BSI-Magazin 2023/01

Mit Sicherheit

Im Blickpunkt:

Digitaler Verbraucher-schutz

Das BSI

Interview mit der neuen BSI-Präsidentin Claudia Plattner

Digitale Gesellschaft

Cyber-Sicherheit im Gesundheitswesen

BSI International

Cyber Resilience Act: Einblick in den europäischen Gesetzesvorschlag

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Editorial

Liebe Leserin, lieber Leser,

vom Homeoffice über das Onlinebanking bis hin zur Onlineanmeldung des Autos ist die Digitalisierung fester Bestandteil des Alltags einer und eines jeden von uns. Sie erleichtert uns an vielen Stellen das Leben. Wir brauchen die Digitalisierung, aber ohne Sicherheit ist sie zum Scheitern verurteilt. Und die Bedrohungslage in diesem Kontext wächst – das wissen wir, wenn wir in den BSI-Lagebericht oder auch einfach in die Nachrichten schauen: Die Anzahl der Cyberangriffe steigt, Deutschland ist ein attraktives Ziel und Lösungen für dieses Problem sind nicht einfach.

Soweit zur Ausgangslage. Doch wie gehen wir das an? Was wir benötigen, ist eine tragfähige Sicherheitsarchitektur, die Widerstandsfähigkeit bringt und uns ermöglicht, mit Angriffen umzugehen, ohne direkt umzufallen. Resilienz aufbauen, die Digitalisierung voranbringen und Cybersicherheit gestalten – genau darin sehe ich die Schwerpunkte der Arbeit von uns allen im BSI. Die wichtigsten Voraussetzungen dafür sind Zusammenarbeit und Austausch: Zum einen die Zusammenarbeit im öffentlichen Bereich mit Behörden, Kommunen, Ländern und dem Bund – und das auch über die Grenzen Deutschlands hinaus mit europäischen und internationalen Partnern. Zum anderen der Austausch mit Wissenschaft, Wirtschaft, Politik und Gesellschaft bis hin zu den einzelnen Verbraucherinnen und Verbrauchern.

Durch diese Schwerpunkte ergeben sich Handlungsfelder, mit denen wir ebenso dringliche wie komplexe Aufgaben vor der Brust haben. Wenn ich aber eins nach meinen ersten Wochen sagen kann, dann dass ich der vollen Überzeugung bin, dass wir als BSI alles mitbringen, um diese Aufgaben gemeinsam voller Tatendrang anzugehen. Ich freue mich darauf, in meiner neuen Rolle als Präsidentin, aber vor allem – wie ich es sehe – als Teil des starken #TeamBSI daran mitzuwirken. Wie wir diese Schwerpunktthemen angehen und welche Inhalte uns gerade besonders umtreiben, erfahren Sie in dieser Ausgabe des BSI-Magazins.

Herzliche Grüße
Ihre

Claudia Plattner
Präsidentin des Bundesamts für Sicherheit
in der Informationstechnik

Inhalt

IT-Sicherheit in der Praxis

BSI International

Digitale Gesellschaft

BSI-Positionspapier zu Chancen und Risiken von KI-Sprachmodellen

Große KI-Sprachmodelle, so genannte Large Language Models (LLMs), sind in der öffentlichen Diskussion omnipräsent. Insbesondere die Ankündigung und Veröffentlichung von Modellen wie ChatGPT haben KI-Sprachmodelle schnell bekannt gemacht. Das BSI hat ein Positionspapier veröffentlicht, in dem es über Stärken, Schwächen und Risiken von KI-Sprachmodellen informiert – sowie über geeignete Vorsichtsmaßnahmen. Manipulierte Bilder, Videos und Sprachausgaben sind aus Sicht des BSI Risiken, denen mit geeigneten Vorsichtsmaßnahmen begegnet werden sollte. So kann z. B. die Authentizität von Texten und Nachrichten durch Verschlüsselngsverfahren nachgewiesen werden, mit denen man ihre Urheberschaft technisch belegen kann.

Unternehmen oder Behörden, die über die Integration von LLMs in ihre Arbeitsabläufe nachdenken, sollten darüber hinaus eine Risikoanalyse für ihren konkreten Anwendungsfall durchführen und die im Positionspapier genannten Risiken dahingehend evaluieren, ob diese für ihre Arbeitsabläufe eine Gefahr darstellen. Darauf aufbauend sollten existierende Sicherheitsmaßnahmen angepasst werden.

KI-Sprachmodelle sollten aus Sicht des BSI derzeit als Werkzeuge betrachtet werden, deren Ergebnisse, etwa bei der Erstellung von Programmcode oder Texten, durch eine menschliche Intelligenz überprüft werden sollten.

Weitere Informationen:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Grosse_KI_Sprachmodelle.pdf?__blob=publicationFile&v=2

Informationssicherheitsmanagement in der IT-Konsolidierung Bund

Im März 2023 wurde vom CIO Board, dem verantwortlichen Entscheidungsgremium für alle operativen Fragestellungen der Verwaltungsdigitalisierung des Bundes, die Neufassung der „Informationssicherheitsrichtlinie IT-Konsolidierung Bund“ beschlossen. Sie enthält für die IT-Konsolidierung Bund (ITKB) hinsichtlich der Informationssicherheit u. a. Regelungen zu Verantwortlichkeiten, Informationsaustausch, zentralen Prüfungen und zum Verbundrisikomanagement.

Ein Kernelement ist die Einrichtung eines Informationssicherheitsmanagementsystems für die ITKB inklusive eines vom BSI gestellten Informationssicherheitsbeauftragen für die IT-Konsolidierung Bund, der sich um Aufbau, Betrieb und Weiterentwicklung dieses Systems kümmert. Hintergrund: Im Großprojekt ITKB wird seit 2015 die IT der Bundesbehörden auf wenige IT-Dienstleister zusammengeführt. Ein Ziel ist, bei steigender Komplexität der IT-Systeme und zunehmenden Cyber-Bedrohungen ein angemessenes Informationssicherheitsniveau zu gewährleisten. IT-Lösungen, die bisher von verschiedenen Behörden eigenverantwortlich betrieben wurden, werden durch die Projekte der ITKB zukünftig zentral und standardisiert bereitgestellt.

Um in diesem komplexen Verbund aus Behörden und Dienstleistern Informationssicherheit gewährleisten zu können, ist es erforderlich, die bestehenden Informationssicherheitsmanagementsysteme der beteiligten Institutionen zu verzahnen. Das zentrale System des ITKB soll dies leisten.

#einfachaBSIchern: Ein smarter Ausblick

Die bundesweite Kampagne, die unter dem Motto #einfachaBSIchern für digitale Sicherheit im Alltag sensibilisiert, geht in die nächste Runde. Auch in diesem Jahr wird #einfachaBSIchern auf informative und humoristische Weise weitere Themen in den Fokus nehmen. Eine erste Themenkampagne legt den Schwerpunkt auf die IT-Sicherheit von vernetzten Geräten. Um auf die Problematik von Fremdzugriffen auf ungeschützte Geräte aufmerksam zu machen, nimmt die Kampagne einige smarte Geräte in den Blick und weist auf humorvolle Art darauf hin, dass die Geräte mehr Freude bringen, wenn vorab ein paar Sicherheitsvorkehrungen getroffen werden.

Eine weitere Themenkampagne in diesem Jahr zielt darauf ab, das dynamische Produktkennzeichen des BSI bei Verbraucherinnen und Verbrauchern bekannter zu machen. Das IT-Sicherheitskennzeichen sorgt für Transparenz bei den vom Hersteller zugesicherten Produkteigenschaften sowie aktuellen Sicherheitsinformationen und ermöglicht damit eine informierte Kaufentscheidung. Dabei wird das Kennzeichen nicht nur für smarte Geräte vergeben, sondern bspw. auch für Breitbandrouter und E-Mail-Dienste.

Über die Kampagne #einfachaBSIchern hat das BSI im vergangenen Jahr erneut eine sehr große Reichweite erzielt. Durch die Alltagsheldinnen und -helden der IT-Sicherheit werden die Verbraucherinnen und Verbraucher seitdem wiederholt für Risiken im digitalen Alltag sensibilisiert. Hierbei wird auf IT-Sicherheitsthemen in den Bereichen Homeoffice, Onlineshopping, Smarthome, Online Gaming und Social Media aufmerksam gemacht.

Weitere Informationen: www.einfachabsichern.de

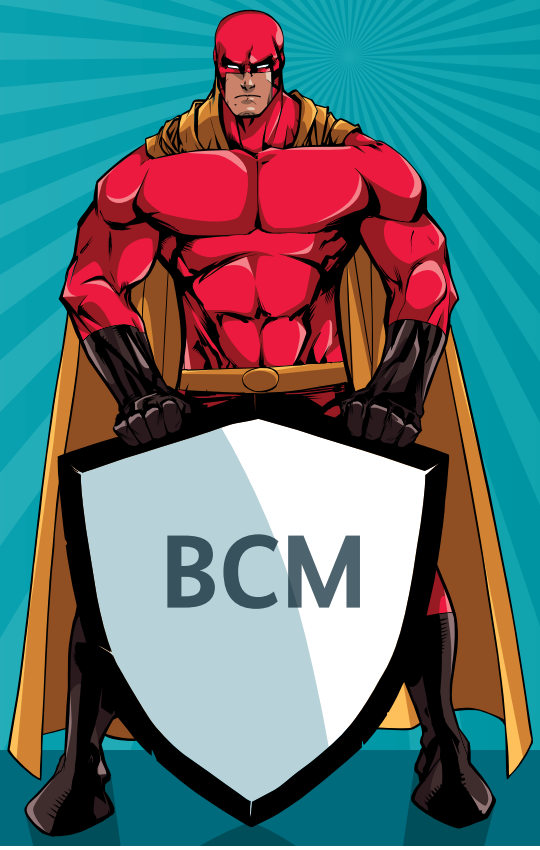
Internationale Cyber-Sicherheitsbehörden fordern sichere IT-Produkte

Qualitätsmängel in Soft- und Hardware-Produkten erhöhen die Angriffsfläche für Cyber-Kriminelle und gefährden damit ganze IT-Infrastrukturen. Das BSI appelliert daher an die Herstellervon IT-Produkten, Sicherheitsaspekte bereits bei der Entwicklung stärker zu berücksichtigen und die Geräte in einer sicheren Konfiguration auszuliefern. Gemeinsam mit seinen Partnerbehörden in den USA (CISA), Kanada (CCCS), Großbritannien (NCSC UK), den Niederlanden (NCSC NL), Australien (ACSC) und Neuseeland (CERT-NZ) hat das BSI daher Empfehlungen an IT-Hersteller veröffentlicht, die Grundsätze „security-by-design“ und „security-by-default“ stärker in ihre Produktentwicklung zu implementieren, und gibt Hinweise zur Umsetzung.

Die gemeinsame internationale Veröffentlichung verdeutlicht, dass Fragen der IT-Sicherheit nur im Verbund mit gleichgesinnten internationalen Partnern gelöst werden können. Sie unterstreicht zudem die Bedeutung des Themas und den dringenden Handlungsbedarf.

Weitere Informationen:

https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default



Mehr Resilienz durch Business Continuity mit IT-Grundschutz

Der BSI-Standard 200-4 BCM ist final

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

Ob der Ausfall eines Rechenzentrums, die Zerstörung einer Produktionsstätte infolge eines Naturereignisses oder eine Cyber-Attacke auf die gesamte IT-Infrastruktur – Institutionen sind einer stetig wachsenden Bedrohungslage ausgesetzt, die zu einer existenzbedrohenden Unterbrechung des Geschäftsbetriebes führen kann. Der BSI-Standard 200-4 Business Continuity Management (BCM) hilft, sich bestmöglich auf Schadensereignisse vorzubereiten, und trägt somit zu ganzheitlicher organisatorischer Resilienz bei (Abbildung rechts).

Der BSI-Standard 200-4 steht nach zwei sogenannten Community-Draft-Phasen, in denen alle interessierten Anwender und Anwenderinnen ihr Feedback geben konnten, bereit. So ließ sich sicherstellen, dass die Ansätze und die Methodik des BSI-Standards 200-4 nicht nur den eigenen Ansprüchen und den aktuellen, theoretischen Entwicklungen im Bereich BCM genügen, sondern auch den ersten Praxistest erfolgreich überstanden haben.

PRAXISERPROBTES STANDARDWERK ALS ANLEITUNG FÜR ALLE

Schon zu Beginn der Entwicklung des neuen BSI-Standards stand fest, dass dieser einen anleitenden, erklärenden Charakter erhalten soll. Grund war die Erfahrung, dass viele Institutionen sich überhaupt erst einmal mit dem Thema BCM systematisch im Rahmen eines eigenen Managementsystems (BCMS) auseinandersetzen müssen.

Daher beschreibt der BSI-Standard alle Schritte eines solchen BCM-Prozesses so, dass auch Institutionen ohne tiefergehende Vorkenntnisse und externe Hilfe dazu befähigt werden, selbstständig ein BCMS aufzubauen. Um den Einstieg weiter zu erleichtern, wurde auch ein Stufenmodell eingeführt. Es ermöglicht erst einen schnellen, rudimentären Einstieg zur Existenzsicherung oder sofort die Etablierung eines ausgereiften, zur entsprechenden ISO-Norm (ISO 22301:2019) kompatiblen Managementsystems. Zusätzlich erleichtert es den Übergang zwischen diesen Stufen.

UMFANGREICHE HILFSMITTEL ZUR PRAXISNAHEN UNTERSTÜTZUNG

Ein weiterer, wesentlicher Bestandteil, um einen selbstständigen Einstieg in das Thema BCM zu ermöglichen, sind die umfangreichen Hilfsmittel zum BSI-Standard 200-4.

Es werden zwei Kategorien von Hilfsmitteln angeboten:

- **Dokumentvorlagen**
  - einfache Papiervorlagen, z. B. für die Leitlinie oder das Notfallhandbuch
  - interaktiver Auswertungsbogen zur Business Impact Analyse (BIA)
- **weiterführende Informationen**

Der Standard und die Dokumentvorlagen sind so aufeinander abgestimmt, dass sich die Dokumentvorlagen unter Anleitung der entsprechenden Kapitel des BSI-Standards 200-4 direkt ausfüllen bzw. anpassen lassen. Die Dokumentvorlagen bieten bereits umfangreiche Standardtexte, die nur noch an die Lage der eigenen Institution angepasst werden müssen.

Neben den Dokumentvorlagen gibt es weitergehende, nicht normative Informationen zu ausgewählten Themen. So werden z. B. weitergehende Informationen zum Tool-Einsatz oder zur Bewältigung von Schadensereignissen gegeben.

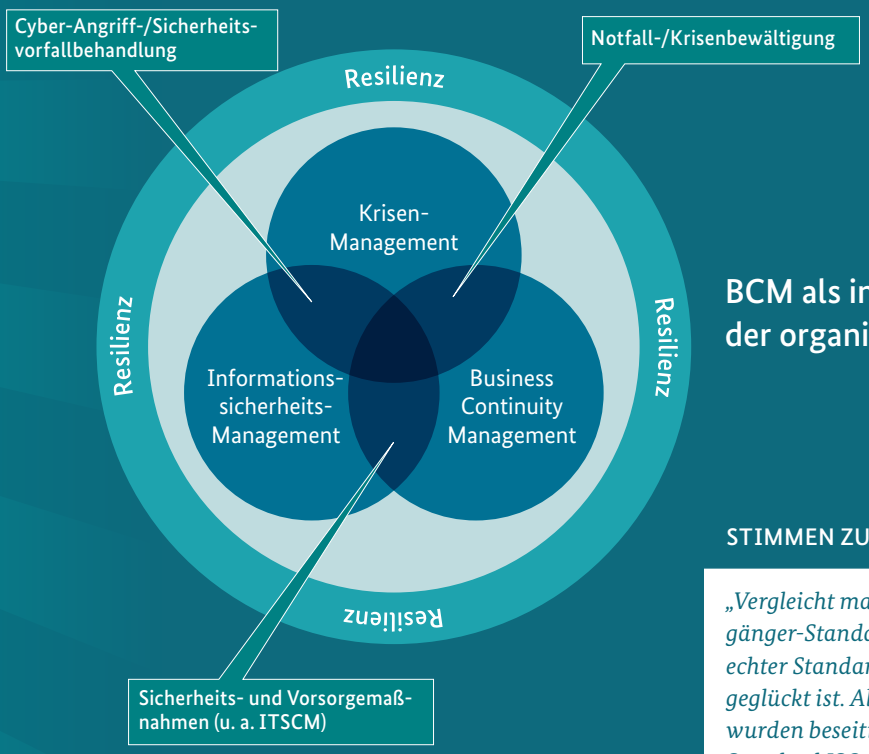


Abbildung: BSI

BCM als integraler Bestandteil der organisatorischen Resilienz

STIMMEN ZUM BSI-STANDARD 200-4 BCM:

„Vergleicht man den neuen BSI-Standard 200-4 mit dem Vorgänger-Standard (100-4), muss man konstatieren, dass nun ein echter Standard für das Business Continuity Management (BCM) geglückt ist. Alle bisherigen, zum Teil unklaren Definitionen wurden beseitigt bzw. durch präzise, an den internationalen Standard ISO 22301 angelehnte Definitionen ersetzt. Dieser Standard eignet sich auch für alle, die noch nie mit dem Thema BCM in Kontakt gewesen sind!“

Matthias Rosenberg, FBCI,
Fellow of the Business Continuity Institute

NICHT NUR FÜR EINSTEIGER, SONDERN AUCH FÜR POWERUSER

Im Fokus stehen neben Einsteigenden auch erfahrene BCM-Anwendende. Mithilfe des bereitgestellten, übersichtlichen Anforderungskataloges lässt sich die Kompatibilität mit dem BSI-Standard 200-4 schnell nachvollziehen. Dieser Anforderungskatalog basiert auf der letzten Aufbaustufe, dem Standard-BCMS, die ein vollumfängliches, ISO-kompatibles BCMS darstellt. Die Kompatibilität zu der relevanten ISO-Norm ISO 22301:2019 lässt sich durch das veröffentlichte ISO-Mapping nachvollziehen, in dem jeder ISO-Control mindestens eine entsprechende Anforderung aus dem BSI-Standard 200-4 zugeordnet ist. Durch den Anleitungscharakter kann der BSI-Standard 200-4 auch zur Umsetzung dieser ISO-Norm genutzt werden. Das Mapping erlaubt eine Transition zwischen beiden Normen.

BSI-STANDARD 200-4 ALS LEBENDES STANDARDWERK

Anwendern und Anwenderinnen steht mit dem BSI-Standard 200-4 ein fortschrittlicher Standard zur Verfügung, den umfangreiche Hilfsmittel abrunden. Selbstverständlich setzt das BSI auch weiterhin auf den Austausch mit der Community. Weitere Anregungen oder auch Kritik sind willkommen unter it-grundschutz@bsi.bund.de. ■

„Mit dem BSI 200-4 liegt ein strukturell und inhaltlich völlig überarbeiteter Standard für das Business Continuity Management vor, der sich dennoch am Kern seines Vorgängers BSI 100-4 orientiert. Die englische Bezeichnung des Titels macht bereits die Nähe zum ISO 22301 deutlich, zu dem der Standard kompatibel ist. Der BSI 200-4 ist sowohl für Praktiker als auch für Einsteiger durch die Überarbeitung ein noch wertvolleres Hilfsmittel für die Implementierung und Weiterentwicklung eines BCM geworden. Ergänzungen zum Standard wie der Anforderungskatalog, das Glossar und die online bereitgestellten Dokumentvorlagen zeigen die klare Umsetzungsorientierung im Unterschied zu den internationalen BCM-Standards und -Normen. Für die Zukunft des Standards wünsche ich mir kürzere Aktualisierungsrhythmen, um der Dynamik des Themas gerecht zu werden (Stichwort: Resilienz). Allen Lesern und Anwendern das Glück, dieses Wissen so wenig als möglich praktisch anwenden zu müssen.“

Matthias Hämmerle,
haemmerle-consulting & bcm-news.de

Weitere Informationen:

www.bsi.bund.de/gs-standard200-4

Kooperation und Kommunikation: Gemeinsam für die Cyber-Abwehr in Deutschland

Ein Blick hinter die Kulissen beim Nationalen Cyber-Abwehrzentrum

von Roland Hartmann, stv. Koordinator des Nationalen Cyber-Abwehrzentrums, und Carolin Wagner, Referat Vorfallsbearbeitung und Verbindungsstelle Nationales Cyber-Abwehrzentrum im BSI

Täglich finden Cyber-Angriffe zur Einflussnahme auf die Gesellschaft und staatliche Entscheidungen sowie Cyber-Spionage und -Sabotage bis hin zur Unterstützung militärischer Operationen statt. Mit der Cyber-Sicherheitsstrategie für Deutschland 2011 wurde das Nationale Cyber-Abwehrzentrum (Cyber-AZ) geschaffen und seitdem kontinuierlich weiterentwickelt.

Das Cyber-Abwehrzentrum wurde als gemeinsame, behörden- und institutionenübergreifende Plattform für einen verbesserten und beschleunigten Informationsaustausch eingerichtet. Zudem soll es zur stärkeren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Sicherheitsvorfälle in Deutschland beitragen.

WER ARBEITET BEIM CYBER-AZ?

Acht gleichberechtigte Kernbehörden arbeiten kontinuierlich im Cyber-AZ zusammen:

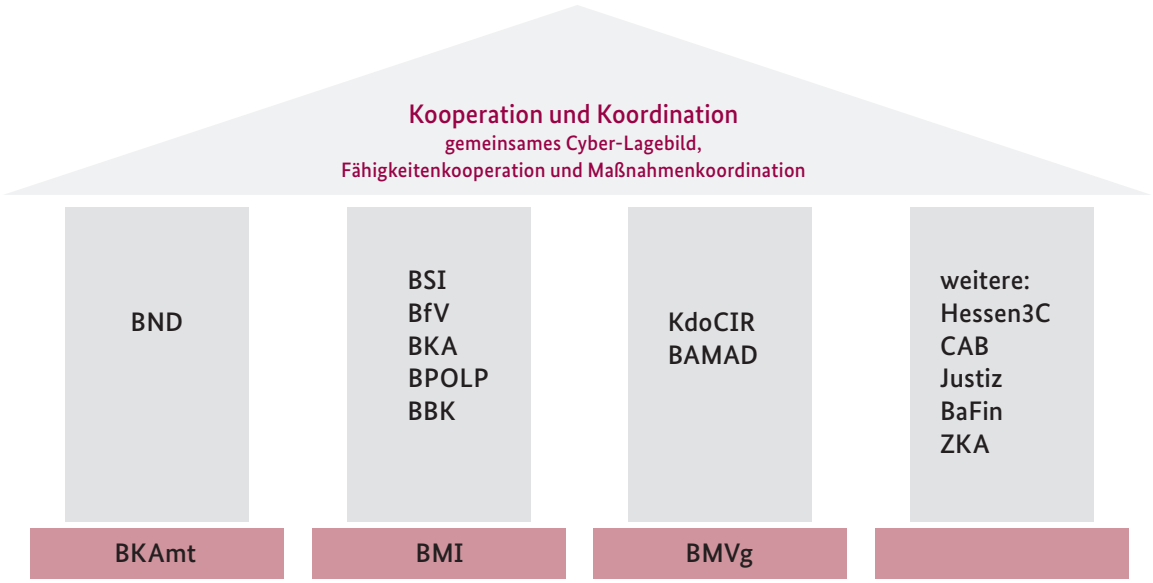
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
- Bundesamt für den Militärischen Abschirmdienst (BAMAD)
- Bundesamt für Verfassungsschutz (BfV)
- Bundeskriminalamt (BKA)
- Bundesnachrichtendienst (BND)
- Bundespolizeipräsidium (BPOLP)
- Kommando Cyber- und Informationsraum (KdoCIR) und
- BSI

Zudem arbeiten das Zollkriminalamt (ZKA) und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) als assoziierte Behörden im Cyber-AZ mit. In den letzten beiden Jahren sind zudem die Schwerpunktstaatsanwaltschaften Köln und Bamberg sowie die Cyber-Abwehr-Bayern (CAB) und das Hessen CyberCompetenceCenter (H3C) hinzugekommen.

„Das Cyber-Abwehrzentrum leistet einen unverzichtbaren Beitrag, die Cyber-Fähigkeiten der Sicherheitsbehörden zu vernetzen. Besonders in Krisenzeiten ist ein eng koordiniertes Vorgehen zum Schutz der Cyber-Sicherheit unerlässlich."

Bundesinnenministerin Nancy Faeser bei ihrem Besuch des Cyber-Abwehrzentrums am 8. August 2022

Diese Erweiterung unterstreicht den gesamtstaatlichen und föderativen Ansatz des Cyber-AZ zur Aufrechterhaltung der Cyber-Sicherheit in Deutschland. Das Cyber-AZ wird stetig organisatorisch und strategisch weiterentwickelt, um den zunehmenden Herausforderungen, z. B. bei der Digitalisierung, gerecht werden zu können. Dies hat die Bundesregierung unter anderem in ihrer Digitalstrategie 2022 verankert.



NATIONALES CYBER-ABWEHRZENTRUM

Das Nationale Cyber-Abwehrzentrum ist die Kooperations-, Kommunikations- und Koordinationsplattform der zuständigen (Sicherheits-) Behörden unterschiedlicher Ressorts, die insbesondere durch ein gemeinsames, aktuelles und umfassendes Cyber-Sicherheitslagebild für Deutschland, strategische Berichterstattungen sowie durch die koordinierende operative und interdisziplinäre Fallbearbeitung unverzichtbare Beiträge zur gesamtstaatlichen Cyber-Sicherheit und somit – auch im Krisenfall – zur Handlungsfähigkeit der Bundesregierung leistet.

MODERIEREN UND INITIIEREN

Die operative Arbeit im Cyber-AZ übernehmen aus den unterschiedlichen Behörden und Einrichtungen entsandte Mitarbeitende. Diese übernehmen vier unterschiedliche Rollen: im Koordinatorenteam, als Verbindungspersonen, im Lageteam und in der Geschäftsstelle. Die Funktionen des Koordinators und seiner zwei Stellvertreter gibt es seit der Neuausrichtung der Zusammenarbeit in 2019. Er moderiert und initiiert notwendige Entscheidungen durch die beteiligten Behörden und Einrichtungen. Alle Behörden und Einrichtungen des Cyber-AZ sind durch Verbindungspersonen vor Ort vertreten. In den täglichen Austausch sind mittlerweile insgesamt über 50 Verbindungspersonen eingebunden. Die Mitarbeitenden in der Geschäftsstelle unterstützen das Cyber-AZ besonders organisatorisch.

DIE LAGE BEOBACHTEN UND BEWERTEN

Das Lageteam erstellt einmal wöchentlich die Cyber-Sicherheitslage Deutschland (CSLD) – das wohl bekannteste Produkt des Cyber-AZ. Es enthält die relevanten Informationen, kongregiert aus den täglichen Lagebesprechungen und zahlreichen behördlichen Lageprodukten, sowie die wichtige behördenübergreifende Bewertung dieser Lageinformationen. Adressiert werden mit den Produkten des Cyber-AZ vornehmlich die Managementebene, d. h. jeweils Ministerien und Behörden des Bundes, aber auch der Länder, die aufgrund ihrer Arbeit einen Bezug zum Thema Cyber-Sicherheit haben.

Weniger sichtbar, aber dennoch sehr wirkungsvoll für die Koordinierung kann das Cyber-AZ binnen kürzester Frist alle vertretenen Behörden und Einrichtungen an einen Tisch holen und – unter Beachtung der geltenden gesetzlichen Bestimmungen – Informationen zu konkreten akuten Sachverhalten oder Vorfällen austauschen. Die Umsetzung von Aktivitäten verbleibt jedoch in der Zuständigkeit der jeweiligen Behörden und Einrichtungen – über eigene operative Befugnisse und Weisungsbefugnisse verfügt das Cyber-AZ nicht.

DAS BSI IM CYBER-AZ

Das BSI nimmt als die Cyber-Sicherheitsbehörde des Bundes eine zentrale Rolle im Cyber-AZ ein. Bei Bedarf und unter Berücksichtigung der Interessen des Betroffenen kann sich das BSI im Cyber-AZ mit anderen Behörden austauschen sowie weitere Maßnahmen koordinieren, um bestmöglich helfen zu können. So ergibt sich durch das gegenseitige Anreichern ein Gesamtlagebild mit weiteren Perspektiven, das aussagekräftiger ist als die einzelnen Zuarbeiten. Die vertrauensvolle Zusammenarbeit mit den Partnern im Cyber-AZ ist für das BSI essenziell, um weitere Informationen zu Cyber-Sicherheitsthemen und -vorfällen schnell, fundiert und unkompliziert zusammenzutragen. So ist es auch bei komplexeren Sachverhalten möglich, dass Betroffenen zuverlässig und aus einer Hand geholfen werden kann. Für das BSI ist das Cyber-AZ die erprobte Plattform für Kommunikation, Kooperation und Koordination zur abgestimmten Cyber-Abwehr mit den Sicherheitsbehörden und eine wichtige Säule für die Cyber-Sicherheit in Deutschland. ■

Auf dem Weg zum sicheren digitalen Zentralbankgeld

BSI entwirft Technische Richtlinie für CBDC

von Sabine Mull und Roland Kirsch, Referat Cyber-Sicherheit im Gesundheits- und Finanzwesen, sowie Dr. Ute Gebhardt und Dr. Christian Berghoff, Referat Bewertungsverfahren für eID-Technologien in der Digitalisierung

Weltweit wird über die Einführung von digitalem Zentralbankgeld diskutiert. Auch die Europäische Zentralbank (EZB) als ausgebende Stelle befasst sich intensiv mit diesem Thema. Durch die Erstellung einer Technischen Richtlinie leistet das BSI seinen Beitrag zur sicheren technischen Umsetzung solcher Währungen.

In den letzten Jahren haben weltweit in verschiedenen Währungsräumen die Aktivitäten zur Einführung von digitalem Zentralbankgeld (Central Bank Digital Currency, CBDC) deutlich zugenommen. Insbesondere in China erfolgt bereits eine umfangreiche Erprobungsphase. Auch die EZB befasst sich intensiv mit dem Thema und denkt über die Einführung eines digitalen Euro nach. Eine positive Entscheidung hierzu wird bis Ende 2023 erwartet.

EIGENSCHAFTEN VON CBDC

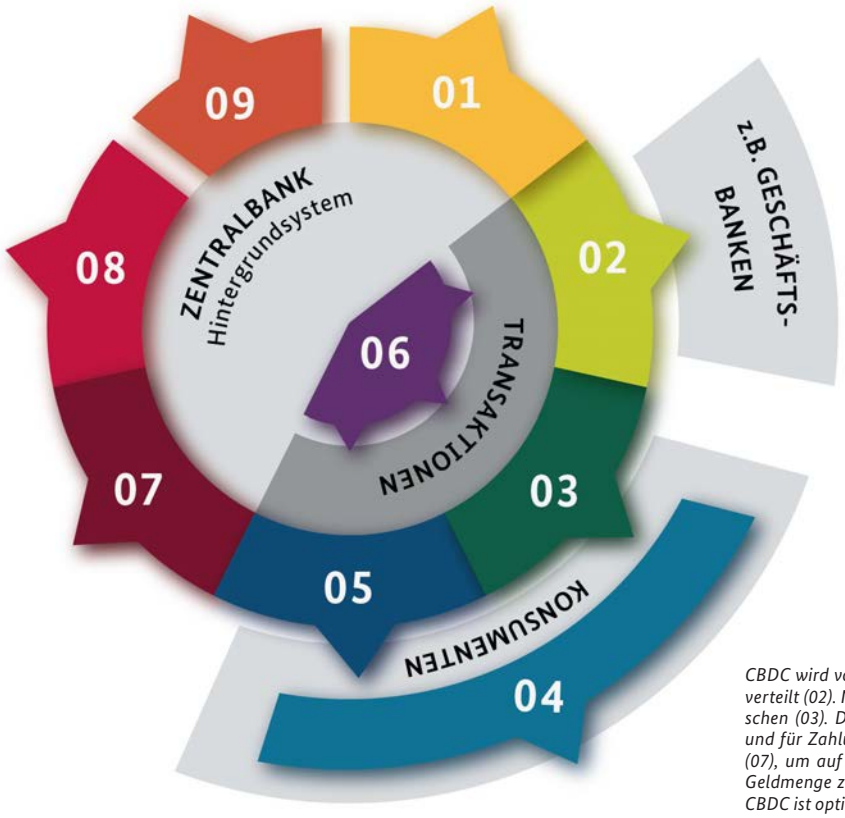
Auch wenn es bisher keine übergreifende Definition von CBDC gibt und die Ausgestaltung in verschiedenen Währungsräumen sicherlich variieren wird, so kristallisieren sich bereits einige grundlegende Eigenschaften von CBDC heraus. Diese sind denen von Bargeld als traditionellem Zentralbankgeld nachgebildet. Finanzpolitisch liegt der wesentliche Unterschied zu Kryptowährungen und Giralgeld der Geschäftsbanken darin, dass CBDC direkt von der jeweiligen Zentralbank herausgegeben wird. Als öffentliches Angebot muss CBDC einem besonders breiten Kreis von Nutzenden zugänglich sein. Dies soll vor allem durch einen barrierefreien Zugang ermöglicht werden. Zugleich gibt es an CBDC die Erwartung, dass sich mit diesen digitalen Währungen Zahlungen anonym, instantan oder ohne Internetverbindungen abwickeln lassen.

ROLLE DES BSI

Gibt eine Zentralbank digitales Geld aus und nutzt die Bevölkerung das digitale Zentralbankgeld großflächig, erhalten die zugrundeliegenden IT-Systeme dadurch eine wichtige volkswirtschaftliche Rolle. Das geht so weit, dass mit ihnen eine neue kritische Infrastruktur etabliert wird. Störungen und Manipulationen dieser Systeme, die zugleich attraktive Ziele für Angreifer darstellen, sind daher unbedingt zu verhindern. Die Systeme sollten daher gemäß dem Grundsatz „security by design“ entwickelt und implementiert werden und die genutzten Maßnahmen auf ein hohes IT-Sicherheitsniveau abzielen. Bislang werden die öffentlichen Diskussionen im Finanzbereich jedoch von finanzpolitischen Aspekten der CBDC dominiert und die IT-Sicherheit nicht im Detail behandelt.

Das BSI als Cyber-Sicherheitsbehörde des Bundes nimmt hier eine Vorreiterrolle ein, indem es das Thema aktiv angeht und wesentliche Leitplanken für die IT-Sicherheit setzt. Mit diesem Ziel ist die Technische Richtlinie TR-03179 „Central Bank Digital Currency“ des BSI entstanden.

Zielgruppe dieser TR sind zunächst die Anbieter von CBDC-Systemen (Backend und Frontend). Sie können die TR als Leitfaden oder möglicherweise als Basis für ein Zertifizierungsverfahren nutzen. Das BSI plant zudem, die Inhalte der TR in die Diskussionen um den digitalen Euro und potenziell auch in die internationale Standardisierung zum Thema CBDC einzubringen.



01 ERZEUGUNG
02 VERTEILUNG
03 GELDWECHSEL
04 SPEICHERUNG
05 ZAHLUNG
06 GÜLTIGKEITSPRÜFUNG
07 AKTUALISIERUNG
08 RÜCKRUF
09 WIEDERHERSTELLUNG (OPTIONAL)

CBDC wird von der Zentralbank erzeugt (01) und z. B. an Geschäftsbanken verteilt (02). Nutzer können dort sonstige Zahlungsmittel gegen CBDC tauschen (03). Diese können Nutzer auf geeigneter Hardware speichern (04) und für Zahlungen (05) nutzen. Die Zentralbank kann CBDC aktualisieren (07), um auf technische Fortschritte zu reagieren, oder zur Kontrolle der Geldmenge zurückrufen (08). Ein Prozess zur Wiederherstellung verlorener CBDC ist optional (09).

Abbildung: BSI

Die TR behandelt in einem ersten Teil zunächst die Anforderungen für die von der Zentralbank betriebenen Backend-Systeme und in einem zweiten Teil die Frontend-Systeme, mit denen die Endnutzer interagieren. Neben allgemeinen IT-Sicherheitsanforderungen, z. B. zu kryptografischen Verfahren, enthält die TR auch Vorgaben an die spezifischen Prozesse über den gesamten CBDC-Lebenszyklus (s. Abbildung oben).

HERAUSFORDERUNGEN AN DIE IT-SICHERHEIT

Herausforderungen an die sichere technische Ausgestaltung von CBDC bestehen insbesondere darin, die unterschiedlichen Bedürfnisse nach Fälschungssicherheit, Offline-Verfügbarkeit, Anonymität der Zahlungen und Usability in Einklang zu bringen.

Um Fälschungen zu erkennen, müsste grundsätzlich bei jeder Zahlung die Gültigkeit der genutzten CBDC von einem Hintergrundsystem der Zentralbank „online" geprüft und bestätigt werden (s. Abbildung oben, Schritt 06). Dies schränkt jedoch die Offline-Verfügbarkeit ein, weshalb unter geeigneten Bedingungen und in definierten Ausnahmefällen solche Online-Gültigkeitsprüfungen durch geeignete Offline-Prüfmechanismen ersetzt und somit auch Offline-Zahlungen ermöglicht werden können.

Die TR CBDC adressiert diese Rahmenbedingungen und die damit verbundenen Zielkonflikte durch umfangreiche konkrete Anforderungen. Diese sind, soweit es möglich ist, zielorientiert formuliert und technologieneutral gehalten, um ausreichenden Spielraum für die technische Umsetzung von CBDC zu gewähren. Mit der Gestaltung der TR setzt sich das BSI proaktiv für den Weg zum sicheren Zentralbankgeld ein. ■

Weitere Informationen:

https://www.ecb.europa.eu/paym/digital_euro/html/index.de.html

Risiko Quantencomputing: Was ist zu tun?

Warum der Umstieg auf quantensichere Kryptografie jetzt auf die Agenda gehört

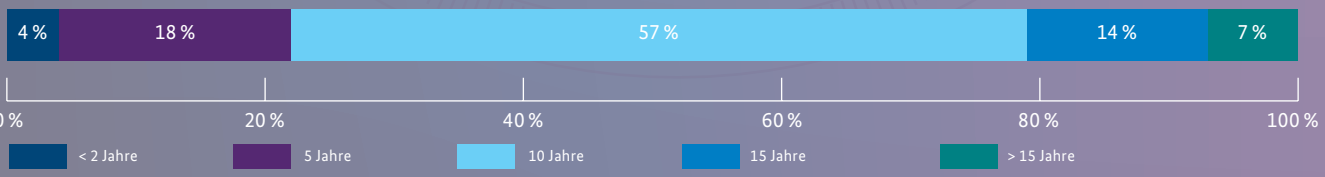
von Dr. Frank Damm und Hans-Peter Fischer, KPMG in Deutschland, Dr. Heike Hagemeier, Referat Technologie- und Forschungsstrategie, und Dr. Manfred Lochter, Referat Vorgaben an und Entwicklung von Kryptoverfahren

Kryptografische Verfahren, die heute noch als sicher gelten, können in Zukunft mit Quantencomputern gebrochen werden. Sie müssen daher in absehbarer Zeit durch neue, quantensichere Methoden ersetzt werden, beispielsweise durch die sogenannte Post-Quanten-Kryptografie. Um Staat, Wirtschaft und Gesellschaft bei diesem Thema bestmöglich zu unterstützen, haben das BSI und KPMG in Deutschland eine Umfrage unter CIOs und CISOs durchgeführt, deren Ergebnisse hier vorgestellt werden.

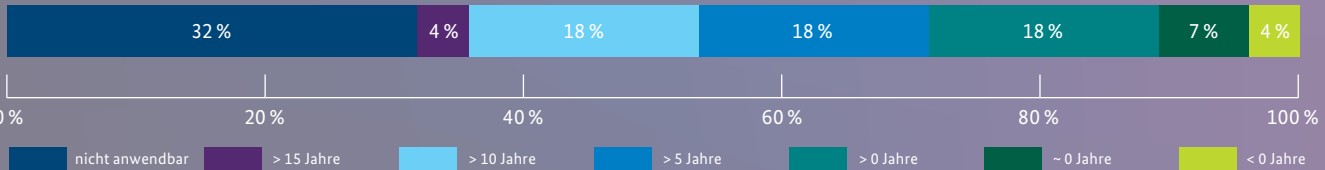
Quantencomputing nutzt die Gesetze der Quantenmechanik, um effiziente Berechnungen durchzuführen, und kann potenziell manche Probleme lösen, bei denen die heute schnellsten Supercomputer versagen. Zwar ist trotz vielversprechender Ankündigungen großer Anbieter noch unklar, wann Quantencomputing tatsächlich einsetzbar sein wird. Dennoch: Die Technologie existiert und wird immer leistungsfähiger. Bei Wettersimulationen, komplexen Klimaberechnungen, der Genomanalyse oder bei der Überwachung komplexer Verkehrsströme kann Quantencomputing für enorme Fortschritte sorgen.

Dagegen steht, dass die Technologie auch in der Lage sein wird, viele der gängigen Verschlüsselungsmethoden und Sicherheitsvorkehrungen für IT-Infrastrukturen auszuhebeln. Diese Verfahren sind Grundbausteine der IT-Sicherheit, auf die wir heute bauen und vertrauen, und im Zeitalter des Quantencomputings werden sie schlicht nicht mehr sicher sein.

Wann, schätzen Sie, werden Quantencomputer in der Lage sein, bestimmte, heute eingesetzte Verfahren zu brechen?



Geschätzte Zeit, um die der Grenzwert zur sicheren Umstellung auf Post-Quanten-Kryptografie verfehlt wird.



Abbildungen: KPMG in Deutschland

Wie hoch ist die maximale Dauer, für die Informationen durch Ihre Organisation vertraulich gehalten werden müssen?

Wann plant Ihre Organisation, mit der Umstellung auf quantensichere Kryptografie zu beginnen?

Wie lange wird Ihrer Meinung nach Ihre Organisation für die Realisierung der Quantenresistenz benötigen?

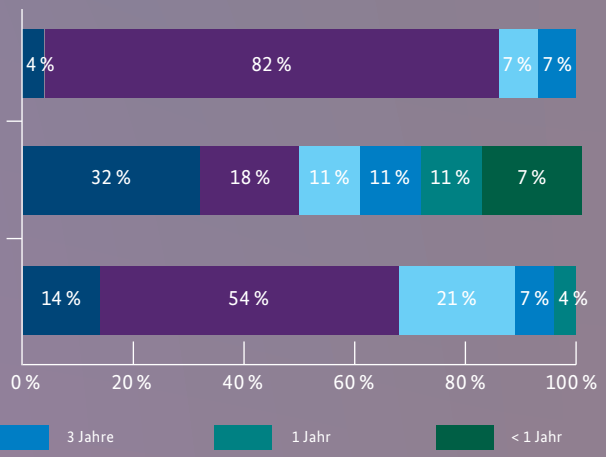


Abbildung: KPMG in Deutschland

BSI WARNT VOR AUSWIRKUNGEN AUF DIE IT-SICHERHEIT

Das BSI warnt schon seit Jahren vor der Bedrohung der Public-Key-Kryptografie durch Quantencomputing. Für den Hochsicherheitsbereich hat das Amt deshalb bereits die Migration zu quantensicheren Lösungen eingeleitet. Grundlage dafür ist die Arbeitshypothese, dass Anfang der 2030er Jahre kryptografisch relevante Quantencomputer zur Verfügung stehen werden. Das ist allerdings keine Prognose zur Verfügbarkeit von Quantencomputern, sondern ein Richtwert für die Risikobewertung.

Wie aber sieht es in der Industrie aus? Dazu haben BSI und KPMG 153 Unternehmen in Deutschland befragt. Ziel war es, herauszufinden, wie gut die Organisationen mit dem Thema und den Empfehlungen des BSI dazu vertraut sind: Wie schätzen sie die Situation generell und für sich ein? Was tun sie schon und was würde helfen, die Migration zu quantensicherer Kryptografie zu beschleunigen?

28 Unternehmen haben diese Fragen beantwortet. Die Auswertung der Ergebnisse zeigt, dass sich alle Teilnehmenden bereits für die Themen Quantencomputing und Kryptografie interessieren und die Auswirkungen von ausreichend leistungsfähigen Quantencomputern auf die Sicherheit als dramatisch ansehen.

„NOCH ZEHN JAHRE BIS ZUR VERFÜGBARKEIT KRYPTOGRAFISCH RELEVANTER QUANTENCOMPUTER“

Diese Arbeitshypothese des BSI für den Hochsicherheitsbereich zur Verfügbarkeit kryptografisch relevanter Quantencomputer deckt sich mit den Einschätzungen der teilnehmenden CIOs und CISOs aus den Unternehmen. Im Mittel erwarten sie, dass Quantencomputer in 10,4 Jahren in der Lage sein werden, aktuell eingesetzte kryptografische Verfahren zu brechen. Kritischer ist die Selbsteinschätzung, dass sie nach eigener Einschätzung die Migration auf quantensichere Kryptografie 6,5 Jahre zu spät abgeschlossen haben werden. Nur elf Prozent der Teilnehmenden sehen eine Chance, Quantensicherheit zu erreichen, bevor die Vertraulichkeit ihrer Daten verletzt wird. Dabei bewerteten 97 Prozent der Teilnehmenden die generelle Relevanz von Quantencomputing für die Sicherheit von heute eingesetzten kryptografischen Verfahren als „hoch“ oder „eher hoch“. Auch das durchschnittliche Risiko für die Daten in der eigenen Organisation schätzen 65 Prozent als „hoch“ oder „eher hoch“ ein.

NUR JEDER VIERTE BERÜCKSICHTIGT DIE GEFAHREN DURCH QUANTENCOMPUTING IM RISIKOMANAGEMENT

Dennoch wird die Gefährdung durch Quantencomputing nur von 25 Prozent der antwortenden Organisationen im Risikomanagement berücksichtigt. Zudem gab jeder dritte Teilnehmende an (32 %), dass die Frage, wann seine Organisation mit der Umstellung beginnen will, bei ihnen „nicht anwendbar/relevant“ sei. Dies legt nahe, dass in diesen Fällen eine Umstellung noch nicht einmal geplant ist. Nach den Faktoren befragt, die Investitionsentscheidungen für quantensichere Kryptografie begünstigen würden, nannten 96 Prozent regulatorische Vorgaben und 89 Prozent die Existenz von Standards.

JETZT DIE MIGRATION ZU QUANTENSICHERER KRYPTOGRAFIE EINLEITEN!

Schon jetzt können Unternehmensverantwortliche Maßnahmen ergreifen, um die Zeit zu verkürzen, die sie für die Umstellung benötigen. Exemplarisch sei an dieser Stelle die Einführung und Pflege eines Krypto-Inventars genannt. Dabei handelt es sich um eine detaillierte Aufstellung, welche kryptografischen Verfahren in einer Organisation eingesetzt werden und wo diese Verwendung finden. Dieses Inventar erlaubt es, die Gefährdung im eigenen Risikomanagement zu berücksichtigen. Der BSI-Leitfaden „Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen“ nennt weitere Maßnahmen, um solche Bemühungen zu unterstützen. ■

Weitere Informationen:

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

https://www.bsi.bund.de/dok/umfrage-pqc

Im Blickpunkt

Digitaler Verbraucherschutz

Die Geburtsstunde des digitalen Verbraucherschutzes

Fabian Hodouschek, BSI-Fachbereichsleiter für Digitalen Verbraucherschutz, Cyber-Sicherheit für Gesellschaft und Bürger, über die Rolle des BSI und die Herausforderungen im digitalen Alltag der Menschen

Warum ist Digitaler Verbraucherschutz aus Ihrer Sicht ein wichtiges Thema im Aufgabenbereich des BSI?

Fabian Hodouschek: Das BSI als nationale Cyber-Sicherheitsbehörde des Bundes verfügt über eine außerordentlich hohe Kompetenz in allen Angelegenheiten der Informationssicherheit. Für die Verbraucherinnen und Verbraucher konnte dieser Sachverstand, zum Beispiel durch unsere Produkte „BSI für Bürger", nutzbar gemacht werden. Das war die Geburtsstunde des Digitalen Verbraucherschutzes im BSI, der jetzt mit der weiteren Entwicklung des BSI-Gesetzes endlich aus der Nische herausgeholt und als eigenständige Aufgabe wahrgenommen wurde. Hierfür bin ich dem Gesetzgeber sehr dankbar, denn es ermöglicht uns, im Sinne der Verbraucherinnen und Verbraucher für die Cyber-Sicherheit in der Digitalisierung zu wirken.

Da wir im BSI nur kurz den Flur hinuntergehen müssen, um die Fachexpertise für die aktuellen Herausforderungen der IT-Sicherheit zu finden, können wir als Verbraucherschutzbehörde in diesem speziellen Bereich sehr effektiv wirken.

In welchen Bereichen sehen Sie besonderen Informationsbedarf bei Verbraucherinnen und Verbrauchern, wo ein Schutzbedürfnis, das vielleicht nicht jedem Einzelnen bewusst ist?

Hodouschek: Neben vielen Annehmlichkeiten bringt die Digitalisierung des täglichen Lebens auch Gefahren mit sich. Ein Beispiel mit potenziell sehr großer Breitenwirkung ist das sogenannte Phishing, bei dem Betroffene mit gefälschten E-Mails und unter Vorspiegelung falscher Tatsachen dazu gebracht werden, sensible Daten wie Passwörter preiszugeben. Cyber-Kriminelle werden zunehmend skrupelloser und nutzen Ängste, Notlagen und aktuelle Ereignisse für Phishing-Attacken aus. Die Aufmachung von Phishing-Mails, das heißt die Ansprache und das Layout, wird auch aufgrund der zunehmenden Verwendung von Künstlicher Intelligenz immer professioneller. Gefälschte E-Mails erkennen zu können wird dadurch erheblich erschwert. Das BSI hat Phishing daher auch als Fokusthema für den aktuellen „Bericht zum Digitalen Verbraucherschutz 2022" ausgewählt .

Welche Ziele verfolgt das BSI mit seinen Aktivitäten beim Digitalen Verbraucherschutz?

Hodouschek: Als BSI sehen wir den Verbraucherschutz als Thema, welches sich nicht nur in Hinweisen und Empfehlungen an Verbrauche-rinnen und Verbraucher erschöpfen darf. Dies würde die Verantwortung für eine sichere Digitalisierung viel zu einseitig auf die Schultern der Menschen verlagern. Daher wollen wir die Rahmenbedingungen schaffen und formulieren, mit denen Anbieter und Hersteller sichere und vertrauenswürdige Produkte gestalten können – etwa indem Produkte von Anfang an mit IT-Sicherheit im Blick entwickelt werden und dann auch in einem sicheren Zustand zum Endverbraucher kommen. Daneben stellen wir die zwei weiteren Säulen unserer Arbeit: Information und Beratung von Verbraucherinnen und Verbrauchern sowie Unterstützung bei der Bewältigung von IT-Sicherheitsvorfällen.

Das BSI untersucht die Bedrohungslage und die Betroffenheit der Verbraucherinnen und Verbraucher systematisch durch Studien und Befragungen – wie etwa jährlich mit dem Digitalbarometer der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des BSI. Welche Themen adressiert das BSI aufgrund der Studienergebnisse nun verstärkt?

Hodouschek: Eine wesentliche Erkenntnis ist, dass die Bedeutung von Updates für die IT-Sicherheit den Befragten nicht immer bewusst zu sein scheint. Deshalb setzen wir in diesem Jahr in unserer Kommunikation einen Fokus auf Basisschutzmaßnahmen, wie beispielsweise den richtigen Umgang mit Updates oder auch Backups. Außerdem sehen wir in den Ergebnissen, dass nicht einmal die Hälfte der Befragten Passwörter nur für einen einzelnen Account nutzt. Die Mehrfach-

„Wir holen die Zielgruppe der Verbraucherinnen und Verbraucher in ihrem digitalen Alltag dort ab, wo sie unterwegs ist.“

verwendung von Passwörtern ist stark risikobehaftet. Denn erlangen Cyber-Kriminelle Zugang zu einem Account, ist es oft möglich, dass sie sich auch Zugang zu weiteren Accounts verschaffen. Dies kann erhebliche Schäden für die Betroffenen nach sich ziehen. Bei der Entwicklung unserer Maßnahmen werden wir auch vom Beirat „Digitaler Verbraucherschutz“ begleitet, der sich aus externen Expertinnen und Experten zusammensetzt.

Dieser hat in seinen 2022 veröffentlichten Handlungsempfehlungen zu „Kommunikation über Sicherheit bei Passwörtern“ u. a. darauf hingewiesen, dass das „erste Gebot“ die Einzigartigkeit von Passwörtern sein sollte. Und in einem Projekt wurde ein Passwort-Merkblatt zur besseren Handhabung vieler Passwörter entwickelt.

Für viele Menschen ist es eine Herausforderung im Bereich der IT und vor allem der sicheren Nutzung von IT, auf dem neuesten Stand zu bleiben. Wie holt das BSI diese ab?

Hodouschek: Wir holen die Zielgruppe der Verbraucherinnen und Verbraucher in ihrem digitalen Alltag dort ab, wo sie unterwegs ist. So hat etwa die bundesweite Kampagne „#einfachaBSIchern“, welche die Sicherheit beim Online-Shopping oder Smart Home aufgreift, eine große Breitenwirkung erzielt. Zudem kann das BSI auf schwerwiegende Sicherheitslücken mit Produktwarnungen reagieren und über die eigenen Social-Media-Kanäle regelmäßig aktuelle Tipps bzw. Hinweise teilen. Und das Interesse an Verbraucherthemen ist hoch, was die beständig wachsende Zahl Abonnierender des 14-tägig erscheinenden Newsletters „Sicher informiert“ und des monatlichen Podcasts „Update verfügbar“ zeigt. Daneben leistet das BSI auch einen Beitrag zur Transparenz von IT-Sicherheit in Produkten mit dem IT-Sicherheitskennzeichen. Verbraucherinnen und Verbraucher können anhand des IT-Sicherheitskennzeichens erkennen, ob ein Hersteller für sein Produkt bestimmte Anforderungen erfüllt hat – das Kennzeichen gibt es zum Beispiel bereits für Heimrouter oder smarte Geräte.

Aus Ihrer persönlichen Sicht als Verbraucher: Wo sehen Sie den größten Handlungsbedarf?

Hodouschek: IT-Sicherheit wird auch künftig ein Thema sein, welches sich schnell weiterentwickelt und für viele Menschen ein „Fachthema“ bleiben wird. Daher sollten die Produkte, die wir in der Digitalisierung nutzen, von vorneherein so sicher sein, dass Nutzenden nicht allein schon dadurch ein Schaden drohen kann, indem sie ein Produkt verwenden. Hersteller und Anbieter müssen daher frühzeitig ihren Pflichten nachkommen und die Produkte von vorneherein sicher machen. In einem zweiten Schritt müssen sie weiterhin mit den Nutzenden gemeinsam daran arbeiten, dass sie sicher bleiben, etwa durch Updates. Mit solchen Themen kann ich als Verbraucher nicht alleine gelassen werden. Aber für die Verbraucherinnen und Verbraucher muss es auch selbstverständlich werden, Sicherheitsmaßnahmen anzuwenden – ähnlich dem Sicherheitsgurt im Auto. Und als BSI werden wir weiterhin daran arbeiten, dass wir die Verbraucherinnen und Verbraucher dabei unterstützen. ■

Digitaler Verbraucherschutz als Gemeinschaftsaufgabe

Bericht zum Digitalen Verbraucherschutz 2022

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

Zum Weltverbrauchertag, der seit 1983 als Aktionstag von internationalen Verbraucherorganisationen jährlich am 15. März begangen wird, hat das BSI die dritte Ausgabe seines „Berichts zum Digitalen Verbraucherschutz" veröffentlicht. Der Bericht ist eine Jahrespublikation und vermittelt analytische Informationen sowie thematische Aufarbeitungen in einem komplexen Handlungsfeld.

Das Jahr 2022 war für die Verbraucherinnen und Verbraucher im Bereich der IT-Sicherheit von den Themen Phishing, Ransomware und Datenleaks geprägt. Hinzu kommen Sicherheitslücken bei digitalen Dienstanbietern, Schwachstellen in digitalen Verbraucherprodukten und Täuschungsversuche bei Onlinediensten. Die Schwerpunkte der Sicherheitsvorfälle im digitalen Verbrauchermarkt zeigen damit eine hohe direkte wie auch indirekte Betroffenheit der Verbrauchergruppen. Es wird deutlich, dass effektiver Digitaler Verbraucherschutz eine Herausforderung ist, die nur im Zusammenspiel vieler Akteure gelingen kann – gerade in Zeiten einer anhaltend angespannten Bedrohungslage im Cyber-Raum. Die Verankerung des Verbraucherschutzes sowohl in der Gesellschaft und bei Anbietern und Herstellern in der Wirtschaft als auch im staatlich-öffentlichen Bereich ist jedoch kein Sprint, sondern ein Marathon.

Doch der lange Atem lohnt sich. Verbraucherinnen und Verbraucher sind den Bedrohungen durch Cyber-Kriminelle nicht schutzlos ausgeliefert – auch das zeigt der aktuelle Bericht. Er bietet unter anderem einen Einblick in die kontinuierliche Arbeit des BSI und seiner Partner, um das Schutzniveau für die Verbraucherinnen und Verbraucher in Deutschland stetig zu verbessern. Dazu zählen Aktivitäten rund um das IT-Sicherheitskennzeichen, die Etablierung des Cyber-Sicherheitsnetzwerkes mit seiner digitalen Rettungskette, die organisatorische Neuausrichtung des Zentralen Service-Centers und vieles mehr.

FOKUSTHEMA: GEFAHRENQUELLE PHISHING

Phishing, eine Komposition aus „password" und „fishing", steht für den gezielten Diebstahl von Zugangsdaten zu Online-Nutzerkonten und ist über die Jahre zu einer konstanten Bedrohung avanciert. Hier setzt der aktuelle Bericht seinen thematischen Schwerpunkt, denn die Methoden und Maschen der Cyber-Kriminellen haben an Qualität wie auch Effektivität dazugewonnen. So hat sich Phishing auf nahezu alle Kommunikationskanäle, die Verbraucherinnen und Verbraucher nutzen, ausgeweitet: Neben Phishing via E-Mail wird beispielsweise Smishing als Angriff per SMS oder Messengernachricht oder auch Vishing per Anruf oder Audionachricht angewandt. Methodisch sind die Cyber-Kriminellen weit fortgeschritten: Phishing-Nachrichten sind mittlerweile so professionell gestaltet, dass sie sich kaum von seriösen Kommunikationsinhalten unterscheiden lassen.

Die Beispiele zeigen, dass sich die technologischen Möglichkeiten von Phishing stetig weiterentwickelt haben. Verknüpft mit psychologischen Komponenten wie der Hilfsbereitschaft, spielen sie mit dem Vertrauen oder der Angst potenzieller Opfer. Oft werden Themen ausgenutzt, die – wie im Berichtsjahr 2022 die Auswirkungen des russischen Angriffskriegs auf die Ukraine, der Inflation und drohender Energieknappheit – von großer gesellschaftlicher Bedeutung und somit Gegenstand einer breiten öffentlichen Debatte sind.

Liebe Kundin, lieber Kunde!

Um die Auswirkungen der gestiegenen Energiepreise für die Verbraucher abzumildern, wird im September ein Pauschalbetrag von 300 Euro an alle Erwerbstätigen ausbezahlt. Dies ist ein Beschluss der Bundesregierung und Inhalt des Entlastungspakets 2022, welches die durch den Ukraine-Krieg entstandene Energiekosten-Explosion etwas abfedern soll.

Wer erhält die Energiepauschale?

- **Steuerpflichtige** mit Einkünften aus Gewinneinkunftsarten (§ 13, § 15 oder § 18 des Einkommensteuergesetzes) und
- **Arbeitnehmerinnen und Arbeitnehmer**, die Arbeitslohn aus einem gegenwärtigen Dienstverhältnis beziehen und in die Steuerklassen I bis V eingereiht sind oder als **geringfügig Beschäftigte** pauschal besteuert werden.

Um Ihre Identät sowie den Anspruch auf eine Auszahlung feststellen zu können, benötigen wir eine Bestätigung Ihrer bereits angegeben Daten bei der Erstellung Ihres Girokontos in einer unserer Filialen.

Geben Sie noch heute Ihre aktuellen Daten auf unserer Homapege an und erhalten Sie innerhalb der nächsten vier Wochen Ihre Auszahlung der Energiepauschale. Dies können Sie ganz bequem von zu Hause aus erledigen, anbei finden Sie einen Direktlink zu den geforderten Angaben.

Vielen Dank für Ihre Zusammenarbeit!

Zur Homepage

Mit freundlichen Grüßen

Ihre Kundenberatung!

Beispiel einer Phishing-Nachricht – Auszahlung der Energiepreispauschale im Herbst 2022, aus der Cyber-Kriminelle auf vielfältige Weise versuchten, Profit zu schlagen. Die Mitteilung richtete sich an Kundinnen und Kunden der Sparkassen: an das Design der Sparkassenorganisation angelehnt, dazu sprachlich gut formuliert und mit Bezug auf eine Gesetzesgrundlage.

Phishing war, ist und bleibt zukünftig ein hochrelevantes Cyber-Sicherheitsthema – vor allem in Bereichen, wo monetäre Aspekte eine große Rolle spielen. So blickt der Bericht speziell auch auf den Bankensektor, in dem Cyber-Kriminelle besonders häufig das Vertrauen von Verbraucherinnen und Verbrauchern mit Hilfe von Phishing-Methoden ausnutzen (siehe Abbildung *Beispiel einer Phishing-Nachricht*). Daten aus dem Phishing-Radar der Verbraucherzentrale Nordrhein-Westfalen, die gemeinsam mit dem BSI analysiert wurden, sowie ein Gastbeitrag des Bundesverbands deutscher Banken e.V. zeigen die besonderen Herausforderungen sowie mögliche Präventionsansätze in diesem Gefahrenfeld auf.

GEMEINSAM MEHR ERREICHEN

Der „Marathonlauf" für nachhaltigen und zugleich effektiven Digitalen Verbraucherschutz kann nur als Gemeinschaftsaufgabe gelingen. Dies macht Dr. Gerhard Schabhüser, Vizepräsident des Bundesamts für Sicherheit in der Informationstechnik, in seinem Vorwort zum Bericht deutlich: „Wir möchten (...) auch alle Akteure im Digitalen Verbraucherschutz ermutigen, noch stärker in die Sensibilisierungs- und Aufklärungsarbeit der Verbraucherinnen und Verbraucher zu investieren. Als Cyber-Sicherheitsbehörde des Bundes leisten wir hierfür unseren Beitrag. Dies gilt für all unsere Anstrengungen, die neben den Verbrauchergruppen selbst zudem die Anbieter und Hersteller von vernetzten Produkten und digitalen Services, wie auch öffentliche und zivilgesellschaftliche Akteure beinhalten." ■

Weitere Informationen:

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/DVS-Bericht/dvs-bericht_node.html

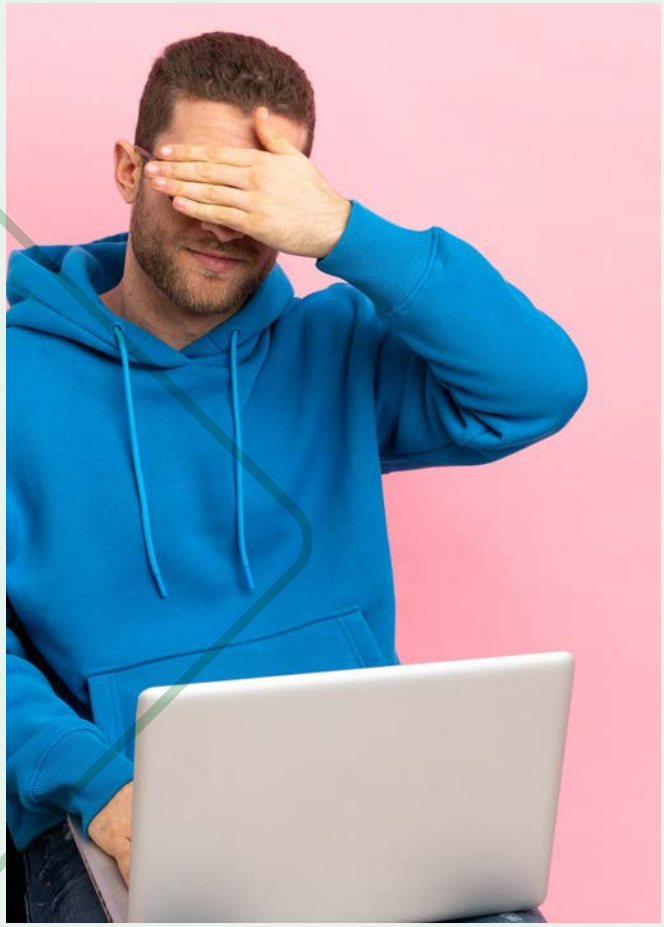
IT-Sicherheit auf dem digitalen Verbrauchermarkt

BSI-Studie zeigt Schwachstellen und Lösungsansätze bei Onlineshopping-Plattformen auf

von Jasmin Henn und Katarina Kühn, Referat Sichere Verbraucherprodukte und -dienste, Marktbeobachtung

Onlineshopping erfreut sich stetig zunehmender Beliebtheit. Es scheint bequemer, vom Sofa aus einzukaufen. Die Auswahl ist größer und die meist schnelle, kostenlose Lieferung überzeugt schließlich auch. Aber über das Onlineshopping werden die Menschen zu gläsernen Verbraucherinnen und Verbrauchern, die den Shops sensible Kontakt- und Zahlungsdaten übermitteln, von denen sie in der Regel nicht wissen, wie gut geschützt diese Daten bei den Anbietern sind.

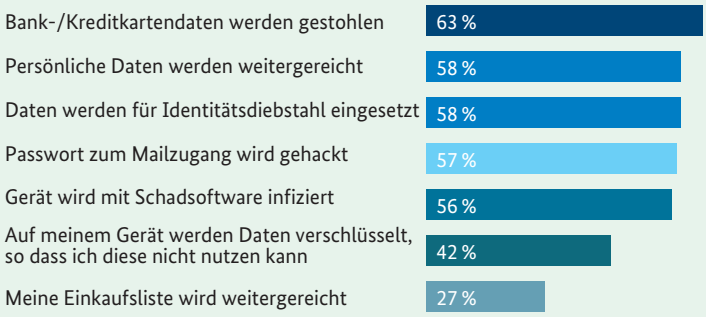
Für die Studienreihe „IT-Sicherheit auf dem digitalen Verbrauchermarkt" hat das BSI untersucht, wie sicher die Daten auf gängigen Onlineshopping-Plattformen sind, ob sich Verbraucherinnen und Verbraucher um die Sicherheit ihrer persönlichen Daten sorgen und wie sie auf sicherheitsrelevante Vorfälle reagieren. Erste Ergebnisse der Studie wurden schon im Artikel „Sicherheit statt Risiko" im BSI-Magazin 2022/02 ab S. 50 aufgegriffen.



ONLINESHOPPING IST BELIEBT, BEREITET ABER AUCH SORGEN

Mehr als neun von zehn Menschen (über 90 %) im Alter zwischen 16 und 74 Jahren in Deutschland, die über einen Internetzugang verfügen, kaufen gelegentlich in Onlineshops ein. Die Mehrheit von ihnen (55 %) macht das mindestens ein- oder mehrmals pro Monat. Dennoch haben zwei von drei Befragten (68 %) dabei Bedenken. Rund die Hälfte der Befragten (50 %) fürchtet sich vor Daten-Leaks, bei denen sensible Kundendaten auf den Plattformen der Anbieter gestohlen und für Identitätsdiebstähle eingesetzt werden können. Nahezu zwei Drittel (63 %) haben Sorge, dass ihre Bank- und Kreditkartendaten entwendet werden. Dies ist keine nur theoretische Sorge: Immerhin rund ein Viertel der Befragten (25 %) hatte bereits negative Erfahrungen mit der Datensicherheit beim Onlineshopping gemacht.

Wie gefährlich schätzen Sie diese Aspekte zu möglichen Gefahren in Zusammenhang mit der Nutzung des Internets ein? (n = 1.018)

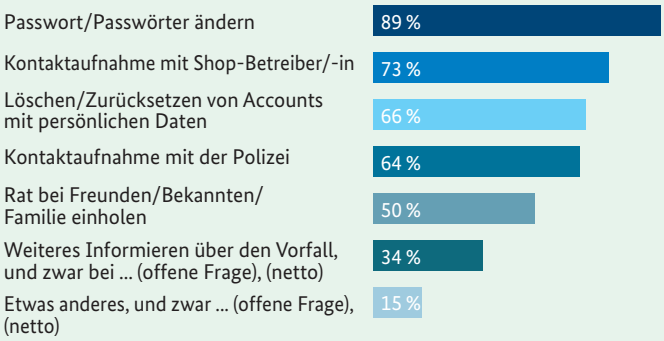


Weitere Informationen:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/onlineshopping-plattformen.html

Am häufigsten reagieren Verbraucherinnen und Verbraucher mit einer Änderung ihrer Passwörter (89 %), wenn es zu einem Datendiebstahl gekommen ist oder die betreffende Onlineshopping-Plattform vor einem Diebstahl warnt. Drei von vier Befragten (73 %) nehmen in einem solchen Fall Kontakt zum Shop-Betreibenden auf, zwei von drei (66 %) setzen ihre Konten zurück oder löschen ihre persönlichen Daten.

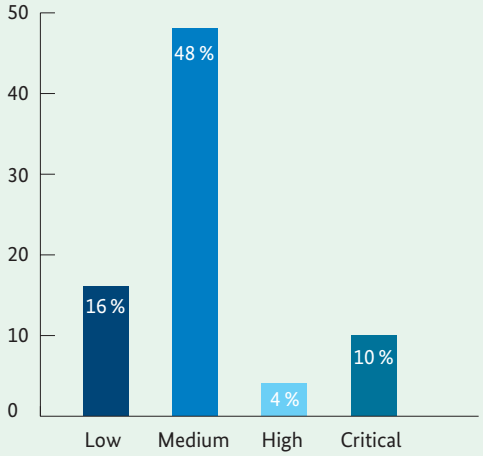
Welche Maßnahmen haben Sie bei Ihrer negativen Erfahrung in Bezug auf die Datensicherheit beim Onlineshopping ergriffen bzw. würden Sie ergreifen? (n = 1.018)



VERBRAUCHERINNEN UND VERBRAUCHER WÜNSCHEN SICH ORIENTIERUNG

Die Befragung macht auch deutlich, dass die Menschen unsicher sind, welche Auswirkungen das Entwenden oder das unrechtmäßige Einsehen von Daten für sie hat. Die große Mehrheit (81 %) geht „sehr wahrscheinlich“ von negativen Auswirkungen auf sie selbst aus, auch wenn rund die Hälfte nicht weiß, welche Auswirkungen das genau wären. Da ist es verständlich, dass sich bei Verbraucherinnen und Verbrauchern daraus ein starker Wunsch nach Orientierung ergibt. So wünschen sich beispielsweise 81 Prozent eine Bewertung der Sicherheit von Onlineshops durch ein Siegel von einer unabhängigen Stelle.

Aufteilung der Schwachstellen nach CVSS-Risikograden



SHOP-SOFTWAREPRODUKTE WEISEN OFT SCHWACHSTELLEN AUF

Die durchgeführte Schwachstellenanalyse von zehn zufällig ausgewählten Software-Produkten, mit denen Onlinehändler ihre Webshops erstellen, bestätigt imgrunde die Sorgen der Verbraucherinnen und Verbraucher: In jedem geprüften Produkt hat das BSI Sicherheitslücken mit teils gravierenden Auswirkungen auf das Sicherheitsniveau von Verbraucherdaten identifiziert. Von den insgesamt 78 gefundenen Schwachstellen wiesen die meisten einen mittleren Risikograd auf (siehe Abbildung). Die Analyse erfolgte auf Basis des „Web Security Testing Guide“ und des „Application Security Verification Standard“ des Open Web Application Security Project (OWASP).

Fast alle untersuchten Produkte (neun von zehn) bieten eine nur unzureichende Passwortrichtlinie. Eine solche erlaubt zum Beispiel einfache und unsichere Passwörter wie „passwort“ oder „12345678“.

In sieben von zehn Shop-Softwareprodukten hat das BSI JavaScript-Bibliotheken identifiziert, die verwundbar gegenüber bekannten Schwachstellen sind. Und in der Hälfte der untersuchten Produkte hat das BSI Software gefunden, die das offizielle End-of-Life-Datum bereits überschritten hat, also keine Sicherheitsupdates von dem Anbieter mehr erhält.

WIE DIE HERSTELLER REAGIEREN

Im anschließenden Coordinated-Vulnerability-Disclosure-Prozess (CVSS) hat das BSI den Anbietern die Ergebnisse der Schwachstellenanalysen eröffnet. In einigen Fällen stellten die Hersteller zeitnah Patches zur Verfügung. Andere informierten das BSI darüber, wie sich einzelne Schwachstellen durch eine sichere Konfiguration des Onlineshops abschwächen lassen. Es wäre sinnvoll, wenn sie diese Informationen auch den Betreiberinnen und Betreibern von Onlineshops zur Verfügung stellen würden, so dass sie selbst ihre Shops absichern können. ■

Digitaler Verbraucherschutz braucht tragfähige Bündnisse und neue Perspektiven

Wissenschaftliche Tagung „Digitaler Alltag in Gefahr?“ gibt neue Antworten

von Dr. Jörg Hübner, Dr. Matthias Korn, Doris Rehn und Dr. Katharina Witterhold, Referat Grundsatzfragen des Digitalen Verbraucherschutzes und Kooperationen

Moderierte das Panel zum Thema „Verbraucherinnen und Verbraucher verstehen – Einbettung von IT-Sicherheit in die digitale Haushaltsökonomie“: Prof. Dr. Martina Angela Sasse von der Ruhr-Universität Bochum und Sprecherin des Beirates Digitaler Verbraucherschutz

Angeregte Diskussionen rund um die aktuellen Herausforderungen des Digitalen Verbraucherschutzes

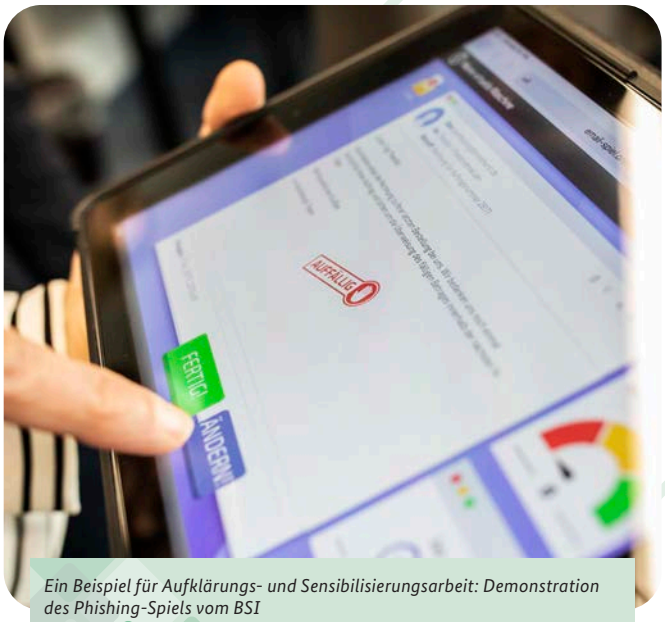
Smartphone und Tablets, Onlineshopping und -banking, Smart Home, E-Auto: Der Alltag der Menschen ist längst digital. Aber ist er auch sicher, wenn Hacker, Hektik und herstellerseitige Sicherheitsmängel uns stressen? Eine wissenschaftliche Tagung sucht nach Antworten.

Im Februar 2023 fand in Sankt Augustin erstmals die wissenschaftliche Tagung „Digitaler Alltag in Gefahr?“ statt. Im Fokus der Veranstaltung auf dem Campus der Hochschule Bonn-Rhein-Sieg, an der Wissenschaftlerinnen und Wissenschaftler aus der IT-Sicherheits- und Verbraucherforschung, institutionelle Akteure sowie Expertinnen und Experten des Digitalen Verbraucherschutzes teilnahmen, stand die verbraucherbezogene IT-Sicherheitsforschung. Ausgehend vom aktuellen Stand der Forschung an der Schnittstelle von IT-Sicherheit und Konsum diskutierten die 65 Teilnehmenden gemeinsame Forschungsanliegen sowie Anknüpfungspunkte für eine inter- und transdisziplinäre Zusammenarbeit.

HOHE DYNAMIK, KURZE LEBENSZYKLEN

Der digitale Verbrauchermarkt zeichnet sich durch eine hohe Dynamik mit immer kürzeren Produktlebenszyklen aus – und das bei einer enormen Anwendungsvielfalt. In der Fachwelt, die sich wissenschaftlich mit Fragen des Digitalen Verbraucherschutzes beschäftigt, steht aufgrund dieser Kurzlebigkeit unter anderem die Effizienz von Schutzmaßnahmen im Vordergrund. Da geht es dann beispielsweise um die Klärung von Fragen wie: Welches Verständnis von IT-Sicherheit haben Verbraucherinnen und Verbraucher? Welche gesellschaftlichen, rechtlichen und technischen Rahmenbedingungen müssen berücksichtigt werden, um die Menschen besser zu schützen oder zu unterstützen?

Fachliche Impulse aus Sicht der Verbraucherwissenschaften lieferte u. a. Prof. Dr. Peter Kenning von der Heinrich-Heine-Universität Düsseldorf



Ein Beispiel für Aufklärungs- und Sensibilisierungsarbeit: Demonstration des Phishing-Spiels vom BSI

Zwei Begriffe fielen in der Fachdiskussion immer wieder: Transparenz und Verantwortung. So ist für die Verbraucherinnen und Verbraucher beispielsweise meist nicht ersichtlich, wie sie ihr Recht im Fall eines Schadens bei der Nutzung onlinefähiger Produkte und Anwendungen durchsetzen. Oft ist es für sie auch unmöglich, potenzielle Gefährdungen ihrer Daten im digitalen Alltag zu erkennen. Allein diese fehlende Transparenz zeigt mit Blick auf die Frage der Verantwortung auf, dass die oft praktizierte Trennung von Zuständigkeiten der Institutionen im Sinne einer Arbeitsteilung zwar vorteilhaft sein mag, im Verbraucheralltag aber die Unterscheidung zwischen IT-Sicherheit, Datensicherheit und Datenschutz nicht unbedingt nachvollziehbar ist.

Gefragt sind daher Ansätze, die den multidimensionalen Anforderungen des Digitalen Verbraucherschutzes gerecht werden. Fachlich eingeschränkte Sichtweisen, die einseitig bei den Faktoren „Technik", „Recht" und „Mensch" ansetzen, genügen dabei kaum. Wie unzureichend diese Sichtweisen sind, zeigt sich besonders deutlich am Begriff der „digitalen Vulnerabilitäten". Verletzlichkeit im digitalen Raum ist nicht mehr nur an Merkmale und Eigenschaften der Verbrauchergruppen selbst geknüpft. Sie entsteht bereits bei der Entwicklung von Soft- und Hardware. Dort öffnen sich erste und schwere Sicherheitslücken, die erst durch Nachlässigkeiten in der Nutzung der Produkte valide oder offenkundig werden.

NEUE PERSPEKTIVEN UND BÜNDNISSE SIND NÖTIG

Gefordert sind daher neue, im digitalen Alltag der Verbraucherinnen und Verbraucher unterstützende und zugleich nachhaltige Designprinzipien, die die Perspektive der Anwenderinnen und Anwender berücksichtigen und mit einer angemessenen Regulatorik durchgesetzt werden können.

Ein effektiver Digitaler Verbraucherschutz fordert auch zu neuen Arbeitsbündnissen auf – im Verbraucherschutz selbst, aber auch mit der IT-Sicherheits- sowie Verbraucherforschung. Die Tagung war dazu ein gelungener Auftakt, nicht nur um den wissenschaftlichen Diskurs zu führen, sondern auch um die Praxisseite intensiver einzubeziehen.

Die Tagung „Digitaler Alltag in Gefahr?" wurde auf Initiative des Beirats Digitaler Verbraucherschutz beim Bundesamt für Sicherheit in der Informationstechnik (BSI) organisiert, vom Institut für Verbraucherinformatik der Hochschule Bonn-Rhein-Sieg, dem Kompetenzzentrum Verbraucherforschung Nordrhein-Westfalen, der Verbraucherzentrale NRW e.V. und dem BSI veranstaltet sowie vom Projekt „Mittelstand 4.0 – Kompetenzzentrum Usability" unterstützt. Der Beirat Digitaler Verbraucherschutz ist ein unabhängiges Gremium und unterstützt das BSI dabei, die Cyber-Sicherheit im digitalen Alltag von Verbraucherinnen und Verbrauchern zielgruppenorientiert und praxistauglich durch geeignete Maßnahmen zu erhöhen. ■

Weitere Informationen:

https://www.bsi.bund.de/dok/beirat-dvs

https://www.bsi.bund.de/dok/1078292

Mehr IT-Basisschutz braucht das Land!

Bei Videos, Social Media & Podcast ist für alle etwas dabei

von Jan Lammertz, Referat Cyber-Sicherheit für Gesellschaft und Bürger

Das Fundament für mehr IT-Sicherheit in der Bevölkerung ist die Vermittlung eines verständlichen Basisschutzes. Und wie es häufig so ist: Jeder Mensch lernt anders. Daher liegt ein Schwerpunkt im Referat Cyber-Sicherheit für Gesellschaft und Bürger auf der multimedialen Ausgestaltung von IT-Sicherheitstipps für den digitalen Alltag.

Laut Digitalbarometer 2022 (einer repräsentativen Bürgerbefragung zur Cyber-Sicherheit) waren rund 29 Prozent der Befragten wissentlich Opfer von Cyber-Kriminalität. Außerdem weiß knapp die Hälfte der Befragten (45 %) um die gängigen Sicherheitsempfehlungen, aber nur 22 Prozent setzen sie vollständig um. Einer der Hauptgründe: ein teils sorgloser Umgang mit Onlinediensten. Ferner haben Verbraucherinnen und Verbraucher qua Alter einen unterschiedlichen Zugang zu Informationen gelernt. Hinzu kommen persönliche Vorlieben im Medienkonsum.

PODCAST „UPDATE VERFÜGBAR“ – DIALOG MIT EXPERTINNEN UND EXPERTEN

Bereits seit September 2020 bekommen Verbraucherinnen und Verbraucher im BSI-Podcast „Update verfügbar“ Cyber-Sicherheitsthemen auf die Ohren. Das Moderatorenteam bespricht gemeinsam oder zusammen mit Externen sowie mit Expertinnen und Experten inner- und außerhalb des BSI aktuelle Geschehnisse rund um Digitalisierung, Netzwelt und Internetkriminalität, z. B.: Woran erkennt man Deepfakes? (mit BSI-Experte Markus Ullmann), Sicherheit beim Gaming (mit Felix Rick von Gameswelt), Fake-Shops und Betrug beim Onlineshopping (mit Hauke Mormann von der Verbraucherzentrale NRW) oder Risiken und Potenziale beim Smart Home (mit TikTok-Influencer Tobias Tullius). Diese Beispiele zeigen die bunte Themenvielfalt des Podcast-Angebots.

Um sich neuen Themen zu nähern, hat es sich bewährt, die Community regelmäßig einzubinden. Mittlerweile gehört „Update verfügbar“ zur Gruppe der Top-zehn-Prozent der Podcasts in Deutschland*. Zu hören ist der Podcast in der BSI-Mediathek, auf dem BSI-YouTube-Kanal, bei Spotify, Deezer und iTunes, Google Podcast und im Feed.

VIDEOS – DAS WICHTIGSTE KURZ UND KNAPP

Video ist nicht gleich Video. Dennoch sollte es eine Gemeinsamkeit geben: Unterhaltung und Information gehen Hand in Hand. So sind im Laufe der letzten Jahre Videos unterschiedlicher Länge und Detailtiefe entstanden, die für verschiedene Kanäle – wie Instagram, YouTube, Facebook oder die Website – konzipiert wurden. Mal sind es animierte Erklärvideos zu Themen wie Ransomware oder Kryptowährungen und

* Zahl bezieht sich auf die monatlichen Gesamtstreams der Podcast-Folgen.

NFT, mal Videoreihen wie Cyber-Sicherheit[2] (Interviews mit Expertinnen und Experten) zur Sicherheit bei Messengern oder Apps. Ein gemeinsamer Adventskalender mit dem YouTuber „Mr. Wissen2Go“ sowie eine Zusammenarbeit mit der „Gameswelt“ anlässlich der Gamescom sind ebenso dabei wie ein interaktives Videoformat, in dem sich der Ausgang der Videos von den Zusehenden beeinflussen lässt. Seit Kurzem treten Beschäftigte aus dem BSI-Referat Cyber-Sicherheit für Gesellschaft und Bürger auch selbst für Instagram-Videos vor die Kamera, um besonders dieser Community immer wieder kurzweilige IT-Tipps zu präsentieren. Das Motto lautet dabei: Die Videos sollen einen alltagsnahen Zugang zu Themen der IT- und Cyber-Sicherheit schaffen.

LAST, BUT NOT LEAST: TEXTARBEIT

Am Anfang steht das Wort. Und das gibt es beim BSI nicht nur auf der Website oder im Newsletter, sondern auch in Form von Printprodukten wie Informationsbroschüren („Wegweiser für den digitalen Alltag“), Flyern und Checklisten. Insbesondere wenn die Technik einmal streikt, kann ein analoges Nachschlagewerk in kompakter Form hilfreich sein.

Grundsätzliche Informationen zur Funktionsweise eines Gerätes oder Dienstes sind dabei die Basis und leiten hin zu einer Schritt-für-Schritt-Anleitung, die den konkreten Anwendungsfall erläutern soll.

Sowohl der „Wegweiser für den digitalen Alltag“ als auch die übersichtlichen Checklisten zu Themen wie Onlinebanking, Phishing, Schadsoftware oder Smartphone-Sicherheit und die SOS-Karte sind auf diese Weise für den Notfall im digitalen Alltag von Verbraucherinnen und Verbrauchern bestens geeignet. ■

Weitere Informationen:

Verbraucherbereich auf der Website:
https://www.bsi.bund.de/VerbraucherInnen

BSI bei Instagram:
https://www.instagram.com/bsi_bund/

BSI bei YouTube:
https://www.youtube.com/@bsi_bund

Ein Jahr IT-Sicherheitskennzeichen, ein Jahr Transparenz

Rückblick und Perspektiven

von Paul Trinks, Referat Erteilung von IT-Sicherheitskennzeichen

Im Februar 2022 hat das BSI im Rahmen des 18. Deutschen IT-Sicherheitskongresses das erste IT-Sicherheitskennzeichen vergeben und damit einen zentralen Auftrag aus dem IT-Sicherheitsgesetz 2.0 vom Mai 2021 umgesetzt. Das Verbraucherkennzeichen ermöglicht es Herstellern und Diensteanbietern, die Sicherheitseigenschaften ihrer Produkte gegenüber ihren Kundinnen und Kunden transparent zu machen. Gleichzeitig können Verbraucherinnen und Verbraucher erstmals Aspekte der IT-Sicherheit schnell und einfach erfassen und in ihre Kaufentscheidung einbeziehen.
Das bisher für 37 Produkte vergebene IT-Sicherheitskennzeichen unterscheidet sich grundlegend von anderen Produktkennzeichen, weil es neben dem statischen Etikett auch einen dynamischen Bestandteil umfasst: Das statische Element bildet die Herstellererklärung ab und führt per Link und QR-Code zum dynamischen Teil des Kennzeichens, der aus einer aktuellen BSI-Verbraucherinformation zum gekennzeichneten Produkt besteht.

Während klassische Kennzeichnungssysteme nur eine Momentaufnahme widerspiegeln, kommt das IT-Sicherheitskennzeichen dem Ziel des Gesetzgebers nach, die sich ständig verändernde IT-Sicherheitslage im Verbraucherbereich nachhaltig abzubilden. Der integrierte Link mit QR-Code erweitert dafür die Aussagekraft des Labels um eine verlinkte Informationsseite. Neben den erklärten Sicherheitseigenschaften können dort bspw. dem BSI bekanntgewordene Schwachstellen und damit zusammenhängende Sicherheitsupdates abgerufen werden.

Die anlasslose und anlassbezogene Prüfung der gekennzeichneten Produkte im Rahmen der BSI-Marktaufsicht fördert die Glaubwürdigkeit und das Vertrauen in das Kennzeichen. So wird eine umfassende und am Interesse des einzelnen Konsumenten ausgerichtete Transparenz erreicht, die einen tatsächlichen Mehrwert gegenüber rein statischen Produktkennzeichen bietet.

ANBIETER VERTRAUEN DEM IT-SICHERHEITSKENNZEICHEN

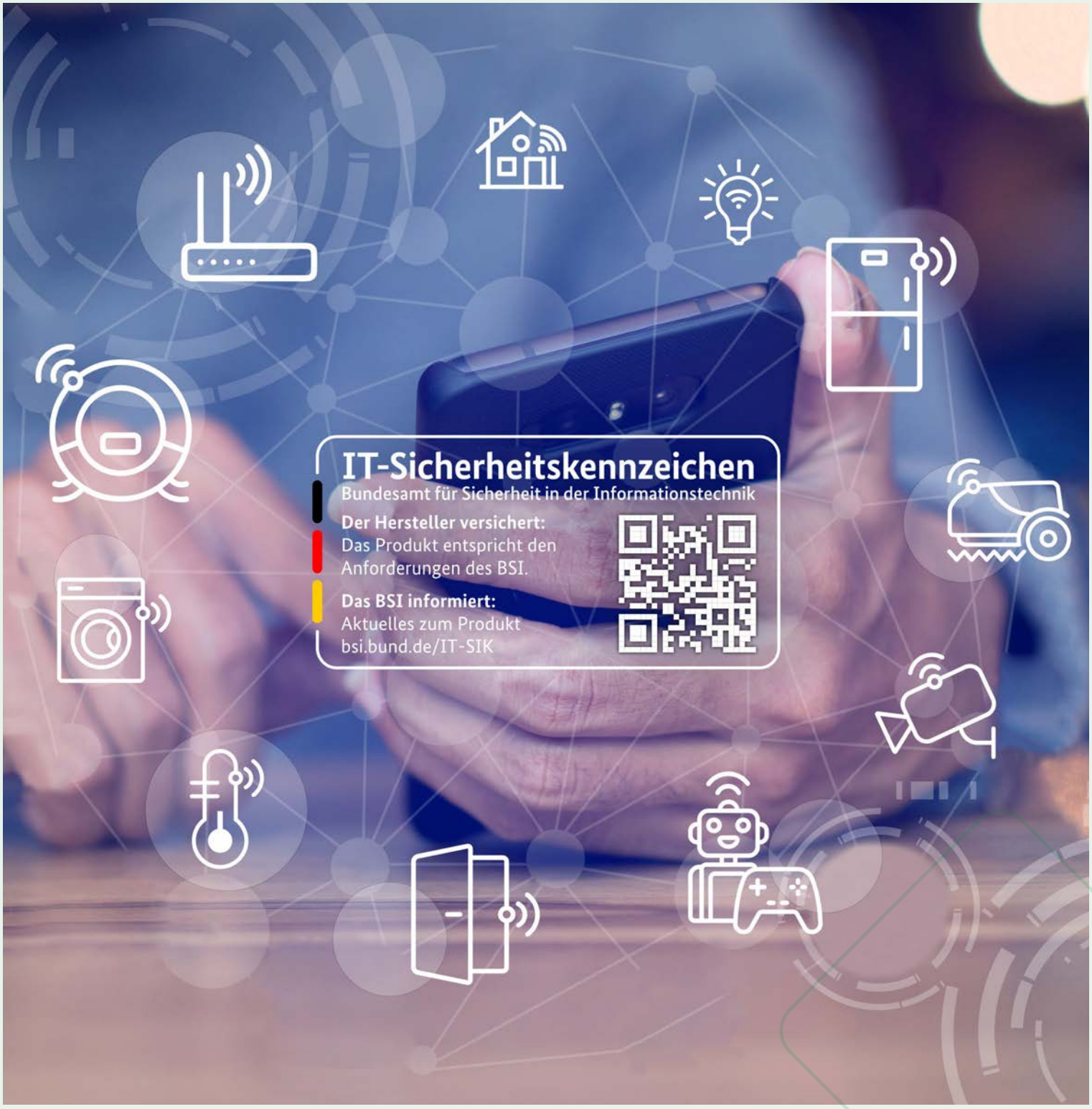
Diese Einschätzung teilt Fabian Bock, Geschäftsführer der mail.de GmbH. Seine Firma hatte im Februar 2022 das erste Kennzeichen überhaupt für ihren E-Mail-Dienst erhalten:

„Das IT-Sicherheitskennzeichen ermöglicht es Herstellern und Diensteanbietern, durch ihr Versprechen in die Sicherheit ihrer IT-Produkte am Markt hervorzustechen. Viel wichtiger aber: Es gibt Verbraucherinnen und Verbrauchern Orientierung beim Thema IT-Sicherheit. Wir haben diese Chance als erster E-Mail-Anbieter in Deutschland erkannt und unsere E-Mail-Produkte mit dem IT-Sicherheitskennzeichen ausgezeichnet. Darauf haben wir viel Resonanz unserer Kundinnen und Kunden erhalten, die sich nach unserer Wahrnehmung auch positiv auf die Nutzungsentscheidung auswirkt.

Seitdem wir das IT-Sicherheitskennzeichen haben, sind viele Marktbegleiter unserem Vorbild gefolgt. Wir begrüßen diese Entwicklung, denn sie zeigt die Akzeptanz des Kennzeichens am Markt und das Bestreben der Anbieter, ihre Dienste sicher zu gestalten. E-Mail-Anbieter, die sich dabei an die Sicherheitsanforderungen des BSI halten, leisten einen wesentlichen Beitrag für die sichere Nutzung des Internets insgesamt. Mit Blick auf den Verbrauchermarkt werden wir deshalb auch in Zukunft nicht zögern, weitere Produkte unseres Hauses mit dem IT-Sicherheitskennzeichen auszuzeichnen.“

BSI ERWEITERT ANWENDUNGSBEREICH DES KENNZEICHENS

Nach der erfolgreichen Einführung arbeitet das BSI daran, das IT-Sicherheitskennzeichen fortzuentwickeln und als zentrales Element des digitalen Verbraucherschutzes zu etablieren. Zu diesem Zweck wird der Anwendungsbereich des Produktkennzeichens fortlaufend erweitert – zuletzt durch die Einführung einer neuen Produktkategorie für smarte Verbrauchergeräte. Diese ermöglicht es Herstellern von IoT- und Smart Home-Produkten seit Kurzem, das IT-Sicherheitskennzeichen für eine Vielzahl vernetzter Verbraucherprodukte zu beantragen. Der neuen Produktkategorie liegt der IoT-Basisstandard ETSI EN 303 645 zugrunde, der im Rahmen der internationalen Standardisierungsarbeit durch Expertinnen und Experten des BSI



mitentwickelt wurde. Die Wahl eines europäischen Standards fördert den Gleichlauf von grenzübergreifenden Cyber-Sicherheitsanforderungen und schafft die Basis für Anerkennungsabkommen mit vergleichbaren Kennzeichnungssystemen.

BLAUPAUSE FÜR DIE GESTALTUNG EUROPÄISCHER UND INTERNATIONALER KENNZEICHEN

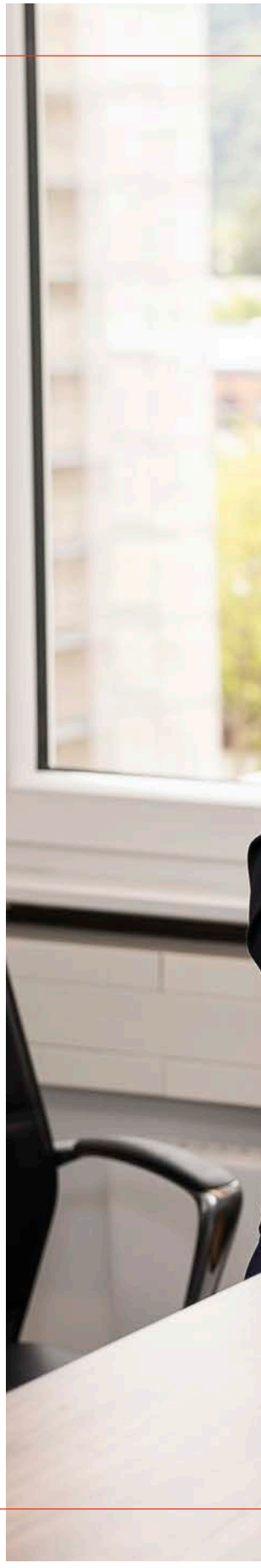
Vor diesem Hintergrund hat das BSI im Oktober 2022 eine bilaterale Vereinbarung mit der Cyber Security Agency Singapore (CSA) zur gegenseitigen Anerkennung des dortigen Cybersecurity Labelling Scheme (CLS) und des deutschen IT-Sicherheitskennzeichens abgeschlossen. Damit wird es Herstellern mit dem IT-Sicherheitskennzeichen ermöglicht, in Singapur ein Cybersecurity Label der Stufe 2 zu erhalten. Mit der gegenseitigen Anerkennung nimmt das BSI seine Rolle als Wegbereiter und Gestalter der sicheren Digitalisierung nicht nur in Deutschland, sondern auch auf internationaler Ebene wahr und platziert das IT-Sicherheitskennzeichen als Vorbild im europäischen und internationalen Kontext. ■

Weitere Informationen:

www.bsi.bund.de/it-sik

Drei Fragen an … Claudia Plattner

**Claudia Plattner ist seit Juli 2023 Präsidentin des BSI.
Zu ihrem Amtsantritt hat sie dem BSI-Magazin ein erstes Interview gegeben.**



Frau Plattner, Sie arbeiten seit mehr als zwei Jahrzehnten in der IT-Branche. Wurden Sie schon einmal gehackt?

Claudia Plattner: Privat noch nicht – ich hoffe das bleibt auch so. Beruflich natürlich schon millionenfach, aber zum Glück nur sehr selten erfolgreich. Ich erinnere mich z. B. aber noch sehr gut an die weltweite Ransomware-Welle des Schadprogramms WannaCry. Damals war ich bei der Bahn und wir waren auch betroffen, z. B. bei den Anzeigetafeln in den Bahnhöfen. Innerhalb von wenigen Tagen war das durchgestanden, aber an dem Beispiel sieht man, wie enorm wichtig Resilienz und gute Prävention sind. Denn ganz klar: Eine 100-prozentige Sicherheit vor Angriffen gibt es nicht! Deshalb ist es entscheidend zu wissen, wie man mit Angriffen umgeht, ohne gleich umzufallen. Und da kann man eine Menge machen, um schnell wieder auf die Beine zu kommen.

Welche Bedeutung hatte IT-Sicherheit zuletzt in Ihrer Arbeit bei der EZB?

Claudia Plattner: Kurz gesagt: Eine sehr, sehr große! Sie stand jeden Tag auf der Agenda, denn in meiner Rolle bei der EZB war ich unter anderem auch für das Thema Cybersicherheit verantwortlich. Das fängt bei den Sicherheitsvorgaben an, dann braucht es Lösungen, um Sicherheit auch in Entwicklung und Betrieb zu gewährleisten. Natürlich muss man auch für den Ernstfall üben und außerdem gilt es, eine moderne, leistungsfähige IT mit der dazugehörigen Sicherheit zu bauen. All das und noch vieles mehr gehörte zu meinem täglich Brot: Ob in der Zusammenarbeit mit den Fachabteilungen oder mit den Länder-Zentralbanken – das Thema IT-Sicherheit hatte immer einen hohen Stellenwert in meinem Arbeitsalltag. Und ganz ehrlich: Das ist auch gut so, denn deshalb nehme ich sie auch so ernst. Das ist generell mein Appell in Sachen Cybersicherheit, der für Politik, Wirtschaft und Gesellschaft gleichermaßen gilt: Nehmt Cybersicherheit ernst!

Welche besonderen Herausforderungen sehen Sie aktuell mit Blick auf die sichere Digitalisierung in Deutschland?

Claudia Plattner: Es ist meine Überzeugung, dass die Digitalisierung nur gelingt, wenn sie sicher ist. Aber Cybersicherheit ist komplex. Daher arbeiten alle Kolleginnen und Kollegen beim BSI gemeinsam daran, aus komplex einfach zu machen: Sei es beispielsweise durch die Entwicklung einheitlicher Sicherheitsstandards für Unternehmen oder die Zertifizierung von IT-Produkten, die Verbraucherinnen und Verbrauchern helfen, ihren digitalen Alltag sicher zu bewältigen. Ich werde mein Bestes geben, damit meine Kolleginnen und Kollegen ihren Job gut machen können. Denn darin sehe ich unsere gemeinsame Aufgabe als BSI: Mit Tatkraft, Wissen und Zuversicht die Digitalisierung aktiv gestalten. ■


„Darin sehe ich unsere gemeinsame Aufgabe als BSI: Mit Tatkraft, Wissen und Zuversicht die Digitalisierung aktiv gestalten.“

BSI setzt Standards für die Cyber-Sicherheit von Bundesbehörden

Sicherheitsvorgaben, Kontrollen und Informationshandeln: Überblick über die Befugnisse des Bundesamtes (Teil 1 von 2)

von Marc Brauer, Martin Kurtz und Rhian Moritz, Referat IT-Sicherheit und Recht

> *„Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft“.*

Passend zu diesem selbstgewählten Leitsatz ist das BSI vom Gesetzgeber mit einer Vielzahl von Aufgaben und Befugnissen ausgestattet, die im BSI-Gesetz (BSIG) genauer definiert sind.

Die Befugnisse des BSI für Tätigkeiten innerhalb der Bundesverwaltung lassen sich grob in drei Kategorien aufteilen:

- Das BSI handelt durch den Erlass von Regeln,
- sammelt und verteilt als Zentrale Meldestelle Informationen
- und ist selbst operativ tätig.

Für jede dieser Aktivitäten ist das BSI mit Befugnissen ausgestattet.

SICHERHEITSVORGABEN UND -ÜBERPRÜFUNGEN

Der § 8 des BSIG legitimiert das BSI, Mindeststandards für die Informationstechnik des Bundes in Form verbindlicher Mindestanforderungen festzulegen. Diese Standards dürfen nur in besonderen Ausnahmefällen unterschritten werden und sind wichtige Werkzeuge für die Prävention von Störungen und Vorfällen, die fortlaufend weiterentwickelt werden.
So definiert das BSI beispielsweise Mindeststandards zur Nutzung von Public-Cloud-Diensten oder für die Verwendung der Transport Layer Security (TLS), mit der eine sichere Übertragung von Daten über öffentlich zugängliche Netze gewährleistet werden kann.

Diese öffentlich verfügbaren Mindeststandards sind unentgeltlich zur Verwendung in kommerziellen Produkten, zum Beispiel in Informationssicherheitsmanagement-System-Tools, freigegeben und können von der Website des BSI heruntergeladen werden.

Grundsätzlich sind alle Stellen des Bundes verpflichtet, sich an diese Standards zu halten, auch zum Beispiel das Informationstechnikzentrum Bund (ITZ Bund) als bundesunmittelbare, nichtrechtsfähige Anstalt des öffentlichen Rechts.

Das BSI überprüft im Rahmen von § 4a BSIG, ob Bundesbehörden notwendige Sicherheitsvorgaben einhalten, darunter auch die Mindeststandards. Der Paragraph umfasst auch ein Kontrollrecht des Amtes für die Sicherheit der IT des Bundes. Dieses Recht gilt unter anderem auch für Rechenzentren, die zuvor nur auf Grundlage einer Entscheidung des Haushaltsausschusses geprüft wurden.

Für die Prüfungen (inklusive IS-Kurzrevision, NdB-Nutzerpflichtenrevision und Rechenzentren-Sicherheitsanalyse) sind die Betreiber verpflichtet, alle erforderlichen Informationen zur Verfügung zu stellen und Zugang zu ihren Räumlichkeiten zu gewähren. Aus seinen Erkenntnissen formuliert das BSI als Prüfbehörde einen Bericht über die

Überblick über die Befugnisse des BSI gegenüber der Bundesverwaltung

- Sicherheitsvorgaben und -überprüfungen
  - Mindeststandards
  - Freigaben und Zulassungen nach Verschlusssachenanweisung
  - Informationshandeln im Rahmen der Zentralen Meldestelle
- Operative Befugnisse (BSI-Magazin 2023/02)
  - Schadsoftware-Erkennungs-System u. a.
  - Scanbefugnis
  - Mobile Incident Response Teams (MIRTs)

Ergebnisse, der auch Verbesserungsvorschläge zur Mängelbeseitigung enthält.

Mit diesen Aktivitäten wird das BSI seinem Beratungs- und Präventionsauftrag gerecht. Die Verantwortung zur Mängelbeseitigung liegt bei den geprüften Einrichtungen. Eine weitere Einflussnahme durch das BSI auf die Umsetzung etwa der Verbesserungsvorschläge besteht dabei aber grundsätzlich nicht.

Im Freigabeprozess und über Zulassungen nach der Verschlusssachenanweisung (VSA) des Bundes macht das BSI auch Vorgaben im Bereich des Geheimschutzes. Im Gegensatz zur Freigabe (§ 50 VSA) geht es bei Zulassungen (§ 51 VSA) nicht um ein konkretes System, sondern um Produkte, die innerhalb solcher Systeme IT-Sicherheitsfunktionen (§ 52 VSA) übernehmen.

INFORMATIONSHANDELN

Auch das Sammeln und Auswerten von Informationen über Sicherheitsrisiken und -vorkehrungen gehört zu den gesetzlichen Aufgaben des BSI. Mit der in § 4 BSIG definierten Rolle als Zentraler Meldestelle und dem Unterhalt des Nationalen IT-Lagezentrums ist das BSI als „Single Point of Contact (SPOC)“ die Stelle, an der alle Informationen zu Cyber-Sicherheitsvorfällen in Deutschland zusammengeführt werden. Neben den Fachreferaten innerhalb des BSI können über das Nationale Cyber-Abwehrzentrum angeschlossene Partnerbehörden zur Bewertung oder zur Bearbeitung von Informationen hinzugezogen werden. Bundesbehörden sind laut § 4 Abs. 3 BSIG dazu verpflichtet, dem BSI alle Informationen, insbesondere zu Sicherheitslücken, Schadprogrammen sowie erfolgten oder versuchten Angriffen, zu übermitteln.

Spiegelbildlich dazu muss das BSI nach § 4 Abs. 2 Nr. 2 BSIG alle Bundesbehörden über sie betreffende Informationen in Kenntnis setzen. Dazu gehören auch Informationen, die über die Allgemeine Meldestelle beim BSI eingehen. ■

Weitere Informationen:

https://www.bsi.bund.de/dok/MST

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Geheimschutz/Geheimschutzberatung/VorschriftenStandards/vorschriftenstandards_node.html

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/nationales-it-lagezentrum_node.html

Zusammenarbeit auf Augenhöhe bringt Vorteile für beide Seiten

Kooperationsvereinbarungen zwischen BSI und Ländern verbessern die Cyber-Sicherheit

von Philipp Gebhard, Referat Nationales Verbindungswesen

Mit der zunehmenden Digitalisierung von Bund, Ländern und Kommunen geht auch eine Erhöhung der Angriffsfläche einher. Gemäß dem Schwächste-Glied-Prinzip, nach dem eine Kette immer nur so stark wie das schwächste Glied ist, besteht deshalb im Bereich der Cyber-Sicherheit – angesichts einer zunehmenden Verflechtung der IT des Bundes und der Länder – die Notwendigkeit der ebenenübergreifenden und kooperativen Zusammenarbeit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stärkt das gesamtstaatliche Cyber-Sicherheitsniveau daher mit bilateralen Kooperationsvereinbarungen.

Die Bund-Länder-Zusammenarbeit im Bereich der Cyber-Sicherheit ist ein fortlaufender Prozess, der mit zunächst unverbindlichen Absichtserklärungen zwischen dem BSI und interessierten Ländern begann, aber schon bald einen Bedarf an verbindlicheren Zusammenarbeitsformen zeigte. In Abstimmung mit dem Bundesinnenministerium des Innern und für Heimat (BMI) hat das BSI daher die Möglichkeit einer Kooperationsvereinbarung entwickelt, die gegenseitige Unterstützung auf Augenhöhe ermöglichen soll.

Mit der Vereinbarung beschließen die Partner in einem gemeinsamen Arbeitsprogramm für eine bestimmte Dauer verbindliche Kooperationsfelder, die sodann sukzessive umgesetzt werden. Die Ziele und Maßnahmen der Kooperationsvereinbarung werden während des gesamten Zeitraums fortlaufend evaluiert und aktualisiert, so dass neue Bedarfe aufgenommen werden können.

WELCHE KOOPERATIONSFELDER GIBT ES?

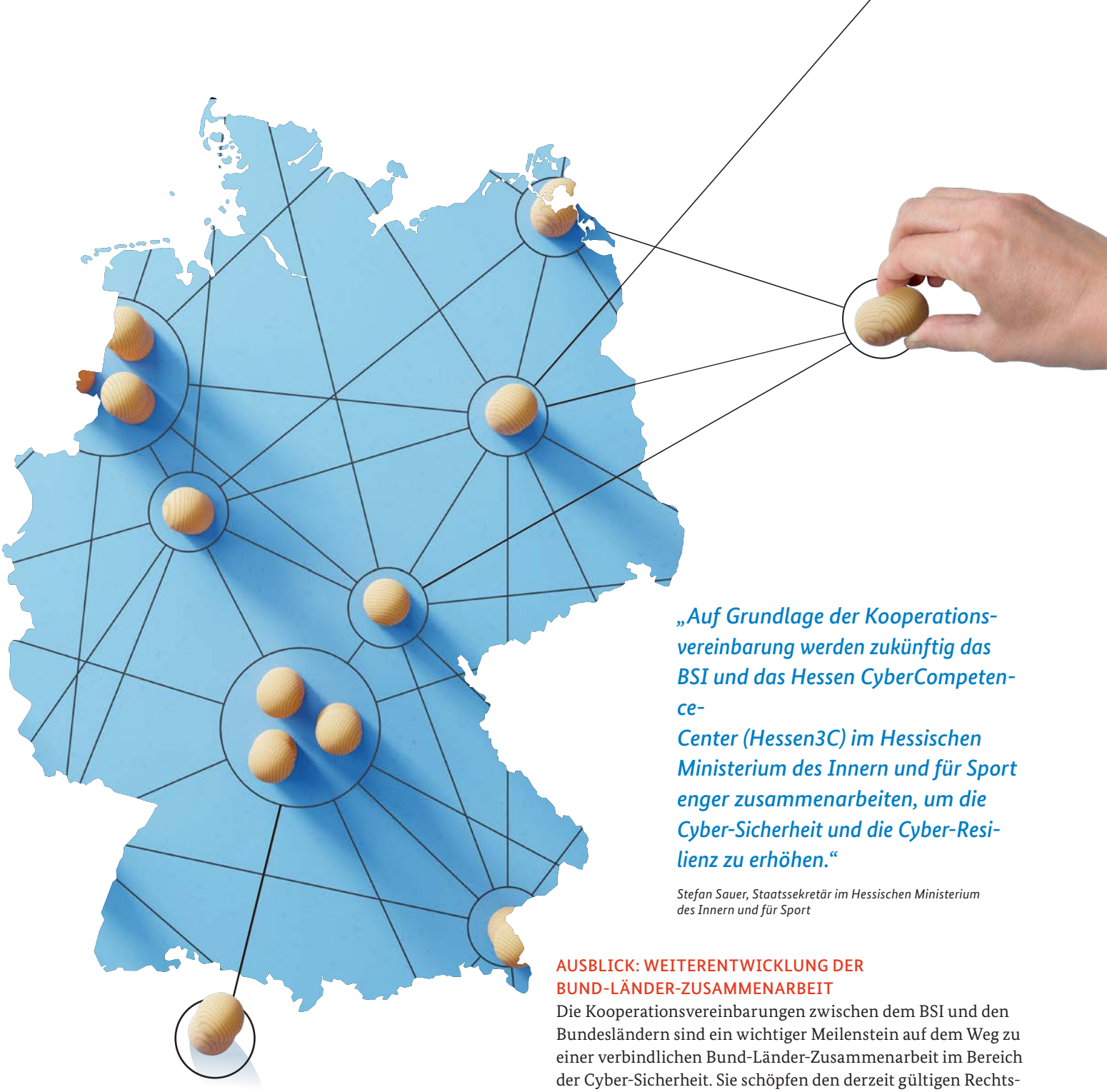
Das BSI kann gemäß § 3 des BSI-Gesetzes (BSIG) die Länder in Fragen der Informationssicherheit beraten und warnen sowie auf deren Ersuchen bei der Sicherung ihrer Informationstechnik und Abwehr von Gefahren unterstützen. Basierend auf diesen Rahmenbedingungen hat das Bundesamt einen Katalog von Kooperationsfeldern erarbeitet, aus dem die Länder die Kooperationen auswählen können, für die sie einen Bedarf haben.

V. l.: Stefan Sauer, Innenstaatssekretär des Landes Hessen; BSI-Vizepräsident Dr. Gerhard Schabhüser

Zu den Kooperationsfeldern gehören unter anderem „Durchführung gemeinsamer Veranstaltungen“, „Beratung des BSI zu bestimmten Fachthemen“ oder die „Unterstützung der Länder bei Vorfallsmeldungen“.

> *„Mit dieser Vereinbarung werden wir uns jetzt noch enger vernetzen und unsere Kräfte weiter bündeln.“*
>
> *Alexander Schweitzer, Digitalisierungsminister des Landes Rheinland-Pfalz*

Die Länder können diese Kooperationsangebote durch eigene Angebote ergänzen, die das BSI seinerseits nutzen kann. Es ist im Sinne der Kooperationsvereinbarung, dass mit dem BSI und den Ländern alle Kooperationspartner in gleichem Maße profitieren. Jede Vereinbarung kann so individuell auf die jeweiligen Bedarfe des Landes und des BSI zugeschnitten werden.



„Auf Grundlage der Kooperationsvereinbarung werden zukünftig das BSI und das Hessen CyberCompetence-Center (Hessen3C) im Hessischen Ministerium des Innern und für Sport enger zusammenarbeiten, um die Cyber-Sicherheit und die Cyber-Resilienz zu erhöhen."

Stefan Sauer, Staatssekretär im Hessischen Ministerium des Innern und für Sport

ABSCHLUSS VON KOOPERATIONSVEREINBARUNGEN MIT DEN LÄNDERN

Die erste Kooperationsvereinbarung unterzeichneten das BSI und das Land Niedersachsen Ende 2021. Danach folgten das Saarland, das Land Hessen und das Land Rheinland-Pfalz. Weitere Vereinbarungen sind bereits geplant oder unmittelbar in Vorbereitung.

Die im Rahmen der Kooperationsvereinbarungen festgelegten Arbeitsprogramme sind derzeit in der Umsetzung. So haben bereits gemeinsame Veranstaltungen sowie Beratungen zum Aufbau eines Managementsystems für Informationssicherheit (ISMS) stattgefunden.

Schon nach vier Kooperationsvereinbarungen steht aus Sicht des BSI fest, dass sich das Cyber-Sicherheitsniveau in Deutschland durch diese Aktivitäten verbessert.

AUSBLICK: WEITERENTWICKLUNG DER BUND-LÄNDER-ZUSAMMENARBEIT

Die Kooperationsvereinbarungen zwischen dem BSI und den Bundesländern sind ein wichtiger Meilenstein auf dem Weg zu einer verbindlichen Bund-Länder-Zusammenarbeit im Bereich der Cyber-Sicherheit. Sie schöpfen den derzeit gültigen Rechtsrahmen der ebenenübergreifenden Zusammenarbeit aus.

Allerdings gibt es den Bedarf an engerer Zusammenarbeit, um aktuellen und künftigen Bedrohungslagen im Cyber-Raum noch adäquater begegnen zu können. So hat das BSI aktuell etwa keine Möglichkeit, die Länder bei der Detektion von Schadsoftware in den Landesnetzen, beispielsweise durch Bereitstellung von Sensorik, zu unterstützen. Deshalb erarbeitet das Bundesamt aktuell ein Konzept zum Ausbau des BSI zur Zentralstelle im Bund-Länder-Verhältnis, das einen Ausbau der gesetzlichen Grundlagen der Bund-Länder-Zusammenarbeit im Bereich Cyber-Sicherheit beleuchtet.

Unabhängig von diesem möglichen Ausbau wird die Option bilateraler Kooperationsvereinbarungen fortbestehen, da so verbindliche und individuelle Kooperationen zwischen dem BSI und den Ländern vereinbart werden können. ■

Karriere gestalten im #TeamBSI

Eine Behörde, viele Karrierepfade

von Alessandra Krüger, Referat Personalentwicklung

Viele Wege führen ins BSI – und auch die Karriereleiter nach oben. Vom Einstieg über eine Ausbildung bis hin zur Förderung eines Masters und einer Fach- oder Führungskarriere: Im BSI gibt es auf jeder Karrierestufe weitere Entwicklungsmöglichkeiten. Alles unter dem Dach einer Behörde.

Karriere- und Entwicklungsmöglichkeiten sind ein wichtiger Faktor bei der Wahl des Arbeitgebers. Deswegen hat es sich das BSI zur Aufgabe gemacht, Zukunftsperspektiven zu schaffen. Die Weiterentwicklung über die klassische Karriereleiter ist dabei ebenso eine Option wie horizontale Fort- und Weiterbildungen.

Der berufliche Einstieg beim BSI ist auf vielen Wegen und in vielen Fachrichtungen möglich. Ausbildungsgänge für Verwaltungsfachangestellte sowie Fachinformatiker und Fachinformatikerinnen Systemintegration, das duale Studium Digital Administration and Cyber Security (DACS), Praktika und Abschlussarbeiten, Referendariate und die Option für Studentenjobs sind einige der Möglichkeiten. Viele Einstiege ergeben sich zudem aus den Stellenangeboten für Personen mit bereits abgeschlossener Ausbildung oder abgeschlossenem Studium.

„Die Ausbildung im BSI ist durchgehend spannend gestaltet. Dabei lernen wir durch die regelmäßige Rotation in den Referaten und Abteilungen, IT-Sicherheit in den verschiedenen Facetten zu gestalten."

Jason, Auszubildender zum Fachinformatiker Systemintegration

„Wir Azubis im Bereich Verwaltung erleben das BSI als einen bunten und aufgeschlossenen Arbeitgeber. Immer wieder wird uns ermöglicht, neue Bereiche kennenzulernen. Auf unseren Wegen erhalten wir jederzeit die erforderlichen Stützräder, um uns bestmöglich weiterentwickeln zu können."

Hannah, Auszubildende zur Verwaltungsfachangestellten

VON DER SCHULE DIREKT INS BSI

Die Ausbildungsgänge sind jeweils die Anfangspfade für den Berufseinstieg im technischen und nicht technischen Dienst. Während sich die Verwaltungsfachangestellten eher mit Themen wie Personalmanagement, Haushaltswesen und Materialbeschaffung beschäftigen, fokussiert die Ausbildung in der Fachinformatik die Umsetzung von Anforderungen in komplexe Hard- und Softwaresysteme sowie die Beratung und Schulung von Kundinnen und Kunden sowie Nutzenden dieser Systeme.

„Was mich im DACS-Studiengang und im BSI besonders begeistert, sind die Themen rund um Cyber-Angriffe und ihre Auswirkungen in unterschiedlichen Bereichen. Zudem lernen wir im Studium interessante Informatik-Grundlagen in Bereichen wie Assembler-programmierung, formale Sprachen, Python oder Java."

Mombert, DACS-Studierender

EINSTIEG ODER AUFSTIEG MIT DEM DACS-STUDIUM

Das duale Studium DACS gliedert sich in vier Studiensemester an der Hochschule des Bundes in Brühl und zwei Praxissemester im BSI. Diese lassen sich an allen Standorten des BSI, in Bonn, Freital oder Saarbrücken, durchführen und führen die Studierenden an die praktischen Aufgaben heran. Im zweiten Praktikum steht die Diplomarbeit an, hier arbeiten die Praktikumsreferate und die Studierenden gemeinsam an einem Thema mit wissenschaftlichem und praktischem Mehrwert. Die Diplomarbeit wird hier also nicht für die Schublade geschrieben, sondern bringt Erkenntnisse und neue Herangehensweisen für das BSI und die Studierenden in ihrer späteren Tätigkeit. Kolleginnen und Kollegen, die bereits im BSI arbeiten, haben die Möglichkeit, das DACS-Studium auch als Aufstiegsmöglichkeit und für den nächsten Karriereschritt zu absolvieren.

NEBENBERUFLICH ZUM BACHELOR ODER MASTER

Weitere Aufstiegsmöglichkeiten über Studiengänge werden den Mitarbeitenden im BSI über die Bachelor- und Masterförderung geboten. Das BSI übernimmt dabei pro Jahr für sechs Mitarbeitende (vier Bachelor, zwei Master) bis zu 50 Prozent der Studiengebühren bei einem nebenberuflichen Studium mit IT-Schwerpunkt. Auch hier unterstützt das BSI bei anstehenden Seminar- und Abschlussarbeiten durch interne Praktika und Hospitationen in unterschiedlichen Bereichen, um den Studierenden ein möglichst umfassendes Bild zu der jeweiligen Thematik zu geben.

IN FÜHRUNG GEHEN

Das Führungskräftenachwuchs-Programm ist seit vielen Jahren ein fester Baustein der Personalentwicklung. Es fördert Potenzialträgerinnen und -träger aus den eigenen Reihen und gibt diesen ein gutes Rüstzeug für eine potenzielle Führungsposition mit. Auch hier wird durch das Programm der Gedanke „voneinander und miteinander lernen" unterstützt, um die Teilnehmenden in wichtigen Führungsqualifikationen zu stärken und zu vernetzen.

FACH- STATT FÜHRUNGSKARRIERE

Doch nicht für alle liegt die Erfüllung der Karriere in einer Führungstätigkeit. Durch Hospitationen in anderen Arbeitsbereichen ebenso wie durch Weiterbildungen und vielfältige Vernetzungsangebote entwickeln Beschäftigte im BSI die eigenen Kompetenzen weiter. Indem Stellen zunächst intern ausgeschrieben werden, haben die Mitarbeitenden die Möglichkeit, andere Aufgabengebiete kennenzulernen.

Für diejenigen, die statt Führung lieber in ihrer fachlichen Tätigkeit bleiben, ihr Spezialwissen vertiefen und intern weitergeben sowie das BSI sowohl national als auch international in Expertengruppen, Fach-Communitys und Gremien vertreten wollen, wurde die Fachkarriere geschaffen. Fachspezialistinnen und -spezialisten sind anerkannte Expertinnen und Experten auf ihrem Gebiet und können dies auch bleiben, ohne auf die nächste Karrierestufe verzichten zu müssen. ■

„Die Fachkarriere ist für mich eine Aufstiegsmöglichkeit, bei der ich weiterhin spannende Themen fachlich bearbeiten und voranbringen kann. Dabei habe ich durch meine gute Vernetzung, aber insbesondere auch durch den Austausch mit den Fachspezialistinnen und -spezialisten aus den anderen Abteilungen einen großartigen Blick auf neue zukunftsorientierte Themen für das BSI."

Angelika, Fachspezialistin

Der 19. Deutsche IT-Sicherheits-kongress

„Digital sicher in eine nachhaltige Zukunft“: Am 10. und 11. Mai 2023 fand der 19. Deutsche IT-Sicherheitskongress statt. Live-Vorträge, Podiumsdiskussionen und virtuelle Messestände machten Cyber-Sicherheit erlebbar. Aber sehen Sie selbst …

9.600 Teilnehmende

24 Aussteller

28 Fachvorträge

176 Paper Einreichungen

Weitere Informationen:

https://www.bsi.bund.de/DE/Service-Navi/Veranstaltungen/Deutscher-IT-Sicherheitskongress/19-Dt-IT-Sicherheitskongress/19-dt-IT-Sicherheitskongress_node.html

Eine quantensichere Public-Key-Infrastruktur für die öffentliche Verwaltung

Die Migration zu einer quantensicheren Verwaltungs-PKI führt die öffentliche Verwaltung in das Post-Quanten-Zeitalter

von Dr. Kaveh Bashiri und Dr. Stavros Kousidis, Referat Vorgaben an und Entwicklung von Kryptoverfahren

Das BSI betreibt die Wurzelzertifizierungsstelle für die Public-Key-Infrastruktur der öffentlichen Verwaltung (V-PKI). Die aktuell verwendeten kryptografischen Algorithmen in dieser V-PKI sind nicht quantensicher. Um der drohenden Gefährdung durch kryptografisch relevante Quantencomputer rechtzeitig begegnen zu können, plant das BSI die Migration zu einer quantensicheren V-PKI.

Zur Absicherung des elektronischen Datenverkehrs in Behörden und öffentlichen Institutionen wird eine Public-Key-Infrastruktur (Verwaltungs-PKI, oder kurz: V-PKI) eingesetzt, deren Wurzelzertifizierungsstelle (Root-CA) vom BSI betrieben wird. Die Endnutzer-Zertifikate aus dieser PKI werden für Standardanwendungen wie S/MIME und TLS benutzt. Aktuell basiert die Kryptografie der V-PKI auf dem nicht quantensicheren RSA-Verfahren.

Public-Key-Infrastrukturen (PKI) sind ein wesentlicher Baustein der Cyber-Sicherheit, da sie ein vertrauenswürdiges Identitätsmanagement bereitstellen. Daher ist die Migration zu einer quantensicheren V-PKI ein wesentlicher Schritt in das Post-Quanten-Zeitalter für die digitale öffentliche Verwaltung.

AUSWAHL GEEIGNETER POST-QUANTEN-VERFAHREN

Ein wichtiger Aspekt bei diesem Migrationsvorhaben ist die Auswahl der Post-Quanten-Verfahren. Neben ihrer Sicherheit und Performance ist die Sicherstellung der Interoperabilität ein wesentliches Kriterium. Demnach kommen nur standardisierte Verfahren infrage. Die Anforderung an die Interoperabilität umfasst aber auch das Einbeziehen allgemeiner Entwicklungen im kommerziellen Bereich, um die Kompatibilität mit Standardanwendungen zu gewährleisten.

Das US-amerikanische National Institute of Standards and Technology (NIST) hat im Juli 2022 das Schlüsseltransportverfahren CRYSTALS-Kyber sowie die Signaturverfahren CRYSTALS-Dilithium, Falcon und SPHINCS+ zur Standardisierung ausgewählt. Die hashbasierten Signaturverfahren XMSS/XMSS^MT und LMS/HSS sind bereits standardisiert, stellen jedoch durch ihre sogenannte Zustandsbehaftung eine Herausforderung für die Schlüsselverwaltung dar. Durch die Zustandsbehaftung ist die Anzahl der erstellbaren Signaturen pro Schlüsselpaar beschränkt und bei jeder Signaturerzeugung muss ein streng monotoner Zähler fehlerfrei hochgezählt werden.

Aus Sicht des BSI kommen auf der Ebene der Endnutzer deshalb ausschließlich nicht zustandsbehaftete Signaturverfahren in Frage, da hier eine Zählerverwaltung nicht praktikabel ist. Welche genauen Verfahren auf dieser Ebene ausgewählt werden, wird erst nach der Veröffentlichung der NIST-Standardisierungsentwürfe entschieden. Auf der Ebene der Root-CA der V-PKI prüft das BSI hingegen den Ansatz, XMSS/XMSS^MT oder LMS/HSS einzusetzen, da deren Sicherheitseigenschaften sehr gut verstanden sind. Das BSI hält die Zustandsverwaltung in der kontrollierten Umgebung der Root-CA, in der grundsätzlich Hardwaresicherheitsmodule zur Signaturerzeugung verwendet werden, für umsetzbar.

Das BSI setzt auf hybride Lösungen, in denen ein standardisiertes Post-Quanten-Verfahren in Kombination mit einem klassischen Algorithmus – z. B. basierend auf Elliptic Curve Cryptography – zum Einsatz kommt. Die einzige Ausnahme hierbei bilden die hashbasierten Signaturverfahren, deren Einsatz aufgrund ihrer Sicherheitseigenschaften auch nicht-hybrid erfolgen kann.

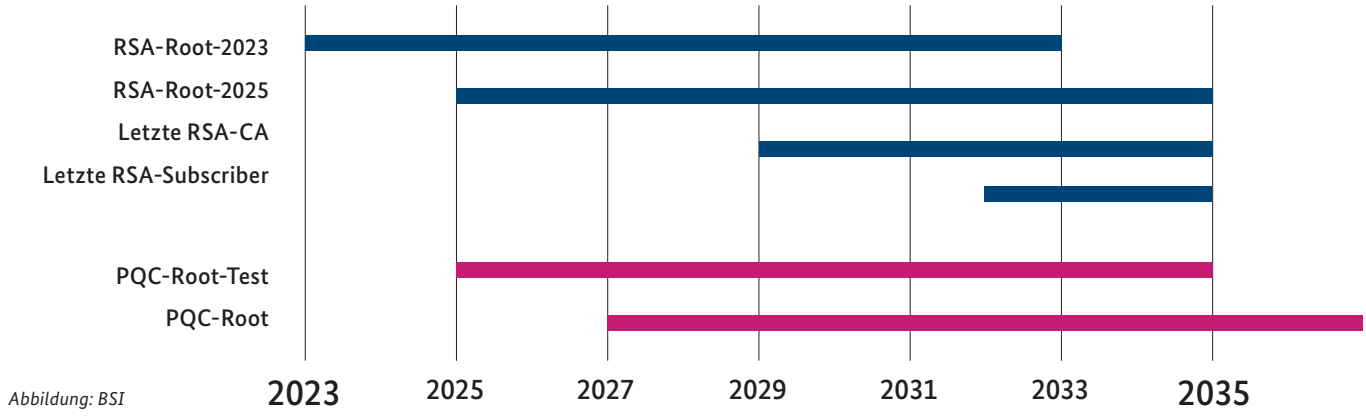


Abbildung: BSI

Beispielhafte Abbildung einer Migration mit einem parallelen Ansatz. Die einzelnen Balken stellen jeweils Gültigkeitszeiträume dar, die Zertifikatsvalidierung erfolgt nach dem Schalenmodell. In diesem Beispiel wird angenommen, dass 2025 eine letzte RSA-Root ausgegeben wird und die Root-Zertifikate jeweils zehn, die (Sub-)CA-Zertifikate sechs und die Endnutzer-Zertifikate drei Jahre gültig sind. PQC steht für Post-Quantum Cryptography.

ZERTIFIKATSGESTALTUNG

Da die aktuell in der V-PKI verwendeten kryptografischen Algorithmen auf RSA basieren, ist es bisher möglich, sowohl für die Signaturerstellung als auch für die Verschlüsselung dasselbe Schlüsselpaar und somit ein einzelnes Zertifikat zu verwenden. In einer quantensicheren PKI werden die Endnutzer hingegen zwangsläufig getrennte Signatur- und Verschlüsselungszertifikate besitzen müssen, da hier nur unterschiedliche Algorithmen zur Auswahl stehen.

Ein wichtiger Aspekt zur Gewährleistung von Interoperabilität ist die Standardisierung der Post-Quanten-Verfahren in gängigen Zertifikatsformaten. Hier leistet das BSI derzeit in Kooperation mit der genua GmbH einen Beitrag für X.509-Zertifikate.

MIGRATIONSKONZEPT

Die Migration soll über einen parallelen Ansatz durchgeführt werden. Das bedeutet, dass die aktuelle, auf RSA basierende V-PKI bis zum vollständigen Umstieg aller Endnutzer-Zertifikate aktiv bleibt, während parallel dazu eine quantensichere V-PKI aufgebaut wird. Dadurch soll ein umfangreicher Testbetrieb sowie ein unterbrechungsfreier Übergang ohne Stichtagsumstellung ermöglicht werden.

Es steht fest, dass eine PKI-Migration im Allgemeinen enorm aufwändig ist und – aufgrund langer Zertifikatslaufzeiten – mit erheblichen Migrationszeiten zu rechnen ist (siehe Abbildung). Daher ist es wichtig, die Migration frühzeitig zu planen und zu initiieren, um den Umstieg auf die Post-Quanten-Kryptografie rechtzeitig und mit der erforderlichen Betriebskontinuität umsetzen zu können. ■

Weitere Informationen:

https://doi.org/10.6028/NIST.SP.800-208

https://datatracker.ietf.org/doc/draft-gazdag-x509-hash-sigs/

Digitale Souveränität braucht die Cloud

Cloud Computing ist das Rückgrat der Digitalisierung und einer modernen und digitalen Verwaltung

von Vera Sikes, Fachbereichsleiterin IT-Infrastrukturen, und Dr.-Ing. Clemens Doubrava, Referatsleiter Virtualisierung und Cloud-Sicherheit

Cloud Computing hat sich auch für geschäftskritische Anwendungen durchgesetzt. Auch die Bundesverwaltung treibt Cloud-Projekte voran, darunter die „Bundescloud“, die „Betriebsplattform Bund“ des Informationstechnikzentrums Bund, die „Microsoft Sovereign Cloud“ und die „Deutsche Verwaltungscloud“.

Cloud Computing ist ein Paradigma: Über ein Netzwerk kann auf einen Pool gemeinsam nutzbarer physikalischer oder virtueller Ressourcen, wie Rechenleistung, Speicher, Anwendungen, bedarfsgerecht zugegriffen werden. Die Administration beim Cloud-Anbieter ist hochautomatisiert. In der Cloud gibt es grundlegende Prinzipien: „Everything as a Service“ – alles wird als Dienst erbracht, „Everything as Code“ – für jeden Cloud-Dienst gibt es einen Bauplan (Code). „Software-Defined“ bedeutet, dass keine Abhängigkeit von der Hardware besteht, und „Serverless Computing“, dass die Dienste auf minimalen Kerneln laufen.

CLOUD-SICHERHEIT

Cloud-Nutzung kommt nicht ohne Gefährdungen. Der Cloud-Nutzer wird vom Cloud-Anbieter abhängig und verliert im Vergleich zum Eigenbetrieb Kontrolle über seine Datenverarbeitung. Cloud-Anbieter stellen aufgrund des hohen Datenvolumens daher ein lohnendes Ziel für Angreifer dar. Zudem sind leistungsfähige Cloud-Infrastrukturen sehr komplex und Schwachstellen sowie Konfigurationsfehler können weitreichende Auswirkungen für viele haben.

Kann angesichts dessen eine Cloud sicher sein? Eine 100-prozentig sichere Cloud gibt es ebenso wenig wie eine 100-prozentig sichere IT. Aber es gibt Cloud-spezifische Aspekte, die für mehr Informationssicherheit sorgen:

- Cloud-Infrastrukturen basieren auf „Zero Trust“: Niemandem wird vertraut, sondern es wird immer geprüft, ob die Berechtigung für eine Verbindung oder einen Datenaustausch vorliegt.
- In der Cloud wird jede Aktion protokolliert. Das erleichtert es, potenzielle Angriffe, Fehlkonfigurationen oder Softwarefehler sehr schnell zu entdecken und darauf zu reagieren.
- Cloud-Anbieter verfügen über hochautomatisierte Update- und Change-Prozesse, so dass Cloud-Infrastrukturen immer auf dem neuesten Stand sind und Sicherheitspatches schnell eingespielt werden.
- Die Administration des Cloud-Anbieters erfolgt über abgesicherte Schnittstellen durch streng überwachte Prozesse, so dass es keinen direkten Zugriff auf Kundendaten gibt.
- Jede Kommunikationsverbindung in der Cloud ist verschlüsselt, ebenso gespeicherte Daten.
- Da in der Cloud alles „Software-Defined“ ist, kann ein Cloud-Anbieter sehr schnell auf Vorfälle reagieren: Netzsegmente trennen, Dienste herunterfahren, Schutzmaßnahmen aktivieren und Dienste schnell wiederherstellen.
- Public-Cloud-Anbieter betreiben in der Regel georedundante Rechenzentren. Fällt ein Rechenzentrum aus, übernimmt ein anderes unterbrechungsfrei.
- Die Sicherheitslösungen der Cloud-Anbieter skalieren aufgrund der hohen Standardisierung und Automatisierung der Cloud-Infrastruktur sehr gut. Davon profitieren alle Kunden gleichermaßen.

CLOUD UND DIGITALE SOUVERÄNITÄT

Digitale Souveränität beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“, definiert der Beauftragte der Bundesregierung für Informationstechnik. Um selbstbestimmt zu handeln, ist eine Wahl- und Wechselmöglichkeit zwischen unterschiedlichen Cloud-Angeboten und -Anbietern unerlässlich. Cloud Computing basiert auf Schnittstellen und je interoperabler sie sind, desto einfacher ist der Wechsel zwischen Cloud-Diensten und -Anbietern. Damit vermeiden Organisationen Abhängigkeiten, die ein selbstbestimmtes Handeln verhindern.

Eine wesentliche Grundlage für Digitale Souveränität ist IT-Sicherheit. Cloud-Infrastrukturen bieten aufgrund ihrer Architektur eine sehr hohe Resilienz auch gegen ausgeklügelte Angriffe, basierend auf präventiven Maßnahmen, Detektionsfähigkeiten und Reaktionsmechanismen. Selbstständiges Handeln impliziert die Möglichkeit, Cloud-Dienste selbst zu entwickeln oder anzupassen. Das geht dann gut, wenn Open-Source-Software eingesetzt wird. Zwar gibt es Cloud-Anbieter die das konsequent umsetzen, aber der Markt wird von Anbietern mit proprietären Lösungen dominiert.

Um Cloud Computing sicher nutzen zu können, arbeitet das BSI an den Cloud-Projekten des Bundes mit, damit dieser zukunftssicher aufgestellt ist und souverän handeln kann. Es unterstützt Cloud-Nutzer dabei, fundierte, risikobasierte Entscheidungen treffen zu können, z. B. auf Basis des BSI C5. So wird Cloud Computing die Grundlage für die Digitalisierung von Unternehmen ebenso wie der Öffentlichen Verwaltung. ■

Weitere Informationen:

Cloud Computing Compliance Criteria Catalogue (C5) des BSI: https://www.bsi.bund.de/C5

Digitale Souveränität: https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html

Wirkungsvoller Schutz für kleine und Kleinstunternehmen

Der CyberRisikoCheck nach DIN SPEC 27076

von Manuel Bach, Referatsleiter Cyber-Sicherheit für Kleine und Mittlere Unternehmen (KMU) und Leiter des DIN SPEC 27076-Konsortiums

Immer mehr Verantwortliche in kleinen und mittleren Unternehmen (KMU) erkennen, dass sie ohne ihre IT-Systeme nicht mehr arbeitsfähig sind und sie diese daher angemessen schützen müssen. Oftmals wissen sie aber weder, wie gut oder schlecht es um ihre Informationssicherheit konkret bestellt ist, noch, welche Wege sinnvollerweise zu gehen sind, um das Schutzniveau zu erhöhen. Hierfür gibt es nun endlich eine praktikable Lösung, die der Staat obendrein auch finanziell unterstützt.

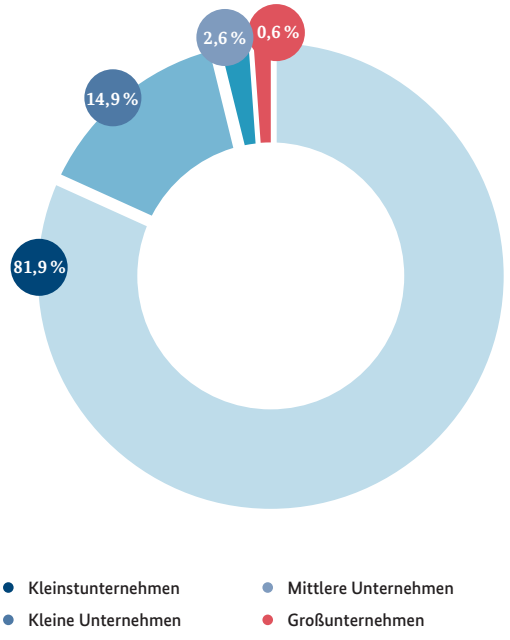
99,4 Prozent der Unternehmen in Deutschland zählen zu den kleinen und mittleren Unternehmen (KMU). Aufgrund der fortschreitenden Digitalisierung ihrer Geschäftsprozesse sind diese inzwischen durch Cyber-Angriffe und IT-Ausfälle genauso bedroht wie vor einigen Jahren nur große Unternehmen und Behörden. Durch den Aufbau eines Referates beim BSI, das ausschließlich für die Belange der KMU zuständig ist, konnte das BSI seine Angebote für diese Zielgruppe mittlerweile deutlich erweitern – der CyberRisikoCheck ist eines davon.

VIELE PARTNER FÜR EINE LÖSUNG

Viele KMU würden gerne mehr für ihre IT-Sicherheit tun, wissen aber oftmals nicht, wie. Bereits existierende Standardwerke zum Aufbau eines Informationssicherheitsmanagementsystems, das IT-Grundschutz-Kompendium des BSI oder Normen wie die ISO/IEC 27001, sind insbesondere für Unternehmen mit weniger als 50 Beschäftigen aber nicht optimal geeignet. Um dieses Problem zu adressieren, wurde daher in Kooperation mit dem Bundesverband mittelständische Wirtschaft (BVMW) ein Konsortium zur Erarbeitung einer DIN SPEC gegründet. Finanziert wurde das Projekt durch das Bundesministerium für Wirtschaft und Klimaschutz im Rahmen seines Programmes „Mittelstand Digital“. Neben dem BSI, das die Leitung des Konsortiums innehatte, und dem BVMW, der die stellvertretende Leitung des Konsortiums übernahm, waren fast 20 weitere Partner beteiligt, u. a. das Deutsche Institut für Normung (DIN), Wirtschaftsförderungen, eine Tochter des Gesamtverbandes der deutschen Versicherungswirtschaft, IT-Grundschutz-Expertinnen und -Experten, -Auditorinnen und -Auditoren sowie Fachkundige zum Thema Datenschutz und IT-Dienstleister.

Ergebnis der achtmonatigen Arbeit des Konsortiums ist die DIN SPEC 27076 „IT-Sicherheitsberatung für kleine und Kleinstunternehmen“ und der darauf basierende CyberRisikoCheck. Durch diesen können KMU bei IT-Dienstleistern eine standardisierte Beratung erhalten, die speziell an ihre Bedürfnisse angepasst ist. Denn auch die Handlungsempfehlungen wurden in der DIN SPEC standardisiert. Dadurch wissen sowohl Auftraggeber als auch Auftragnehmer, welche Leistung zu erwarten bzw. zu erbringen ist.

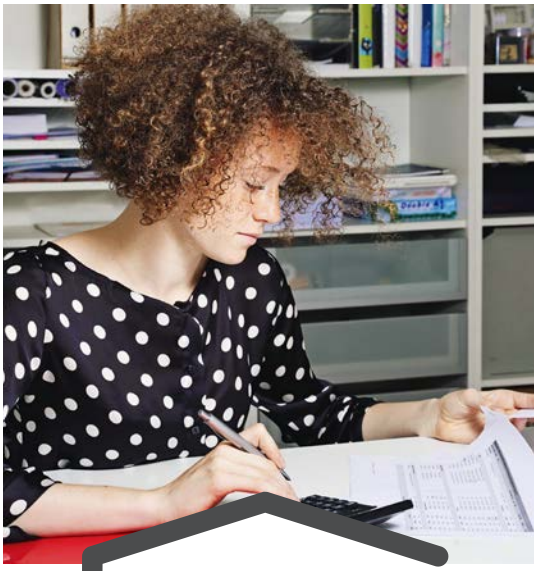
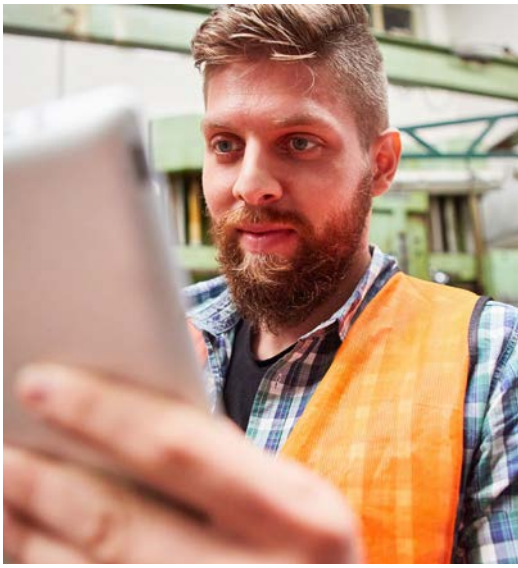
Unternehmen in Deutschland nach Größe
Angaben in %



Quelle: Statistisches Bundesamt, Stand: Juli 2021





CyberRisiko Check

DURCHFÜHRUNG DES CYBERRISIKO-CHECKS

Beim CyberRisikoCheck befragt ein IT-Dienstleister ein Unternehmen in einem ein- bis zweistündigen Interview. Darin werden 27 Anforderungen aus sechs Themenbereichen daraufhin überprüft, ob das Unternehmen sie erfüllt. Für die Antworten werden nach den Vorgaben der DIN SPEC Punkte vergeben. Als Ergebnis erhält das Unternehmen einen Bericht, der u. a. die Punktzahl und für jede nicht erfüllte Anforderung eine Handlungsempfehlung enthält. Die Handlungsempfehlungen sind nach Dringlichkeit gegliedert und erhalten auch Hinweise darauf, welche staatlichen Fördermaßnahmen (auf Bundes-, Landes- und kommunaler Ebene) das jeweilige Unternehmen in Anspruch nehmen kann.

Der CyberRisikoCheck ist keine IT-Sicherheitszertifizierung. Er ermöglicht einem Unternehmen jedoch eine Positionsbestimmung des eigenen IT-Sicherheitsniveaus. Er zeigt zudem auf, welche konkreten Maßnahmen ein Unternehmen umsetzen bzw. bei einem IT-Dienstleister beauftragen sollte.

VORTEILE FÜR ALLE BETEILIGTEN

Die Kosten für einen CyberRisikoCheck belaufen sich auf die Kosten eines Beratertages. Auf Bundesebene werden der Check und sich daran anschließende Handlungsempfehlungen bereits jetzt über das Programm „go-digital“ mit 50 Prozent bezuschusst. Mehrere Bundesländer haben inzwischen ebenfalls Förderbereitschaft signalisiert.

Da das BSI die anonymisierten Erhebungsdaten der CyberRisikoChecks erhält, kann das Nationale IT-Lagezentrum zukünftig erstmals auf valide Daten zur Cyber-Sicherheit der KMU zurückgreifen und in die BSI-Berichte zur Cyber-Sicherheitslage mit aufnehmen. Der CyberRisikoCheck trägt damit auch zur Weiterentwicklung präventiver Angebote von Bund, Ländern und Kommunen bei. ■

Weitere Informationen:

www.bsi.bund.de/kmu

www.bsi.bund.de/dok/crc

www.foerderdatenbank.de

Sichere E-Mail-Kommunikation

Technische Richtlinien für Transport und Authentizität von E-Mails

von Kristina Pohl, Referat Cyber-Sicherheit in Smart Home und Smart Cities

Die E-Mail ist 2023 weiterhin ein wichtiges Kommunikationsmittel, das auch für vertrauliche Nachrichten in sensiblen Bereichen Verwendung findet. Dennoch werden E-Mails häufig ohne Signatur und Verschlüsselung versendet.

Deshalb beschreiben die Technischen Richtlinien für sicheren E-Mail-Transport (BSI TR-03108) und E-Mail-Authentizität (BSI TR-03182) Maßnahmen, mit denen E-Mail-Diensteanbieter (EMDA) das Sicherheitsniveau – ohne zusätzlichen Aufwand für die Nutzenden – deutlich verbessern können.

PRAXISNAHE STANDARDS UND TECHNOLOGIEN

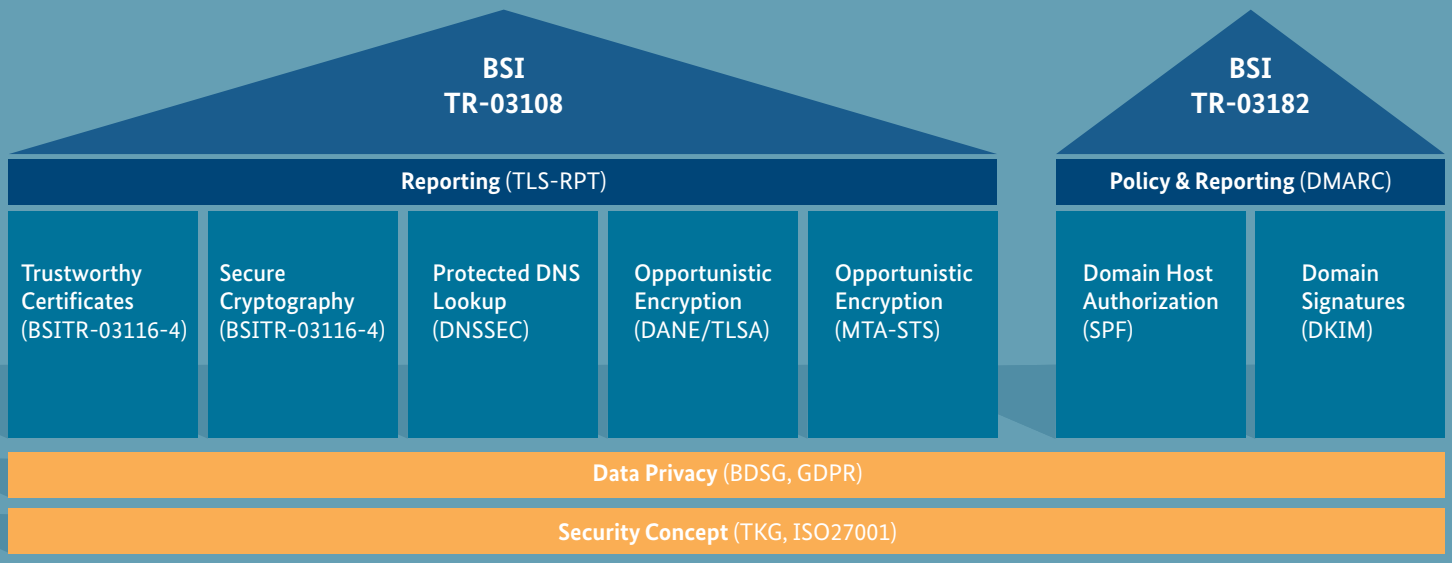
Um dem Stand der Technik fortlaufend gerecht zu werden, wurde die bisherige TR-03108 aktualisiert und erweitert. Dabei wurde besonders auf bereits am Markt etablierte Sicherheitsstandards und Technologien gesetzt. Zugleich wurden die Vorgaben für die zu nutzenden Kryptoalgorithmen modernisiert und die Forderung nach einem Reporting-Mechanismus aufgenommen. Letzterer ermöglicht die kontinuierliche Verbesserung aller übrigen Sicherheitsmaßnahmen und die frühzeitige Erkennung von Problemen wie beispielsweise Verbindungsfehlern.

SICHER VERSCHLÜSSELN: SO GEHT'S

EMDA ermöglichen durch die Implementierung von TLS (Transport Layer Security) jedem Kommunikationspartner die Zustellung verschlüsselter E-Mails und durch DANE (DNS-based Authentication of Named Entities) die Verifikation der genutzten Zertifikate. Letztere dienen der Authentisierung und Verschlüsselung auf Transportebene. Der sendende EMDA sorgt durch die Implementierung von DANE dafür, dass eine E-Mail verschlüsselt werden muss, wenn die Empfängerseite DANE unterstützt. Die Nutzung von DANE schützt somit davor, dass durch eine Manipulation bei der Aushandlung der Kommunikationssicherheit diese auf ein unsicheres Niveau reduziert wird (sog. Downgrade-Attacke).

Da DNS-Fingerprints zur Verifikation der Zertifikate auf DNS-Servern veröffentlicht werden, ist die Verwendung von DNSSEC (Domain Name System Security Extensions) Voraussetzung für DANE. Nur mit DNSSEC lässt sich eine sichere Abfrage beim DNS-Server gewährleisten. Manche EMDA sehen die Implementierung von DNSSEC jedoch als größere Herausforderung an, da die DNS-Einträge ihrer Domains angepasst werden müssen.

Für den Fall, dass der Kommunikationspartner DANE nicht unterstützt, wurde der Standard MTA-STS (Mail Transfer Agent-Strict Transport Security) als zusätzliche Option in die aktualisierte Version der TR-03108 aufgenommen. Mittels MTA-STS kann ein EMDA einem anfragenden Mail-Server mitteilen, dass eine TLS-gesicherte Verbindung unterstützt wird und sich das verwendete Zertifikat über den MTA-STS-Server verifizieren lässt. MTA-STS ist einfacher implementierbar, bietet aber ein geringeres Schutzniveau als DANE.



AUFBAU TR-03108 UND TR-03182

Quelle: BSI

ANFORDERUNGEN AN DIE AUTHENTIZITÄT VON E-MAILS

In der neuen TR-03182 werden erstmals Anforderungen an die Authentizität von E-Mails formuliert. Mit den Technologien DKIM (Domain Keys Identified Mail) und SPF (Sender Policy Framework) wird die Identität einer Senderdomain überprüft. Dadurch sollen SPAM, Spoofing und Phishing erschwert werden. Mit DMARC (Domain-based Message Authentication, Reporting and Conformance) gibt es auch in dieser TR einen Reporting-Mechanismus, der Voraussetzung für die Konformität zur TR ist. Dieser ermöglicht den EMDA, ihre Sicherheitsmaßnahmen kontinuierlich zu optimieren, indem die Kommunikationspartner via Reporting aktiv auf Probleme hinweisen.

Beide Richtlinien geben zudem Hinweise für eine korrekte Implementierung und sinnvolle Konfiguration, um Fehler bei der Umsetzung der Maßnahmen schon von Beginn an zu vermeiden.

IT-SICHERHEITSKENNZEICHEN UND ZERTIFIZIERUNG

Als praktische Orientierungshilfe für Nutzende auf der Suche nach einem EMDA vergibt das BSI das IT-Sicherheitskennzeichen auf Basis der TR-03108 (s. auch Artikel auf S. 28). Hierbei verspricht ein EMDA, die verpflichtenden Anforderungen der TR zu erfüllen, und unterstellt sich der Marktüberwachung durch das BSI.

Zusätzlich zum IT-Sicherheitskennzeichen können EMDA sich die Erfüllung der Anforderungen der TR-03108 durch ein Zertifikat bestätigen lassen. Das BSI arbeitet derzeit an der Optimierung des bestehenden Verfahrens. Dabei werden für die TR-03108 zukünftig beim BSI anerkannte Prüfstellen den Nachweis über die Erfüllung der Anforderungen für eine Zertifizierung durch das BSI erbringen. Durch die Entwicklung und Aktualisierung der vorgestellten Technischen Richtlinien sowie durch die Optimierung des Zertifizierungsverfahrens leistet das BSI einen wichtigen und praxisorientierten Beitrag für mehr E-Mail-Sicherheit. ■

Weitere Informationen:

https://www.bsi.bund.de/SiteGlobals/Forms/IT-Sicherheitskennzeichen/IT-Sicherheitskennzeichen_Formular.html?cl2Categories_Produkttyp=e-mail-dienste

Cyber Resilience Act: Europäischer Gesetzesvorschlag für mehr Sicherheit in digitalen Produkten

Im September letzten Jahres veröffentlichte die Europäische Kommission den Entwurf für den geplanten Cyber Resilience Act. Das BSI als die Cyber-Sicherheitsbehörde Deutschlands unterstützt mit seiner Expertise die Ausgestaltung des europäischen Rechtsakts und lud hierzu bereits zu einem ersten „BSI im Dialog“ ein.

von Lena Schnepper und Patrick Seidel, Referat Fachgremienarbeit für Prüf- und Zertifizierungsverfahren, Qualitätsmanagement

Im Herbst vergangenen Jahres hat die Europäische Kommission den Entwurf für einen sogenannten Cyber Resilience Act (CRA) veröffentlicht (deutsch „Verordnung zur Cyber-Widerstandsfähigkeit“), den EU-Kommissionspräsidentin Ursula von der Leyen 2021 in ihrer Rede zur Lage der Europäischen Union angekündigt hatte. Der CRA soll den Zugang zu europäischen Märkten regeln und formuliert dafür verpflichtende Anforderungen an die Cyber-Sicherheit eines breiten Spektrums an Produkten mit digitalen Elementen. Die Verordnung nutzt das New Legislative Framework (NLF), das seit 2008 den Ordnungsrahmen für die europäische Produktregulierung bildet. Das NLF diente bislang vor allem dazu, die physische Produktsicherheit (englisch „safety“) zu regulieren. Mit dem CRA wird das Framework erstmals und vollumfänglich um einen die digitale Sicherheit adressierenden „Security“-Aspekt erweitert. Künftig müssen Herstellerinnen und Hersteller an Produkten mit digitalen Elementen das CE-Kennzeichen anbringen, das die Prüfung des Produkts dokumentiert und die Erfüllung der grundlegenden Cyber-Sicherheitsanforderungen des CRA bescheinigt.

UNTERSCHIEDLICHE PRODUKTKLASSEN – ABGESTUFTE PRÜFUNGEN

Dem aktuellen Entwurf zufolge benötigen unkritische Produkte mindestens eine Selbstbewertung durch die Herstellerin oder den Hersteller. Produkte der Klasse „Kritisch I“ können einer Selbstbewertung nach einer harmonisierten europäischen Norm (hEN) unterzogen werden. Für die Klasse „Kritisch I“ sind beispielsweise Passwort-Manager oder Router für den Privatgebrauch vorgesehen. Sollte für ein Produkt dieser Klasse keine hEN vorliegen, so muss das Produkt eine unabhängige Konformitätsprüfung durch eine notifizierte Drittstelle durchlaufen. Für Produkte, die in die Klasse „Kritisch II“ fallen, wie u. a. Router für den industriellen Gebrauch oder Chipkartenleser, ist eine solche Konformitätsprüfung immer vorgeschrieben. Die Europäische Kommission behält sich vor, durch einen Delegierten Rechtsakt zusätzlich die Risikoklasse „Hochkritisch“ einzuführen. Produkte dieser Klasse müssen nach einem Zertifizierungsschema des Cyber Security Acts (CSA) zertifiziert werden. Damit auch bei den anderen Klassen eine bessere Durchlässigkeit zwischen CRA und CSA gewährleistet ist und standardisierte Prüfvorgaben bereitgestellt werden können, sollte die Konformitätsvermutung für CSA-Zertifizierungsschemata automatisch gelten.

Gleichzeitig wird bereits eine Prüfinfrastruktur unter dem CSA aufgebaut, auf die der CRA gezielt zurückgreifen sollte, um Mehrkosten und Bürokratieaufwände zu vermeiden. Damit würde auch die ausreichende Verfügbarkeit von Konformitätsbewertungsstellen für die benötigten unabhängigen Drittstellenbewertungen bei Inkrafttreten des CRA sichergestellt.

Weitere Informationen:

https://digital-strategy.ec.europa.eu/de/library/cyber-resilience-act

https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/Cyber-Security-Act/cyber-security-act_node.html

Konstruktiver Austausch bei „BSI im Dialog“: Die Teilnehmenden setzten sich mit offenen Fragen zum Vorschlag des CRA auseinander und diskutierten u. a. über die Schnelligkeit bei der Entwicklung von Standards sowie den Ausbau von benötigten technischen Kompetenzen.

BSI im Dialog

Weitere Informationen zu unseren Dialog-Veranstaltungen:

https://www.bsi.bund.de/DE/Service-Navi/Veranstaltungen/BSI-im-Dialog/bsi-im-dialog.html

BSI IM DIALOG: AUSTAUSCH MIT NATIONALEN STAKEHOLDERN

Am 28. November 2022 fand in Berlin die Veranstaltung „BSI im Dialog: Cyber Resilience Act – ein Schritt auf dem Weg zu mehr Cyber-Sicherheit in Europa?“ statt, an der Vertreterinnen und Vertreter aus Industrie, Politik und Zivilgesellschaft teilnahmen. Ziel dieser Veranstaltung war es, mit nationalen Stakeholdern in einen ersten Dialog hinsichtlich des CRA-Entwurfs zu treten. Die Veranstaltung wurde von dem Abteilungsleiter der Abteilung SZ (Standardisierung und Zertifizierung) des BSI, Sandro Amendola, eröffnet. Danach hielt Maika Föhrenbach, Vertreterin der EU-Kommission, eine Präsentation, die die wesentlichen Inhalte des CRA skizzierte. Anschließend präsentierte das BSI Impulse zum Thema Digitaler Verbraucherschutz und SBoM (Software Bill of Materials) im CRA.

Nach den Vorträgen fand eine Paneldiskussion statt. Von den Teilnehmenden wurde der CRA-Entwurf insgesamt begrüßt. So hat der CRA das Potenzial, internationaler Maßstab für Cyber-Sicherheitsregulierungen zu werden und damit nicht nur Verbraucherinnen und Verbraucher vor unsicheren Produkten zu schützen, sondern auch einen Beitrag für resiliente Infrastrukturen zu leisten. Nichtsdestotrotz gäbe es noch offene Fragen und Anpassungsbedarf, insbesondere im Hinblick auf das effektive Zusammenspiel mit anderen bereits existierenden Regulierungen wie z. B. dem CSA oder dem Delegierten Rechtsakt der Radio Equipment Directive. Dennis Kügler, Fachbereichsleiter von SZ 1 im BSI, unterstrich, dass das BSI als die nationale Behörde für Cyber-Sicherheit mit seiner Expertise die Ausgestaltung des CRA begleitet. ■

Das fehlende Puzzleteil für Cyber-Sicherheit

Maika Föhrenbach und Benjamin Bögel arbeiten bei der EU-Kommission in Brüssel in der Unit Cybersecurity and Digital Privacy Policy (CNECT.H.2) und befassen sich intensiv mit dem Cyber Resilience Act. Im Interview mit dem BSI-Magazin geben sie einen Einblick in den europäischen Prozess zur Stärkung der Cyber-Resilienz.

Cyber-Sicherheit ist auf der europäischen Ebene ein wichtiges Thema, an dem die EU-Kommission mit dem Cyber Resilience Act (CRA) arbeitet. Können Sie in wenigen Sätzen erläutern, um was es sich beim CRA handelt?

Maika Föhrenbach: Der Cyber Resilience Act ist das fehlende Puzzleteil im europäischen Rechtsrahmen für Cyber-Sicherheit. Die im Januar in Kraft getretene NIS-2-Richtlinie verpflichtet die Mitgliedstaaten, dafür zu sorgen, dass kritische Infrastrukturen und andere wichtige Unternehmen ihre Netzwerke sicherer machen. Allerdings können die Netwerke nur so sicher sein wie die Hard- und Software, die darin zum Einsatz kommt. Gleiches gilt für Verbraucherinnen und Verbraucher, deren Sicherheit entscheidend von der Sicherheit der verwendeten Produkte abhängt. Hier kommt der CRA ins Spiel.

Welches Ziel verfolgt die EU-Kommission mit dem CRA?

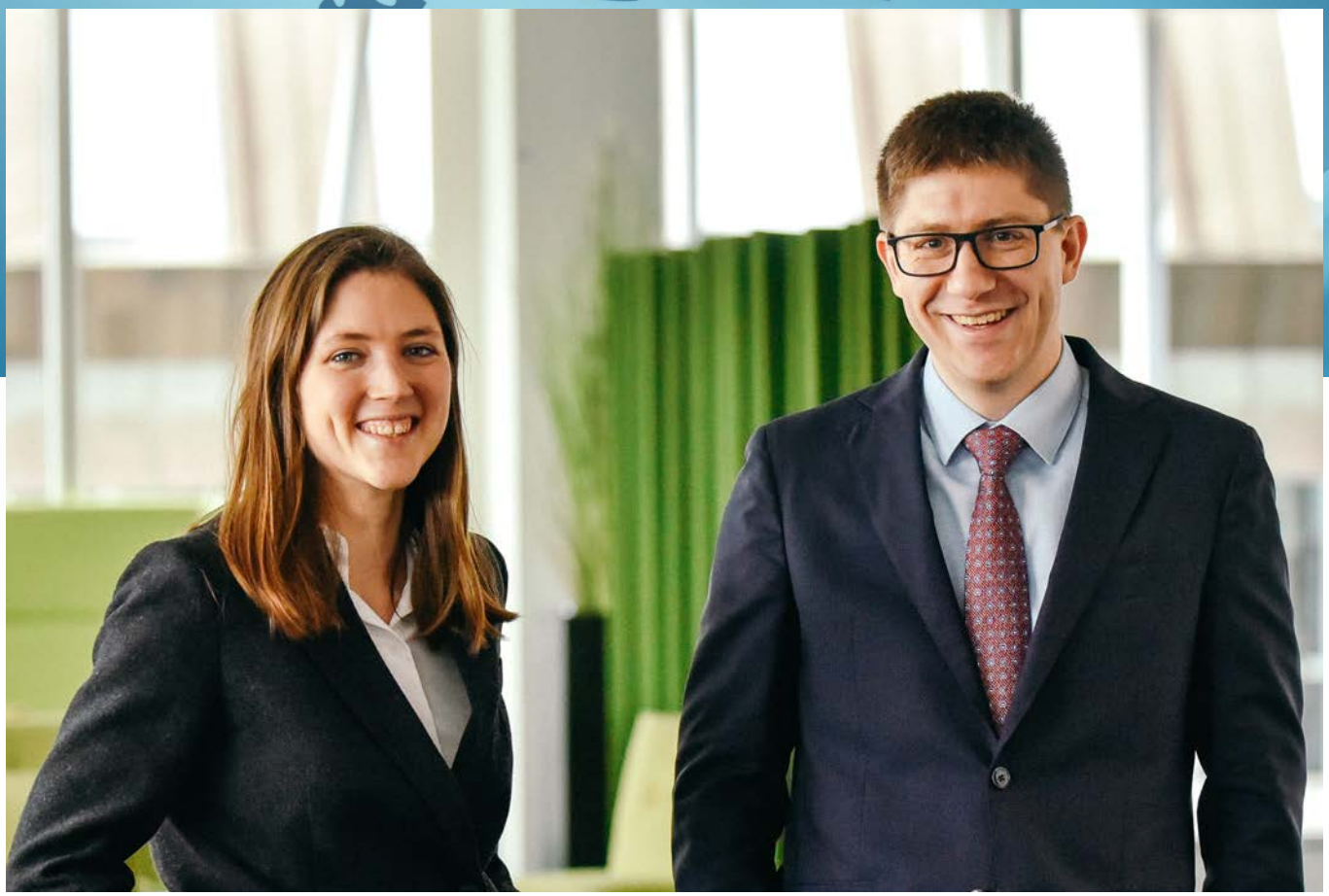
Benjamin Bögel: Leider ist es um die Sicherheit von Hard- und Software-Produkten eher schlecht bestellt. Bei zwei Dritteln aller Cyber-Sicherheitsvorfälle im Bereich kritischer Infrastrukturen nutzen Angreifer Schwachstellen in Software aus. Obwohl die Hersteller seit vielen Jahren um diese Probleme wissen, haben sie die Sicherheit ihrer Produkte nicht wesentlich verbessert. Der CRA verpflichtet daher Hersteller von Hard- und Software, künftig die Produktsicherheit bei der Entwicklung von Anfang an mitzudenken und über den gesamten Lebenszyklus ernst zu nehmen. Insbesondere wollen wir erreichen, dass Nutzer auch nach dem Kauf noch einen Rechtsanspruch auf Sicherheitsupdates haben.

Mit dem Cyber Security Act wurden bereits gewisse Strukturen aufgebaut, beispielsweise eine Marktüberwachung und Konformitätsbewertungsstellen. Zeitgleich finden bereits Standardisierungsaktivitäten auf Grundlage des Delegierten Rechtsakts der Funkanlagenrichtlinie statt. Inwieweit fügt sich der CRA in dieses regulatorische Gefüge ein und kann von den geleisteten Vorarbeiten profitieren?

Maika Föhrenbach: Mit dem Cyber Security Act wurde im Jahr 2019 ein Rahmen zur freiwilligen Zertifizierung der Sicherheit von Produkten, Diensten und Prozessen entwickelt. Der CRA ergänzt das nun um einen verbindlichen Anforderungskatalog. Bestehende Zertifizierungen können dabei übernommen werden. Der Delegierte Rechtsakt der Funkanlagenrichtlinie verfolgt dasselbe Ziel wie der CRA, hat aber einen wesentlich engeren Anwendungsbereich, der insbesondere Software nicht erfasst. Die Standards, die dafür entwickelt werden, sind eine wichtige Grundlage für künftige CRA-Standards.

In dieser Ausgabe des BSI-Magazins steht der Digitale Verbraucherschutz (DVS) im Vordergrund. Wie wirkt sich der CRA auf den Verbraucherschutz aus?

Benjamin Bögel: Verbraucherinnen und Verbraucher werden anhand des ihnen bereits vertrauten CE-Kennzeichens erkennen können, dass ein Produkt wesentlichen Cyber-Sicherheitsanforderungen genügt. Transparenzvorschriften und ein Label speziell für Cyber-Sicherheit sollen ihnen zusätzlich bei ihren Kaufentscheidungen helfen. Außerdem können sie darauf vertrauen, dass der Hersteller sie auch nach dem Kauf nicht im Regen stehen lässt, sondern weiterhin die Sicherheit der erworbenen Produkte verbessert. Dazu müssen die Hersteller klipp und klar kennzeichnen, über wie viele Jahre die Nutzer mit Sicherheitsupdates rechnen können.



Wie ist der aktuelle Status beim CRA? Maika Föhrenbach und Benjamin Bögel von der EU-Kommission begleiten den Prozess von Brüssel aus.

Welche anderen Stakeholder – auch das BSI ist am Prozess beteiligt – bringen sich in die Ausgestaltung des CRA ein? Wie läuft ein so komplexes Vorhaben auf europäischer Ebene ab?

Maika Föhrenbach: Vergangenes Jahr hat die Kommission online eine öffentliche Konsultation durchgeführt, an der sowohl Bürgerinnen und Bürger als auch Unternehmen teilnehmen konnten. Insbesondere die nationalen Cyber-Sicherheitsbehörden wie das BSI waren in die Vorbereitungen eingebunden. Nachdem die Kommission am 15. September 2022 ihren Vorschlag für den CRA vorgelegt hat, sind jetzt die Mitgliedstaaten und das Europäische Parlament am Zug. Sie müssen sich auf einen gemeinsamen Text einigen. Spätestens nach Inkrafttreten wird die Kommission die europäischen Normungsorganisationen damit beauftragen, europäische Standards zu entwickeln. Dort können dann die Hersteller ihre Fachexpertise einbringen. Die Vorbereitungen dafür laufen bereits jetzt auf Hochtouren.

Welche positiven Auswirkungen erwarten Sie als Fachleute, aber auch als Verbraucher von der Umsetzung des CRA?

Benjamin Bögel: Europa ist einer der wichtigsten Absatzmärkte für Hard- und Software. Der CRA ist daher eine große Chance für die europäischen Hersteller, weil er das Zeug hat, einen globalen Standard zu setzen. Anwender, egal ob Unternehmen oder Verbraucherinnen und Verbraucher, werden von einem höheren Sicherheitsniveau profitieren. Nationale Marktüberwachungsbehörden werden die Einhaltung der Regeln sicherstellen. Als Verbraucher freue ich mich darauf, dass ich aufgrund der neuen Transparenzregeln in Zukunft bei meiner Kaufentscheidung neben den Produktfeatures viel stärker auch Cyber-Sicherheitsmerkmale berücksichtigen kann. ■

Weitere Informationen:

https://www.bsi.bund.de/dok/ncca

Hochrangiges Treffen der europäischen Cyber-Sicherheits-behörden in München

Auf Initiative und Einladung des BSI tauschen sich die Leitungen von Europas Cyber-Sicherheitsbehörden im Vorfeld der Münchner Sicherheitskonferenz aus.

von Clarissa Wilkie, Referat Internationale Beziehungen

Am Vortag der Münchner Sicherheitskonferenz 2023, die vom 17. bis zum 19. Februar 2023 stattgefunden hat, kamen zum dritten Mal zahlreiche Direktorinnen und Direktoren der für Cyber-Sicherheit zuständigen Behörden aus ganz Europa zusammen, um sich auf Leitungsebene über die aktuellen nationalen und europäischen Herausforderungen der Cyber-Sicherheit auszutauschen. Gastgeber und Moderator der Veranstaltung war BSI-Vizepräsident Dr. Gerhard Schabhüser.

Der Veranstaltungsort des Treffens war der Bayerische Hof in München, der gleichzeitig Austragungsort der Münchner Sicherheitskonferenz (MSC) ist, dem weltweit wichtigsten sicherheitspolitischen Expertentreffen. Dass die Veranstaltung des BSI in Zusammenarbeit mit der MSC organisiert wurde, unterstreicht die internationale politische Bedeutung, die die Cyber-Sicherheit inzwischen erlangt hat.

Dieser Bedeutung werden auch das BSI und seine europäischen Partnerbehörden in ihrer Arbeit gerecht. Informationssicherheit als Voraussetzung einer erfolgreichen Digitalisierung endet schließlich nicht an Landesgrenzen. Angesichts der grenzübergreifenden IT-Gefährdungslage und der Herausforderungen der Digitalisierung bietet das Treffen die einzigartige Möglichkeit, abseits des Tagesgeschäfts strategisch bedeutsame Themen zu diskutieren, die alle gleichermaßen betreffen.

ABWECHSLUNGSREICHES PROGRAMM ZUR FÖRDERUNG DES AUSTAUSCHS

Das Programm des Direktorentreffens besteht aus drei wichtigen Elementen. Zu Beginn präsentiert jedes Land in Kurzform ein sogenanntes National Update, das die wichtigsten staatlichen Entwicklungen hinsichtlich Cyber-Sicherheit beschreibt, z. B. im Bereich der Gesetzgebung, der Umsetzung von Cyber-Sicherheitsstrategien oder der Neugründungen von (operativen) „National Cyber Security Centres“. Anschließend folgt eine Diskussionsrunde, in der neben der Einschätzung der IT-Bedrohungslage vor allem auch strategische Handlungsmöglichkeiten für die Behörden erörtert werden, sowohl individuell als auch ganz besonders im Sinne der europäischen Zusammenarbeit und gegenseitigen Unterstützung. Im abschließenden Programmteil besteht für alle Teilnehmenden stets die Möglichkeit, sich außerhalb des Plenums in eigens dafür vorgesehenen Räumlichkeiten zu bilateralen Seitengesprächen zu verabreden – ein Angebot, das sich einer enorm hohen Nachfrage erfreut und damit die große Bedeutung einer vertrauensbildenden persönlichen Begegnung zeigt.

Linke Seite oben:
Das Hotel Bayerischer Hof München während der Sicherheitskonferenz
Bild rechts oben: 25 Direktorinnen und Direktoren folgten der Einladung des BSI
Bilder unten: Europäische Cyber-Sicherheitsbehörden an einem Tisch: BSI-Vizepräsident Dr. Gerhard Schabhüser moderierte als Gastgeber den intensiven Austausch

SCHAFFUNG EINES NEUEN, EXKLUSIVEN FORMATS

Mit dem „Cyber Security Directors' Meeting" – so der offizielle Veranstaltungstitel – hat das BSI im Jahr 2020 ein Format geschaffen, das es in dieser Form auf Ebene der europäischen Fachbehörden für Cyber-Sicherheit bislang noch nicht gab. Damit leistet das BSI auch einen wichtigen Beitrag zur besseren Vernetzung der Behörden, die jeweils in ihrem Land für das Thema federführend zuständig sind. An dem Treffen nehmen nicht nur Vertreterinnen und Vertreter aus den EU-Mitgliedstaaten teil, sondern auch aus den vier EFTA-Staaten, Island, Liechtenstein, Norwegen und der Schweiz, sowie aus dem Vereinigten Königreich und von der Agentur der Europäischen Union für Cybersicherheit (ENISA). ■

DAS INTERNATIONALE ENGAGEMENT DES BSI

Die internationale Zusammenarbeit ist für das BSI seit seiner Gründung vor über 30 Jahren ein essenzieller Faktor zur Verbesserung der Cyber-Sicherheit.

Ziel des BSI ist, neben seiner nationalen Rolle als Cyber-Sicherheitsbehörde des Bundes, Cyber-Sicherheit auch international mitzugestalten sowie die eigene technologische Beurteilungsfähigkeit zu stärken. Um seiner Verantwortung dafür angemessen nachzukommen, intensiviert und erweitert das BSI kontinuierlich seine Beziehungen mit Behörden, Organisationen, Unternehmen sowie Akteuren der Wissenschaft und Zivilgesellschaft weltweit.

Die Arbeit in diversen Fachgremien zur Informations- und Cyber-Sicherheit im EU-, NATO- und internationalen Kontext ist dabei wesentlicher Bestandteil des internationalen Engagements des BSI.

Cyber-Sicherheit im Gesundheitswesen

Wie das BSI die Digitalisierung in der Arztpraxis stärkt

Die Corona-Pandemie hat verdeutlicht, wie hilfreich Apps und andere digitale Anwendungen sein können. Die Kontaktnachverfolgung infizierter Personen ließ sich beschleunigen und konnte so einen elementaren Beitrag in der gemeinschaftlichen Pandemiebekämpfung leisten.

von Pascal Jeschke und Kristina Ernst, Referat Cyber-Sicherheit im Gesundheits- und Finanzwesen

Das deutsche Gesundheitswesen erschließt die digitalen Potenziale ebenfalls, so dass die Digitalisierung den Versorgungsalltag zunehmend prägt. Wie auch in anderen Digitalisierungsfeldern legt die Cyber-Sicherheit hierbei den notwendigen Grundstein für eine gelingende Digitalisierung in Deutschland. Ein sorgfältiger Umgang mit Gesundheitsdaten ist jederzeit geboten, da eine Veröffentlichung immensen gesellschaftlichen Schaden für die betroffene Person bedeuten und eine Manipulation der Daten das leibliche Wohl gefährden kann. Als die Cyber-Sicherheitsbehörde des Bundes betrachtet das BSI die Digitalisierung im Gesundheitswesen und beschreibt aktuelle Aufgaben und Herausforderungen erstmalig im veröffentlichten Lagebild Gesundheit 2022.

WEITERENTWICKLUNG DER TELEMATIKINFRASTRUKTUR

Ein zentraler Baustein des digitalen Gesundheitswesens ist die Telematikinfrastruktur (TI). Das von der gematik GmbH konzipierte Gesundheitsnetz mit seinen unterschiedlichen Anwendungen stellt die Grundlage für den sicheren Austausch von Gesundheitsdaten zwischen Leistungserbringern dar. Das bestehende Netz wird stetig erweitert, so dass beispielsweise die elektronische Patientenakte und das elektronische Rezept neuere Anwendungen sind. Das BSI begleitet die Entwicklungen solcher Anwendungen, damit sich die notwendigen Sicherheitsstandards frühestmöglich etablieren lassen.

Sicherheitssäulen der TI 2.0

Quelle: BSI

Ein großes Vorhaben der kommenden Jahre befasst sich mit dem konzeptionellen Neuaufbau des Gesundheitsnetzes. Derzeit wird der Zugriff auf das Gesundheitsnetzwerk durch den Konnektor, einen Router in der jeweiligen Praxis, beschränkt. Zukünftig soll der Zugriff auch aus mobilen Versorgungssituationen, beispielsweise Hausbesuchen, heraus ermöglicht werden. Doch dafür bedarf es einer Neuarchitektur des Netzes. Die gematik GmbH und das BSI vereinbarten frühzeitig elementare Sicherheitseigenschaften der Weiterentwicklung der TI zur TI 2.0. Eine ausführlichere Betrachtung der Weiterentwicklung der TI zur TI 2.0 finden Sie im Lagebild Gesundheit 2022.

CYBER-SICHERHEIT VOR ORT

Die Cyber-Sicherheit des derzeitigen zentralen Gesundheitsnetzes und dessen Weiterentwicklung sind unerlässlich. Bei einer ganzheitlichen Betrachtung der Cyber-Sicherheit in der ambulanten Versorgung müssen Maßnahmen zur Sicherung des Netzes um angemessene Sicherheitsvorkehrungen in den Praxen erweitert werden. Denn die Sicherheitsvorkehrungen des Netzes können keine vollumfängliche Sicherheit in der jeweiligen Praxis garantieren. Daher ist die Erstellung und Evaluierung der IT-Sicherheitsrichtlinie gem. § 75b SGB V zusammen mit der Kassenärztlichen Bundesvereinigung und der Kassenzahnärztlichen Bundesvereinigung eine spezialgesetzliche Aufgabe im Gesundheitswesen. Die Richtlinie definiert Maßnahmen für den Praxisalltag, so beispielsweise den sicheren Umgang mit Speichermedien oder den Bezug von Apps, und wurde 2020 veröffentlicht. 2022 hat das BSI eine Handreichung für Leistungserbringer veröffentlicht, die die Sicherheitsrichtlinie ergänzt.

Dies bietet den Anlass, die derzeitige IT-Sicherheit in den Arztpraxen verstärkt zu betrachten. Das BSI führt zu diesem Zweck 2023 drei Projekte durch.

Das Projekt Cyber-Sicherheit in Arztpraxen (CyberPraxMed) betrachtet das Netzwerk in Arztpraxen und die Einbindung medizinischer Geräte in das Praxisnetzwerk. Ergänzend zu der Erhebung der Sicherheit in den Praxen widmet sich das andere Projekt Sicherheit von Praxisverwaltungssystemen (SiPRa) der Cyber-Sicherheit der essenziellen Praxisverwaltungssoftware. Diese beiden Projekte werden durch eine 2023 begonnene Umfrage im Projekt Evaluierung der IT-Sicherheitsrichtlinie in Arztpraxen (SiRiPrax) ergänzt. Hierbei werden Leistungserbringer gezielt hinsichtlich der Umsetzung der IT-Sicherheitsrichtlinie gem. § 75b SGB V und möglicher Umsetzungsschwierigkeiten befragt. Die Ergebnisse aus diesen unterschiedlichen Projekten ermöglichen es dem BSI, gezielt die Cyber-Sicherheit in Arztpraxen durch entsprechende Empfehlungen oder Vorgaben zu verbessern und somit einen essenziellen Beitrag in diesem Themengebiet zu leisten. ■

Weitere Informationen:

Lagebild Gesundheit 2022
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Lagebild_Gesundheit_2022.html

Handreichung § 75b SGB V:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/E-Health/Hinweise-IT-Sicherheitsrichtlinie-SGB/Hinweise_IT-Sicherheitsrichtlinie-SGB_node.html

BSI gestaltet internationale Standards

Digitale Siegel machen hoheitliche Papierdokumente fälschungssicher

von Dr. Guido Frank und Nicolas Thenée, Referat eID-Strukturen für die Digitalisierung

2022 wurden in Europa die ersten Schengen-Visa mit digitalen Siegeln ausgegeben. In Hamburg startete die Wohnsitz-Ummeldung via Online-Ausweisfunktion, bei der die Adressänderungsaufkleber fälschungssicher mit digitalem Siegel abgesichert sind. Damit findet der Einsatz kryptografisch signierter 2D-Barcodes auf hoheitlichen Dokumenten immer weitere Anwendungsfelder. Durch die internationale Standardisierung des vom BSI entwickelten JAB-Codes ist es zudem möglich, die Datenkapazität noch einmal deutlich zu erhöhen.

Während die Integrität elektronischer Ausweisdokumente heute mit kryptografischen Mechanismen wie digitalen Signaturen abgesichert ist, gibt es weiterhin Bedarf an hoheitlichen Papierdokumenten. Dabei ist die Nutzung eines speziellen Sicherheitspapiers häufig allerdings nicht mehr ausreichend, um Fälschungen zu verhindern.

Mit der Technischen Richtlinie BSI TR-03137-1 hat das BSI den Grundstein für die kryptografische Absicherung von hoheitlichen Papierdokumenten gelegt. Die Technische Richtlinie (TR) definiert ein optisch verifizierbares digitales Siegel, welches in Form eines digital signierten zweidimensionalen Barcodes (DataMatrix) auf dem Dokument aufgebracht wird und dadurch die Prüfung der Echtheit und Unversehrtheit der aufgedruckten Daten ermöglicht. Die TR spezifiziert den Aufbau und die Nutzung digitaler Siegel im Kontext hoheitlicher Dokumente.

Die im Siegel codierten Daten werden mit dem privaten Schlüssel des Dokumentenherstellers über ein Online-Personalisierungssystem signiert und können mit einem entsprechenden Lesegerät (etwa ein Smartphone mit passender App, wie z.B. die prototypische App SealVa für Android) einfach verifiziert werden. Bei einer ungültigen Signatur ist von einer Fälschung auszugehen. Bei einer erfolgreichen Signaturprüfung müssen die im Siegel enthaltenen Daten noch mit denen des Aufdrucks abgeglichen werden, um sicherzustellen, dass das Dokument nicht manipuliert wurde.

Als Infrastruktur für die Verifikation der digitalen Siegel dienen im Hintergrund bewährte Systeme, die bereits für elektronische Reisepässe und eID-Dokumente eingesetzt werden. Das BSI betreibt die „Nationale Wurzelzertifizierungsstelle“ für hoheitliche Dokumente und stellt die benötigten Zertifikate für den Dokumentenhersteller aus.

ANWENDUNGEN DES DIGITALEN SIEGELS

Die erste Anwendung fand das digitale Siegel im Rahmen der Flüchtlingssituation 2015 mit dem Ankunftsnachweis für Asylsuchende. Dieser half dabei, die Identifizierung von Asylsuchenden zu verbessern und so die Asylverfahren in Deutschland zu beschleunigen.

Danach wurde die TR des BSI in die Standards für maschinenlesbare Reisedokumente (Doc 9303 Serie) der ICAO überführt. Damit ist nun auch die länderübergreifende Nutzung der digitalen Siegel möglich. Auf Basis einer Entscheidung der EU-Kommission schützt das Siegel seit 2022 auch ausgestellte Visa in Europa vor Fälschungen und erhöht damit die Sicherheit der Grenzkontrolle.

Muster eines Visa-Stickers mit digitalem Siegel

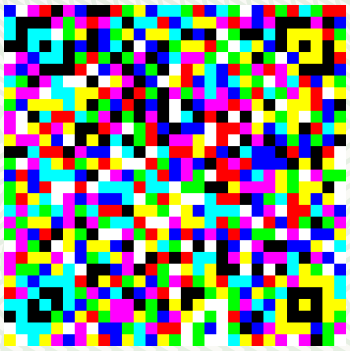
Auch auf nationaler Ebene spielt die TR-03137-1 eine wichtige Rolle. Die in Hamburg gestartete Online-Ummeldung ermöglicht über die Online-Ausweisfunktion des Personalausweises die Ummeldung von zu Hause aus. Niemand muss dafür mehr beim Amt erscheinen. Dabei werden nicht nur die Adressdaten auf dem Chip geändert, sondern – über einen digital gesiegelten Adressaufkleber – auch die auf dem Ausweis aufgedruckte Adresse. Der Aufkleber erreicht die Antragstellenden auf dem Postweg.

IN FARBE: PLATZSPARENDER JAB-CODE

Die Integration von digitalen Siegeln auf hoheitlichen Dokumenten stellt Behörden vor die Herausforderung, dass aus Platzgründen nur eine sehr kleine Fläche für den Druck zur Verfügung steht, wodurch die Speicherkapazität meist stark eingeschränkt ist und nicht alle aufgedruckten Merkmale (darunter das Gesichtsbild) im Barcode codiert werden können.

Um dieses Problem zu lösen, hat das BSI in Zusammenarbeit mit dem Fraunhofer SIT den farbigen JAB-Code entwickelt und diesen in die Standardisierung eingebracht. Seit April 2022 steht der JAB-Code als internationaler Standard ISO/IEC 23634 zur Verfügung. Durch die verwendeten Farben kann eine wesentlich höhere Datendichte erzielt werden. So lassen sich bei gleicher Größe wesentlich mehr Daten speichern.

So könnte es mit dem JAB-Code künftig möglich sein, unter geeigneten Rahmenbedingungen alle aufgedruckten Daten im Barcode abzusichern und so die Fälschungssicherheit auf ein neues Niveau zu heben. ■



Beispieldarstellung eines JAB-Codes mit Visa-Profil, Referenz BSI TR-03137

Weitere Informationen:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03137/tr03137_node.html

BSI-Basis-Tipp

Schritt für Schritt zur Datensicherung

Geht das Smartphone verloren oder stellt der Computer den Dienst ein, ist guter Rat schnell teuer. Einfache Sicherungskopien können helfen.

Dem Digitalbarometer 2022 des BSI und der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) zufolge legen 26 Prozent der Befragten regelmäßig Sicherheitskopien ihrer Daten an, um sich vor Datenverlust zu schützen. Das bedeutet auch, dass etwa drei Viertel der Befragten keine Sicherungen erstellen – oder nur unregelmäßig. Dabei gehören Datensicherungen zu den wichtigsten Werkzeugen, um Fotos, Dokumente oder ganze Systeme vor Gefahren abzuschirmen. Denn haben Cyber-Kriminelle beispielsweise Ihre Festplatte verschlüsselt, wurde Ihr Handy gestohlen oder ist der Laptop nass geworden, sind Sicherungskopien oft die letzte Rettung. Mit ihrer Hilfe können wichtige Daten wiederhergestellt werden, so dass sich solche Notfälle gelassener hinnehmen lassen. Betroffene können die Datensicherung einspielen und den Vorfall abhaken.

WANN SIND SICHERHEITSKOPIEN DIE RETTUNG?

Defekt des Gerätes

versehentliche Löschungen

verschiedene Schadprogramme

Gerätediebstahl

Naturkatastrophen oder Gebäudeschäden

Probleme mit dem Cloud-Service

Eine Datensicherung erstellen

Windows 10 & 11

1) Klicken Sie auf das Windows-Suchfeld oder die Lupe auf der Taskleiste.
2) Dort tippen Sie „Systemsteuerung“ ein und klicken auf den gleichnamigen Eintrag.
3) Wählen Sie anschließend unter „System und Sicherheit“ den Menüpunkt „Sichern und Wiederherstellen (Windows 7)“.
4) Dort angekommen wählen Sie „Sicherung einrichten“.

Scannen Sie den QR-Code, um die vollständige Anleitung zu erhalten.

macOS

1) Am oberen Bildschirmrand finden Sie ein kleines Apple-Logo. Klicken Sie darauf, können Sie die „Systemeinstellungen“ auswählen. Unter dem Reiter „Allgemein“ wählen Sie den Eintrag „Time Machine“.

Scannen Sie den QR-Code, um die vollständige Anleitung zu erhalten.

Apple iOS & iPadOS

Der Apple-Dienst „iCloud“ ist in der Basis zwar kostenlos, dabei ist aber die Speicherkapazität eingeschränkt. Damit kann dieser Sicherungsweg dazu führen, dass Sie ein kostenpflichtiges Abonnement benötigen. Alternativ können Sie Sicherungskopien Ihres Geräts kostenlos, z. B. per iTunes, am Computer erstellen.

Scannen Sie den QR-Code und lesen Sie, wie eine Datensicherung am PC oder Mac funktioniert.

1) Öffnen Sie die Einstellungen des iPhone oder des iPad.
2) Klicken Sie auf Ihre Apple-ID und anschließend auf „iCloud“.
3) Unter dem Menüpunkt „iCloud-Backup“ lässt sich die Option „Backup dieses iPhone erstellen“ aktivieren. Das Gerät erstellt dann in regelmäßigen Abständen aktuelle Sicherheitskopien des Betriebssystems und der persönlichen Daten, die es in die Apple-Cloud hochlädt.

Android

Da zahlreiche Versionen von Android auf unterschiedlichsten Geräten im Umlauf sind, kann es sein, dass die folgende Anleitung nicht genau Ihrem System entspricht. Dabei ist die Methode grundsätzlich in den meisten Android-Varianten sehr ähnlich.

Zusätzlich bieten die Hersteller der Geräte für die Sicherung der Daten oft eigene Dienste an, die möglicherweise besser zu Ihren jeweiligen Anforderungen passen oder weitere Funktionen bieten. Informationen dazu finden Sie auf den Webseiten der Diensteanbieter.

1) Wählen Sie unter „Einstellungen“ den Punkt „System“. Es kann je nach Gerät sein, dass sich die Funktion hinter „Zusätzliche Einstellungen“ oder „Erweiterte Einstellungen“ verbirgt. Dort findet sich der Punkt „Konten und Sicherung“ oder „Sicherung“.
2) Im Folgenden klicken Sie dann auf einen Button, der mit „Aktivieren“ oder „Jetzt sichern“ betitelt ist.
3) Wählen Sie das Sicherungskonto aus sowie die Daten, die gesichert werden sollen.
4) Jetzt erstellt das Gerät in regelmäßigen Abständen aktuelle Sicherheitskopien des Betriebssystems, der ausgewählten Daten und Einstellungen und lädt diese in die Cloud hoch.

Wenn Sie nur einzelne Daten, wie Fotos oder Videos, ohne Rückgriff auf einen Cloud-Dienst sichern möchten, geht das bequem am Computer, indem Sie das Gerät per USB-Kabel mit dem PC verbinden. Das Smartphone oder Tablet wird dort wie ein externes Laufwerk behandelt, so dass Sie Daten manuell kopieren können. Für vollständige Datensicherungen Ihres Android-Geräts am Computer oder erweiterte Funktionen benötigen Sie in der Regel zusätzliche Software.

Linux/Ubuntu

Wenn Sie ein Linux-Betriebssystem verwenden, gibt es mehrere Möglichkeiten, Ihre Daten zu sichern. Timeshift oder rsync beispielsweise bieten komfortable Lösungen zur Sicherung einzelner Verzeichnisse oder ganzer Laufwerke. Da die Sicherungsmethode aber stark vom verwendeten Programm abhängt, empfehlen wir, die verfügbaren Linux-Leitfäden zu nutzen. Hier finden Sie eine beispielhafte Anleitung, um eine Datensicherung unter Ubuntu anzulegen. Unter Ubuntu ist das Programm für Datensicherungen „Déjà Dup“ vorinstalliert. Bei vielen Distributionen lässt sich das Tool mittels „sudo apt-get install Déjà Dup“ installieren.

1) Unter Ihren Anwendungen finden Sie das Programm „Datensicherungen“. Falls nicht, können Sie über die Suchfunktion nach „Datensicherungen“ oder „Déjà Dup“ suchen.
2) Haben Sie das Programm geöffnet, entdecken Sie im Reiter „Übersicht“ die Möglichkeit, automatische Datensicherungen zu aktivieren.

Scannen Sie den QR-Code, um die vollständige Anleitung zu erhalten.

Sollten diese Anleitungen nicht zu Ihrem Gerät, Ihrem Betriebssystem oder zu Ihrem individuellen Problem passen, empfehlen wir, dass Sie beim jeweiligen Hersteller oder Anbieter nachschauen, um dort möglicherweise eine noch spezifischere Hilfestellung zu finden.

Weitere Informationen:

Back-up – Doppelt gesichert hält besser:
https://www.bsi.bund.de/dok/10655274

Datenverlust – wie schütze ich mich:
https://www.bsi.bund.de/dok/6598916

Bestellen Sie Ihr BSI-Magazin!

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Referat Öffentlichkeitsarbeit

Postfach 20 03 63
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, Hausnr.

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 20 03 63, 53133 Bonn. Die von Ihnen angegebenen Daten werden ausschließlich für die Verwaltung des Versands bzw. die Übermittlung der Informationen verwendet, 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/DE/Service/Datenschutz/datenschutz_node.html

Impressum

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI) 53175 Bonn
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik 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:	Juli 2023
Redaktion:	Katrin Alberts, Sonia Golás, Brigitte Hoffmann, Mark Schulz, Bundesamt für Sicherheit in der Informationstechnik; Faktor 3 AG, Kattunbleiche 35, 22041 Hamburg, www.faktor3.de
Konzept und Gestaltung:	Bundesamt für Sicherheit in der Informationstechnik
Druck:	Appel und Klinger Druck & Medien GmbH Bahnhofstraße 3 96277 Schneckenlohe www.ak-druck-medien.de
Artikelnummer:	BSI-Mag23/717-1
Bildnachweise:	Titel: AdobeStock © Worawut; Seite 3: © bundesfoto.de/Uwe Völkner; Seite 4 – 5 (von links nach rechts): AdobeStock © Malchev, AdobeStock © NicoElNino, AdobeStock © comicsans, AdobeStock © TJ Barnwell, MSC, Matthias Balk, AdobeStock © Deivison; Seite 6 – 7: AdobeStock © ArtemisDiana, AdobeStock © Gorodenkoff, BSI, BSI, AdobeStock © imageteam; Seite 8 – 9: AdobeStock © Malchev; Seite 10: © Peter Jülich; Seite 11: BSI; Seite 12 – 13: Kombination aus AdobeStock © FotoBob und AdobeStock © Елена Бутусова; Seite 14 – 15: AdobeStock © Jackie Niam; Seite 16: AdobeStock © akhenatonimages; Seite 19: BSI; Seite 20: AdobeStock © Rido; Seite 21: BSI, BSI; Seite 22: AdobeStock © luismolinero; Seite 23: AdobeStock © denis_vermenko; Grafiken Seite 22 – 23: BSI; Seite 24 – 25: BSI / bundesfoto / Christina Czybik; Seite 26: AdobeStock © NDABCREATIVITY, AdobeStock © fotofabrika; Seite 27: AdobeStock © Drobot Dean, AdobeStock © Robert Kneschke; Seite 26 – 27 Illustration: AdobeStock © jozefmicic; Seite 29: AdobeStock © chinnarach, Icons und Montage: BSI; Seite 30 – 31: © bundesfoto.de/Uwe Völkner; Seite 32 – 33: AdobeStock © garrykillian; Seite 34: Hessisches Ministerium des Innern und für Sport; Seite 35: AdobeStock © NicoElNino; Seite 36 – 37, Illustration: AdobeStock © PureSolution, Portraitfotos: BSI und privat; Seite38 – 39: BSI / bundesfoto / Uwe Völkner; Seite 40 – 41: AdobeStock © ArtemisDiana, Diagramm: BSI; Seite 42 – 43: AdobeStock © comicsans, AdobeStock © TJ Barnwell; Seite 45: Adobe-Stock © contrastwerkstatt, AdobeStock © Robert Kneschke, AdobeStock © industrieblick, AdobeStock © deliris, AdobeStock © mariesacha, AdobeStock © Robert Kneschke; Seite 46 – 47: AdobeStock © Phruetthiphong; Seite 48 – 49: Kombination aus AdobeStock © ooddysmile, AdobeStock © BAIVECTOR und AdobeStock © bittedankeschön; Seite 49: BSI, BSI; Seite 50 – 51: AdobeStock © ooddysmile; Seite 51: AdobeStock © evgeniya, EU-Kommission; Seite 52 – 53: MSC, Matthias Balk; Seite 54: AdobeStock © anttoniart; Seite 56 – 57 (Hintergrund): AdobeStock © Rodin Anton; Seite 56: BSI; Seite 57: BSI, AdobeStock © Denys Rudyi; Seite 58: AdobeStock © Deivison, Icons: BSI; Seite 59: AdobeStock © Deivison; Seite 60: AdobeStock © Deivison

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

Follow us:

Lust auf Digitalisierung und Cyber-Sicherheit?

Übernehmt spannende Aufgaben und leistet einen wertvollen Beitrag für die sichere Digitalisierung in Deutschland – im #TeamBSI.

Bundesamt
für Sicherheit in der
Informationstechnik

Mehr Infos auf:

www.team-bsi.de