationen und der Wegweiser „Cloud-Dienste sicher nutzen“:

https://www.bsi.bund.de/cloud-sicherheit

Cloud-Dienste sicher nutzen
Cloud-Dienste sind praktisch, bergen aber auch Risiken. Wenn Sie einen Cloud-Dienst nutzen, lagern Sie private und schützenswerte Daten an den Cloud-Anbieter aus. Dabei geben Sie Kontrolle und Verantwortung ab und müssen sich vermeintlich darauf verlassen, dass Ihre Daten ausreichend geschützt werden.

Wir haben fünf wichtige Tipps zusammengestellt, mit denen Sie Ihre Daten in der Cloud schützen können:

- Sorgen Sie für einen ausreichenden Basisschutz Ihres Zugangsgerätes zum Beispiel durch Bildschirmsperren und eine automatische Update-Funktion.
- Sichern Sie den Zugang zu Cloud-Diensten mit einem sicheren Passwort und wenn möglich mit einem zweiten Faktor ab.
- Prüfen Sie die Datenschutzbestimmungen und Allgemeinen Geschäftsbedingungen des Anbieters und informieren Sie sich, ob Ihre Daten innerhalb der EU, in der die europaweite Datenschutz-Grundverordnung gilt, gespeichert werden. Die Risiko-Abwägung zur Nutzung des jeweiligen Cloud-Service muss dabei individuell getroffen werden.
- Achten Sie bei der Auswahl des Anbieters darauf, dass die Übertragung Ihrer Daten über eine sichere Verbindung erfolgt (erkennbar an https) und verschlüsseln Sie persönliche Daten, bevor Sie diese in die Cloud laden.
- Wenn Sie Daten mit anderen Personen teilen möchten, geben Sie so wenige Informationen wie möglich frei und begrenzen Sie die Freigabe zeitlich.

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

BSI

Save the Date

18. Deutscher IT-Sicherheitskongress

1.-2. Februar 2022 (digital)

Jetzt anmelden! Die Teilnahme ist kostenlos.

www.bsi.bund.de

Bestellen Sie Ihr BSI-Magazin!

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Referat 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 im Juni und im Dezember 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**.

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:	Dezember 2021
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-Mag21/714-1
Bildnachweise:	Titel: GettyImages © C.J. Burton; S. 4-5: © Secunet Security Networks AG; AdobeStock © only kim; S. 6: AdobeStock © your123; S. 9: AdobeStock © Graphic in Motion; S. 10-11: AdobeStock © Olga, © BMBF/Hans-Joachim Rickel, AdobeStock © AKS; S. 14-15: AdobeStock © Sikov, AdobeStock © Olena; S. 16: AdobeStock © phive2015; S. 18: AdobeStock © vpanteon; S. 23: AdobeStock © putilov denis; S. 24-25: AdobeStock © rh2010, © BSI; S. 26-27: © BSI; S. 30-31: GettyImages © gremlin, AdobeStock © Halfpoint, AdobeStock ©Jacob Lund; S. 32-33: AdobeStock ©TTstudio, © BSI, © BSI; S.36: © BSI; S.41: AdobeStock © Robert Kneschke; S.42: AdobeStock © TIMDAVIDCOLLECTION; S.44-45: AdobeStock © peterschreiber.media, AdobeStock © Olive; S. 47: AdobeStock © egor; S.49: © BSI; S.51: AdobeStock © Feodora; S. 54: AdobeStock © Inna; S. 56-57: AdobeStock © Grecaud Paul, GettyImages © merovingian; S.61: AdobeStock © Max Brosza; S .63: AdobeStock © ZinetroN; S.64: AdobeStock © rh2010; S.66-67: AdobeStock © pickup, AdobeStock © tippapatt; S. 68: AdobeStock © Ronny Behnert, © Bundeswahlleiter; S. 70-71: AdobeStock © AVTG, AdobeStock © katie martynova

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