BSI-Magazin 2024/01

Mit Sicherheit

Im Blickpunkt:

Cybersicherheit

NIS-2 kommt – das bietet das BSI für Unternehmen

IT-Sicherheit in der Praxis

Mobiles Arbeiten auch in Zukunft sicher

Digitale Gesellschaft

Social Engineering: Schutz vor KI-gestützten Cyberangriffen

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Werde Teil der Cybernation Deutschlands.

Ihr wollt die sichere digitale Zukunft voranbringen und eure Expertise rund um Cybersicherheit einbringen? Dann kommt ins **#TeamBSI** und startet mit eurer Karriere voll durch.

Bundesamt
für Sicherheit in der
Informationstechnik

Mehr Infos auf:

www.team-bsi.de

Editorial

Liebe Leserin, lieber Leser,

Anfang des Jahres ging das neue Nationale IT-Lagezentrum in Bonn an den Start. Es ist das Herz unserer IT-Sicherheit, in dem Spezialistinnen und Spezialisten des BSI die Cybersicherheitslage in Deutschland rund um die Uhr im Blick behalten. Damit ist es uns gelungen, eine Infrastruktur zu schaffen, die wir für substanziell mehr Cybersicherheit in Deutschland brauchen. Es ist ein erster Schritt auf dem Weg zur Cybernation Deutschland.

Die „Cybernation Deutschland bauen" ist dabei unsere Antwort auf die aktuelle Bedrohungslage: Das Sicherheitsniveau der Digitalisierung in unserem Land muss erhöht werden – in staatlichen Institutionen, in Unternehmen und nicht zuletzt für jede und jeden Einzelnen. Gemeinsam sorgen wir dafür, dass Deutschland cyberresilient wird!

Wie kann uns das gelingen? Indem wir Cybersicherheit pragmatisch gestalten und messbar machen. Indem wir technologische Expertise gezielter nutzen und auch den Markt für Cybersicherheitsprodukte und Dienstleistungen stärken. Das Ziel ist ambitioniert, aber alternativlos. Denn es geht ums Ganze: Deutschland muss widerstandsfähig sein und bleiben, um Cyberbedrohungen abzuwehren. Gleichzeitig muss sichergestellt sein, dass Bürgerinnen und Bürger genauso wie Unternehmen und Behörden digitalen Technologien vertrauen können.

Das BSI engagiert sich auch auf europäischer Ebene für einen starken digitalen Verbraucherschutz. So haben wir im Februar dieses Jahres in Dresden das erste Europäische Symposium „Cybersecurity for Europe: Integrating the Consumer Perspective" organisiert. Das Symposium hat europäische Cybersicherheitsorganisationen an einen Tisch gebracht und sich als Plattform für Vernetzung, Austausch und Wissensvermittlung bewährt.

Außerdem blicken wir in dieser Ausgabe auf ein Jubiläum des Deutschen IT-Sicherheitskongresses: Zum 20. Mal brachte das BSI bei dem etablierten Forum für Cybersicherheit die Fachcommunity zusammen, die IT-Sicherheit am Puls der Zeit diskutierte. Anlässlich des Jubiläums rekapituliert der ehemalige BSI-Präsident Michael Hange im Interview die Anfangsjahre, als Ost- und Westdeutschland beim Schutz der IT-Infrastruktur zusammenwuchsen. Jubiläen feiern in diesem Jahr auch der IT-Grundschutz und CERT-Bund – diese und viele weitere spannende Themen haben wir in der aktuellen Ausgabe des BSI-Magazins zusammengestellt.

Ich wünsche eine anregende Lektüre!

Herzliche Grüße

Claudia Plattner
Präsidentin des Bundesamts für Sicherheit
in der Informationstechnik

Inhalt

IT-Sicherheit in der Praxis

BSI International

Digitale Gesellschaft

Digitaler Verbraucherschutz: BSI-Jahresrückblick 2023 erschienen

Anlässlich des Weltverbrauchertages am 15. März hat das BSI seinen Jahresrückblick 2023 im Bereich des Digitalen Verbraucherschutzes veröffentlicht. Darin werden unter anderem IT-Sicherheitsvorfälle und Trendthemen mit Bedrohungspotenzial aus dem Jahr 2023 näher beleuchtet. So zählten Datenleaks bei Unternehmen und öffentlichen Einrichtungen sowie Phishing-Angriffe auf Verbraucherinnen und Verbraucher zu den häufigsten Bedrohungen. Gleichzeitig sorgen neue Trends wie die Verbreitung von künstlicher Intelligenz für eine hohe Dynamik im digitalen Verbrauchermarkt. Die genannten Vorfälle verdeutlichen, dass der Schutz und die Widerstandsfähigkeit der Menschen bei ihren Aktivitäten im Netz dringend verbessert werden müssen. Der thematische Schwerpunkt der Jahrespublikation widmet sich daher der „Digitalen Verbraucherresilienz“. Im Mittelpunkt steht die Frage, was widerstandsfähige Verbraucherinnen und Verbraucher ausmacht, die dadurch besser in der Lage sind, sich vor Bedrohungen zu schützen, im Notfall schnell zu reagieren und Schäden zu minimieren.

Erste Digitalministerkonferenz: Claudia Plattner spricht über KI

Anlässlich der ersten Digitalkonferenz (DMK), die Bundesdigitalminister Dr. Volker Wissing und die Digitalverantwortlichen der Länder am 19. April 2024 ins Leben gerufen haben, um die digitale Transformation der Bundesrepublik Deutschland erfolgreich zu gestalten, sprach BSI-Präsidentin Claudia Plattner über Chancen und Risiken Künstlicher Intelligenz. KI ist eine Schlüsseltechnologie der Digitalisierung und birgt ein vielfältiges Nutzungspotential auch für die öffentliche Verwaltung. Stetig neue Angriffsvektoren auf KI-Systeme erfordern aber auch eine permanente Weiterentwicklung von Gegenmaßnahmen. Claudia Plattner würdigte die neue Digitalkonferenz: *„Im Namen des BSI gratuliere ich zur neu gegründeten DMK. Wir haben uns sehr gefreut, heute hier dabei sein zu dürfen; denn das zeigt uns, dass die Digitalverantwortlichen aus Bund und Ländern die Themen Digitalisierung und Cybersicherheit zusammendenken. Auch und gerade im Hinblick auf KI ist es von entscheidender Bedeutung, dass wir vorhandene Kompetenzen bündeln und eng, verstetigt und einheitlich zusammenarbeiten. Wir als BSI würden den Ländern gerne eine ganzheitliche Beratung zu allen Aspekten der IT-Sicherheit in Verbindung mit KI anbieten und unsere Informationen und Tools bereitstellen. Schon heute können wir in den gemeinsamen Erfahrungsaustausch gehen – diese Möglichkeit nehmen wir sehr gerne wahr.“*

Bundesdigitalminister Dr. Volker Wissing, HPI-Geschäftsführer Prof. Dr. Ralf Herbrich, die Digitalverantwortlichen der Länder und BSI-Präsidentin Claudia Plattner

V.l.: David Steinacker (GovTech Campus) und Thomas Caspers (BSI)

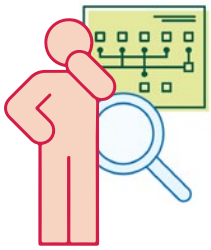
Zukunft der sicheren Cloud: BSI tritt GovTech Campus bei

Das BSI ist dem GovTech Campus in Berlin beigetreten. Dieser fördert die Kollaboration zwischen Verwaltung, Technologie-Szene, Unternehmen, Wissenschaft und Zivilgesellschaft. Im Verbund mit Projektpartnern arbeitet das BSI dort in einem Cloud-Reallabor daran, Public-Cloud-Dienste für die Bundesverwaltung und Betreiber Kritischer Infrastrukturen sicher nutzbar zu machen. Dabei geht es unter anderem darum, die Public Clouds großer Cloud-Serviceanbieter aus Deutschland und Europa und der sogenannten Hyperscaler aus den USA systematisch so zu erweitern, dass auch sensible und als Verschlusssachen eingestufte Daten sicher dort abgelegt und verarbeitet werden können. Thomas Caspers, BSI-Abteilungsleiter Technik-Kompetenzzentren zum neuen Engagement des BSI: *„Cloud Computing ist Rückgrat und Treiber der Digitalisierung in allen Bereichen, und damit ist Cloud-Sicherheit unentbehrlich für die Resilienz moderner Informationstechnik. Um eine sichere Cloud-Nutzung zu ermöglichen, liefert das BSI technologisch führende und unmittelbar einsatzfähige Lösungsbeiträge für das gesamte Cloud-Betriebsspektrum. Dabei steht im Mittelpunkt unseres Interesses als Cybersicherheitsbehörde, Digitale Souveränität und Kritische Infrastrukturen krisenfest und gleichzeitig zukunftsfähig zu machen.“*

Mehr als 60 IT-Dienstleister ließen sich für die Durchführung des CyberRisikoChecks schulen.

Erfolgreicher Start: Schulungen zum CyberRisikoCheck

Um kleine und mittlere Unternehmen (KMU) dabei zu unterstützen, ihre Cyberresilienz zu erhöhen, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeinsam mit Partnern den CyberRisikoCheck entwickelt. Er bietet KMU eine standardisierte, bedarfsgerechte Beratung durch IT-Dienstleister. Im April kamen erstmalig über 60 IT-Dienstleister nach Bonn, um sich zur Durchführung des CyberRisikoChecks schulen zu lassen. Sie können mit der neuen Expertise Unternehmen dabei unterstützen, eine Positionsbestimmung des eigenen IT-Sicherheitsniveaus vorzunehmen. BSI-Präsidentin Claudia Plattner: *„Der CyberRisikoCheck ist ein echtes Win-Win-Win-Produkt: für die kleinen Unternehmen, für die IT-Dienstleister und für das BSI. Damit haben wir den Grundstein für ein KMU-Cybersicherheitslagebild gelegt, und das ist ein wichtiger Schritt auf dem Weg zur Cybernation Deutschland. Wir freuen uns, dass schon jetzt mehr als 120 weitere IT-Dienstleister ihr Interesse an einer Durchführung es CyberRisikoChecks bekundet haben.“*



Neu für die Verwaltung: BSI-Support zur Schwachstellenanalyse von Verwaltungsportalen

Im März hat das BSI die Broschüre „Einstiegshilfe für die Schwachstellenanalyse von Verwaltungsportalen“ für Digitalisierungsverantwortliche in der Verwaltung veröffentlicht. Im Fokus steht die sichere Bereitstellung von Webportalen als Schnittstelle zu Bürgerinnen und Bürgern. Die hohe Komplexität birgt dabei die Gefahr von ausnutzbaren Schwachstellen in den Verwaltungsportalen, welche die Digitalisierung verlangsamen und das Vertrauen in die Verwaltung nachhaltig schädigen könnten. Mit Schwachstellenanalysen werden sowohl die Informationssicherheit als auch die Einhaltung der gesetzlichen Vorgaben dokumentiert. Schwachstellenanalysen verringern die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs und leisten einen Beitrag zur sicheren Digitalisierung der deutschen Verwaltung.

Aktuelle Entwicklungen im Bereich Sicherheit & Künstliche Intelligenz

KI hat Hochkonjunktur: Folgerungen für die Sicherheit und Transparenz von KI-Systemen sowie die Cyberbedrohungslage

von Dr. Matthias Heck, Referatsleiter Bewertungsverfahren und technische Unterstützung des digitalen Verbraucherschutzes in der Künstlichen Intelligenz, und Dr. Raphael Zimmer, Referatsleiter Sicherheit in der Künstlichen Intelligenz

Künstliche Intelligenz (KI) ist in unserem Alltag angekommen. In diesem Text werden drei zentrale Themen im Zusammenhang mit KI diskutiert: der Einfluss von missbräuchlicher KI-Nutzung auf die Cyberbedrohungslage, die Sicherheit von KI-Systemen und die Transparenz dieser Systeme.

KI hilft uns, schneller und effizienter zu arbeiten. Sie kann aber auch missbräuchlich eingesetzt werden: Kriminelle Akteure nutzen bereits heute aktiv Künstliche Intelligenz. So können sie mittels KI-Programmierassistenten schneller Schadsoftware entwickeln und anpassen. KI kann außerdem dabei helfen, Schwachstellen in Programmcodes zu identifizieren.

Eine große Rolle spielt KI auch bei der Distribution von Schadsoftware im Rahmen von Social Engineering. Mittels KI können Angreifer effektiver zuschlagen, etwa indem sie individualisierte E-Mails in überzeugender Qualität erstellen – mit dem Ziel, Nutzende so zu manipulieren, dass sie Daten preisgeben, Geld versenden oder sonst den Kriminellen in die Hände spielen. Auch können extrahierte Datenmengen bei Angriffen effektiver analysiert und sensible Inhalte schneller identifiziert werden, um beispielsweise Erpressungsversuchen Nachdruck zu verleihen. Wird KI eingesetzt, senkt das außerdem die Anforderungen an die Täter, denn für bestimmte Aufgaben wird kaum noch technisches Vorwissen benötigt.

Eine Analyse des britischen National Cyber Security Centre zu den kurzfristigen Auswirkungen von KI auf die Cyberbedrohungslage geht fast sicher davon aus, dass KI zu mehr und stärkeren Cyberangriffen in den nächsten beiden Jahren führen wird. Deshalb ist es wichtig, dass sich Deutschland zeitnah zu einer Cybernation entwickelt, die Cybersicherheit aktiv in allen Bereichen umsetzt.

Aufgrund der zunehmenden Arbeitsgeschwindigkeit von Cyberkriminiellen werden resiliente Infrastrukturen mit schnellen Patch-, Detektions- und Reaktionsfähigkeiten benötigt. Auch der Schulung und Sensibilisierung von Anwendenden kommt eine noch stärkere Bedeutung zu. Aufgrund der zunehmenden Dynamik müssen die Anstrengungen auf der Verteidigungsseite intensiviert werden.

ZUNEHMENDE BEDEUTUNG DER SICHERHEIT VON KI-SYSTEMEN

Nachdem die Sicherheit von KI-Systemen mehrere Jahre ein eher akademischer Forschungsbereich war, ist das Thema durch die weite Verbreitung von KI-Systemen in der Praxis mittlerweile sehr relevant. 2023 haben vor allem Entwicklerinnen und Entwickler geprüft, wie KI-Sprachmodelle gewinnbringend in ihre Anwendungen integriert werden können. Mittlerweile sehen wir, dass auch andere Zielgruppen aktiv KI-Anwendungen in die Praxis bringen: Durch die Bereitstellung von Chatbot-Baukästen können professionelle Anwendende ohne tiefergehende KI- und IT-Kenntnisse selbst Chatbots modular zusammenstellen. Durch Anweisungen (siehe Abbildung) können die Rolle und das Verhalten des Chatbots bestimmt werden. Für Hintergrundinformationen zu Produkten oder einer Firma können Dokumente als Wissensbasis hinterlegt werden. Es ist möglich, dem Chatbot Zugriff auf das Internet zum Abrufen von Echtzeitinformationen zu gewähren und über Funktionsaufrufe Systeme im Backend anzusteuern. Darüber hinaus können von der KI kontextabhängig passende Bilder erstellt und Programmcodes geschrieben sowie kompiliert werden. Auch komplexe Datenauswertungen sind möglich.

BSI-PUBLIKATION „GENERATIVE KI-MODELLE“ HILFREICH

Bei der Konfiguration eines solchen Chatbots gibt es aus Sicherheitsperspektive vieles zu beachten. Beispielsweise

Konzeptionelle Darstellung eines Chatbot-Baukastens mit verschiedenen Komponenten

können hinterlegte Dokumente oder Anweisungen in der Regel von Nutzenden extrahiert werden. Dies gilt auch dann, wenn der Chatbot explizit angewiesen wurde, über diese Dokumente keine Auskunft zu geben. Vor der Benutzung solcher Chatbot-Baukästen ist daher eine umfangreiche Sensibilisierung der Nutzerinnen und Nutzer empfehlenswert. Ein guter Einstieg ist die BSI-Publikation „Generative KI-Modelle: Chancen und Risiken für Behörden und Industrie“, die regelmäßig vom BSI aktualisiert und ergänzt wird.

AUCH AUF DIE TRANSPARENZ KOMMT ES AN

Wissenschaftlich gesehen sind KI-Modelle oder -Systeme transparent, wenn sie selbsterklärend sind. Dies trifft auf verschiedene Algorithmen zu, etwa auf den Entscheidungsbaum. Dort kann der Weg einer Vorhersage oder Aussage des KI-Systems ohne großen Aufwand nachvollzogen werden. Algorithmen hinter neuen und modernen KI-Systemen, wie wir sie bei großen Sprachmodellen oder bei generativer KI-Anwendung finden, weisen diese Transparenz leider nicht auf. Im Gegenteil, sie werden oft als Black-Box-Modelle bezeichnet: Es sind Systeme, die keinen Einblick erlauben. So ist zwar während der Anwendung die Eingabe nachvollziehbar, aber aufgrund welcher Entscheidungen das System eine Ausgabe erzeugt, kann nicht nachvollzogen werden. Da aber gerade diese Systeme mehr und mehr praktisch angewendet werden – etwa beim automatisierten Zusammenfassen von Texten – ist der Transparenzgedanke auch für diese Systeme wichtig.

ERWEITERUNG DES TRANSPARENZBEGRIFFS NOTWENDIG

Daher ist es notwendig, den Begriff der Transparenz im Zusammenhang mit KI-Systemen zu erweitern. Im Beispiel des oben beschriebenen Chatbots müsste nicht nur transparent gemacht werden, wie die Ausgabe zustande kommt, auch Randbedingungen des Systems sollten beschrieben werden. So sollten die verwendeten Modelle und Trainingsdaten, der exakte Einsatzzweck sowie die Limitierungen der Systeme inklusive möglicher Risiken und Gefahren offen kommuniziert werden, so wie auch der physische Ort, an dem das System betrieben wird. Wichtig wäre auch eine klare Angabe, wie die Daten weiterverwendet werden, die Nutzerinnen und Nutzer in das System eingeben.

Transparente KI-Systeme haben zwei entscheidende Vorteile: Sie stärken sowohl die Verbraucherinnen und Verbraucher, die die Systeme anwenden, als auch von Auswirkungen betroffene Dritte und sie sensibilisieren die Entwicklerinnen und Entwickler für Gefahren und Risiken. ■

Informationen zu Kurz-URLs und (sprechenden) Dok-IDs gibt es hier:

https://www.ncsc.gov.uk/news/global-ransomware-threat-expected-to-rise-with-ai

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Generative_KI-Modelle.pdf?__blob=publicationFile&v=5

www.bsi.bund.de/ki

Cybersicher? Aber sicher!

Was Unternehmen tun können, um heute ihr Cybersicherheitsniveau zu erhöhen und sich damit bestmöglich auf die Umsetzung der NIS-2-Richtlinie vorzubereiten

von Katrin Kubica, Leiterin Referat Kooperation mit Herstellern und Dienstleistern

Cybersicherheit muss auf die Agenda: In diesem Jahr steht besonders die europäische NIS-2-Richtlinie im Fokus. Unternehmen sollten spätestens jetzt Maßnahmen ergreifen, um ihr Cybersicherheitsniveau zu erhöhen. Unabhängig von regulatorischen oder gesetzlichen Vorgaben hat das BSI hierfür Angebote und Hilfestellungen entwickelt.

Die Mitgliedsstaaten sind verpflichtet, die NIS-2-Richtlinie (Network and Information Security Directive) bis spätestens Oktober 2024 in nationales Recht umzusetzen. Das ist eine EU-weite Regelung, die Unternehmen und Institutionen dazu verpflichtet, ihre jeweiligen Cyber- und Informationssicherheitsmaßnahmen zu verbessern.

Ob Deutschland das sogenannte NIS2UmsuCG bis zum Herbst verabschiedet hat, ist noch unklar. Fest steht, dass die Erhöhung des IT-Sicherheitsniveaus alternativlos ist. Vor allem für kleine und mittlere Unternehmen (KMU) ist das eine große Herausforderung. Die personellen, finanziellen und strukturellen Hürden sind immens, gleichzeitig steigt der Handlungsdruck aufgrund der wachsenden Bedrohungslage. Wie überall gilt: Anzufangen ist der wichtigste Schritt. Hat ein Unternehmen diesen Schritt getan, kann es sich im Austausch mit anderen Firmen und mit dem BSI als Cybersicherheitsbehörde des Bundes gemeinsam in Richtung mehr Cybersicherheit entwickeln.

ANGEBOTE DES BSI

Das BSI gibt es seit mehr als 30 Jahren und es verfügt über einen großen Erfahrungsschatz an Methoden, Empfehlungen und Standards für mehr Cyberresilienz in der Wirtschaft. Neben den BSI-Angeboten zur Selbsthilfe gibt es zahlreiche Möglichkeiten zum Austausch und zur Kooperation. Einen ausführlichen Überblick über die BSI-Angebote für die Wirtschaft finden Sie auf Seite 12.

AUSBLICK

Das NIS2UmsuCG wird sich enorm auf die Erhöhung des Cybersicherheitsniveaus in Deutschland auswirken. Unternehmen und Institutionen werden zu etlichen Maßnahmen verpflichtet. Die geplanten Auflagen und Regulierungen sind sinnvoll und längst überfällig. Unternehmen werden künftig noch mehr geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen müssen, um die IT und Prozesse ihrer erbrachten Dienste zu schützen, Störungen zu vermeiden und Auswirkungen von Sicherheits-

„Ob heute oder auf Basis von NIS-2: Unternehmen sollten anfangen, die Erhöhung ihres Cybersicherheitsniveaus voranzubringen. 100-prozentige Sicherheit gibt es nicht, aber jede Maßnahme zählt!“

Katrin Kubica, Leiterin Referat Kooperation mit Herstellern und Dienstleistern

vorfällen gering zu halten. Hierzu zählen u. a. verpflichtende Schulungen für Geschäftsleitungen, Maßnahmen zur Bewältigung von IT-Sicherheitsvorfällen, ein Back-up- und ein Krisenmanagement sowie der Einsatz von Multi-Faktor-Authentifizierung.

Cybersicherheit ist nicht nur Voraussetzung für eine gelungene Digitalisierung, sondern entscheidend für unser Zusammenleben, unsere wirtschaftliche Stärke und digitale Souveränität. Begreifen wir die Umsetzung der NIS-2-Richtlinie als einen bedeutenden EU-weiten Regulierungsrahmen und einen wichtigen Beitrag zur Cybernation Deutschland. Denn nur mit einem einheitlichen hohen Cybersicherheitsniveau begegnen wir heute und in Zukunft den wachsenden Herausforderungen in der IT-Sicherheit. Mehr Cybersicherheit ist nicht optional. Es ist die Gelingensbedingung. Das BSI unterstützt nicht nur mit den oben genannten Angeboten, sondern auch darüber hinaus. Sobald das NIS2UmsuCG verabschiedet wurde, wird das BSI zur Umsetzung informieren.

Dazu entwickelt das BSI den „NIS-2-Checker“, der es Unternehmen ermöglicht, anhand weniger Fragen schnell zu überprüfen, ob sie von der NIS-2-Richtlinie der EU betroffen sind. Sobald die nationale Umsetzung der Richtlinie erfolgt ist, wird auch der NIS-2-Checker aktualisiert. Der NIS-2-Checker weist ergebnisbezogen auf alle sich ergebenden Pflichten hin und bietet Hilfestellung bei der Umsetzung an. ■

NIS-2 kommt – das bietet das BSI für Unternehmen

Allianz für Cyber-Sicherheit

Kurzbeschreibung:
Mit der 2012 gegründeten Allianz für Cyber-Sicherheit verfolgt das BSI das Ziel, die Widerstandsfähigkeit des Wirtschaftsstandortes Deutschland gegenüber Cyberangriffen zu stärken. Die Initiative ist Europas größte öffentlich-private Partnerschaft im Bereich Cybersicherheit für mehr Prävention in der Wirtschaft.

Zielgruppe:
Unternehmen jeder Größenordnung, Verbände, Handelskammern, Forschung

Das bietet die ACS Unternehmen:
- die Expertise des BSI und der ACS-Partner,
- vertrauensvollen Erfahrungsaustausch zu Themen wie Angriffsvektoren, geeigneten Schutzmaßnahmen, Tipps zum Sicherheitsmanagement, Vorfallsbehandlung etc.,
- exklusive und für ACS-Teilnehmer kostenfreie Partner-Angebote zum Ausbau ihrer Cybersicherheitskompetenz,
- Teilnahme an Expertenkreisen, Erfahrungskreisen und den Cyber-Sicherheits-Tagen,
- regelmäßige aktuelle Informationen und Veranstaltungen zur Cybersicherheit.

» **Aktuell empfehlen wir:** „Management von Cyber-Risiken – Ein Handbuch für die Unternehmensleitung“

IT-Grundschutz

Kurzbeschreibung:
Der IT-Grundschutz ist mit seinem Baukastenkonzept ein ganz wesentliches Instrument, um Informationssicherheit zu erhöhen und kontinuierlich zu verbessern.

Zielgruppe:
Behörden und Unternehmen jeder Größenordnung

Das bietet der IT-Grundschutz Unternehmen:
Der IT-Grundschutz bietet ein systematisches Vorgehen, das es ermöglicht, notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen.

Aktuell empfehlen wir:
IT-Grundschutz-Profile, die für bestimmte Branchen spezifische Anwendungsfelder erarbeitet haben, erleichtern die Umsetzung zusätzlich. Für Handwerksbetriebe, Reedereien, chemische Betriebe, IT-Dienstleister und viele andere gibt es diese Profile bereits. Weitere wie Luftsicherheit und IT-Sicherheit von Lieferketten sind in der Erstellung.

» http://www.bsi.bund.de/IT-Grundschutz

UP KRITIS

Kurzbeschreibung:
Der UP KRITIS ist eine unabhängige Partnerschaft zwischen KRITIS-Betreibern, deren Verbänden und den zuständigen Behörden zu den Themen Cyber- und physische Sicherheit. Als KRITIS-Betreiber können Sie kostenfrei und ohne Verpflichtungen daran teilnehmen, auch wenn Ihre Organisation unterhalb der Schwellenwerte der BSI-Kritisverordnung liegt.

Zielgruppe:
KRITIS-Betreiber, deren Verbände und die zuständigen Behörden

Das bietet der UP KRITIS Unternehmen:
Im UP KRITIS haben Sie viele Möglichkeiten: Sie können sich in Ihrer Branche und branchenübergreifend vernetzen. Gemeinsam mit anderen Betreibern und den zugehörigen staatlichen Stellen

Cyber-Sicherheitsnetzwerk

Kurzbeschreibung:
Das Cyber-Sicherheitsnetzwerk (CSN) ist ein freiwilliger Zusammenschluss von qualifizierten Expertinnen und Experten für eine IT-Vorfallsbearbeitung. Mit dem Cyber-Sicherheitsnetzwerk soll eine flächendeckende dezentrale Struktur aufgebaut werden, die effizient und kostengünstig KMU sowie Bürgerinnen und Bürgern bei IT-Sicherheitsvorfällen Unterstützung anbietet.

Zielgruppe:
Unternehmen und Privatleute (KMU sowie Bürgerinnen und Bürger)

Das bietet das CSN Unternehmen:
Das CSN bietet qualifizierte Expertinnen und Experten für die IT-Vorfallsbearbeitung an, die sich bereit erklären, ihr individuelles Fachwissen zur Behebung von IT-Sicherheitsvorfällen zur Verfügung zu stellen. Sie unterstützen durch die Übernahme reaktiver Tätigkeiten, IT-Sicherheitsvorfälle zu erkennen und zu analysieren, das Schadensausmaß zu begrenzen sowie weitere Schäden abzuwenden.

» **Aktuell empfehlen wir:** Digitale Rettungskette:

UP KRITIS

können Sie in Arbeitskreisen beispielsweise den Stand der Technik mitbestimmen oder an Krisenübungen teilnehmen. Sie erhalten Informationen zu nationalen und internationalen Gesetzesvorhaben und können diese kommentieren. Sie erhalten Cybersicherheitswarnungen und Management-Infos und können selber Vorfälle melden.

» **Aktuell empfehlen wir:**
Das Papier „Nutzung von cloud-basierten Diensten in Kritischen Infrastrukturen – eine Hilfestellung des UP KRITIS“

CyberRisikoCheck

Kurzbeschreibung:
Der CyberRisikoCheck ermöglicht es kleinen und mittleren Unternehmen (KMU), nach einem einfachen, kostengünstigen und standardisierten Verfahren (DIN SPEC 27076) ihr Cybersicherheitsniveau zu ermitteln.

Zielgruppe: Klein- und Kleinstunternehmen
(< 50 Beschäftigte), mittlere Unternehmen

Das bietet der CyberRisikoCheck Unternehmen:
KMU erhalten nach einer ein- bis zweistündigen Befragung durch einen IT-Dienstleister einen ausführlichen Bericht, in dem etwaige Defizite beschrieben sind und konkrete Handlungsempfehlungen gegeben werden. Die Befragung überprüft in sechs Themenbereichen insgesamt 27 Anforderungen. Die Handlungsempfehlungen sind nach Dringlichkeit gegliedert und informieren auch über staatliche Fördermaßnahmen auf Bundes-, Landes- und kommunaler Ebene, die das Unternehmen in Anspruch nehmen kann.

» **Aktuell empfehlen wir:** Führen Sie baldmöglichst für Ihr Unternehmen einen CyberRisikoCheck durch. Weiterführende Informationen und qualifizierte Dienstleister finden Sie unter:

Quantencomputer als IT-Risiko

Die BSI-Studie zur aktuellen Bedrohungslage

von Dr. Heike Hagemeier, BMI-Referat Internationale Cybersicherheit und Cybersicherheitsforschung, und Stephanie Reinhardt, BSI-Referat Vorgaben an und Entwicklung von Kryptoverfahren

Quantentechnologien bieten enormes Potenzial, bisher unlösbare oder aufwendige Probleme zu bewältigen. Zur Wahrheit gehört aber auch, dass mit der Entwicklung von leistungsfähigen Quantencomputern unsere IT-Sicherheit bedroht wird.

Bisher existiert kein Quantencomputer, der kryptografisch relevante Algorithmen ausführen kann. Wenn es so weit ist, sind unsere vertrauliche Kommunikation und sicherheitsrelevante Daten jedoch gefährdet. Bereits jetzt speichern Angreifer verschlüsselte Informationen, um sie entschlüsseln zu können, sobald die erforderliche Technologie zur Verfügung steht („store now, decrypt later“).

Das BSI hat im Projekt „Laufende Aktualisierung der Studie Entwicklungsstand Quantencomputer“ eine Studie aus den Jahren 2017 bis 2020 fortgeführt. Die Untersuchung dient der Einschätzung des Entwicklungsstands von Quantencomputern, die potenziell zur Kryptoanalyse genutzt werden können. Zudem wird die Relevanz von ausgewählten Quantenalgorithmen betrachtet.

JÜNGSTE ENTWICKLUNGEN DER HARDWARE

Die größte Herausforderung bei der Entwicklung von Quantencomputern ist aktuell ihre Fehleranfälligkeit. Die Korrektur dieser Fehler ist durch einen enormen Overhead gekennzeichnet – die logischen Qubits, die einen Algorithmus beschreiben, bestehen aus einer großen Zahl von Bauelementen, den physikalischen Qubits. Zwar konnten inzwischen bereits erste Erfolge bei der Fehlerkorrektur erzielt werden, doch bislang weist die Hardware in den meisten Fällen noch nicht die nötige Qualität auf, um mittels Fehlerkorrektur eine Verbesserung zu erreichen.

Zurzeit wird an vielen unterschiedlichen Quantencomputer-Plattformen geforscht und es ist noch nicht abzusehen, welche sich durchsetzen werden. Für die Studie wurde ein Schichtenmodell zur Bewertung der Plattformen entwickelt. Es beginnt mit der Demonstration von Grundfunktionen und steigt bis zur fehlertoleranten Implementierung von Algorithmen an. Im Vergleich zur letzten Version der Studie wurden deutliche Fortschritte erzielt, vor allem etwa bei Ionenfallen und supraleitenden Qubits. Die Fertigung supraleitender Schaltkreise ist technologisch bereits weit entwickelt und lässt sich gut optimieren. Dies führt zu verfügbaren Quantenprozessoren mit mehr als 1.000 Qubits. Noch sind diese Qubits allerdings recht fehleranfällig und können zudem nicht alle direkt untereinander interagieren – die sogenannte Konnektivität ist gering. Im Vergleich dazu können auf Ionenfallen basierende Quantencomputer genauere Rechenoperationen durchführen und weisen eine höhere Konnektivität auf. Dafür ist es hier deutlich schwieriger, eine hohe Anzahl an Qubits zu realisieren. Bevor fehlerkorrigierende Quantencomputer zur Verfügung stehen, werden bereits „Noisy Intermediate-Scale Quantum (NISQ) Technologies“ eingesetzt. Bei ihnen werden Fehler nicht korrigiert, sodass nur eine begrenzte Anzahl an Rechenschritten ausgeführt werden kann. Die aktuelle Version der Studie betrachtet erstmalig auch Algorithmen, die für die Kryptoanalyse mit NISQ-Rechnern ausgelegt sind.

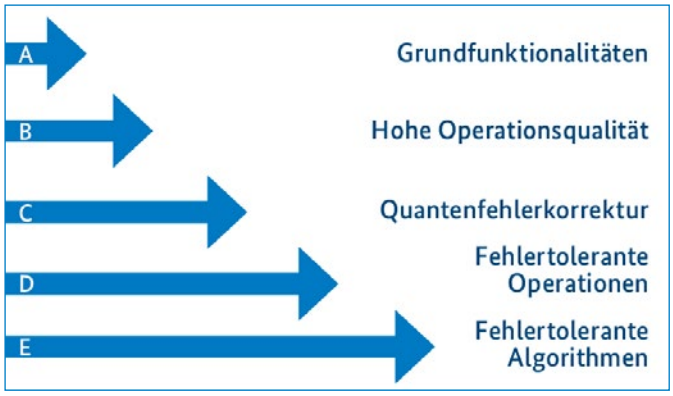


Abbildung 1: Schichtenmodell zur Bewertung von Quantencomputer-Plattformen

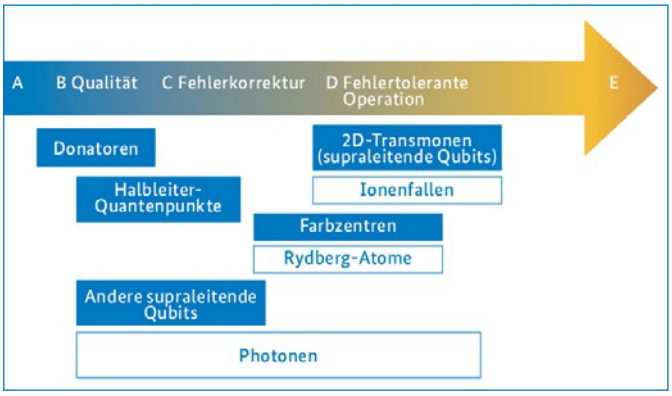


Abbildung 2: Einordnung der Technologien gemäß ihrer Entwicklungsstufe

RELEVANZ VON QUANTENCOMPUTERN FÜR DIE KRYPTOANALYSE

Ein Großteil der heute eingesetzten Public-Key-Kryptografie basiert auf dem Faktorisierungs- oder dem Diskreter-Logarithmus-Problem. Peter Shor zeigte in den 1990er-Jahren erstmals, dass diese beiden Probleme effizient lösbar sind, wenn ein hinreichend leistungsfähiger Quantencomputer verfügbar ist. Um einschätzen zu können, ab wann Quantencomputer einen solchen Vorteil in der Kryptoanalyse bringen, ist auch die genaue Analyse der Quantenalgorithmen selbst erforderlich. Eine Abschätzung von Gidney und Ekerå aus dem Jahr 2021 besagt z. B., dass mit 20 Millionen physikalischen Qubits das RSA-2048-Verfahren in acht Stunden gebrochen werden kann. Dieses wird beispielsweise im Internet breit eingesetzt, um die Vertraulichkeit und Authentizität von Daten zu sichern.

Für die Analyse symmetrischer Kryptografie bieten Quantencomputer ebenfalls Möglichkeiten, wie etwa den Suchalgorithmus von Grover und den Algorithmus von Simon. Die Auswirkungen sind nach aktuellem Stand jedoch deutlich weniger gravierend.

Inzwischen gibt es auch eine breite Palette an heuristischen Algorithmen, die speziell für einen Einsatz mit NISQ-Rechnern ausgelegt sind. Bisher wurde jedoch zu keinem dieser Algorithmen die Skalierbarkeit nachgewiesen. Dies lässt eine geringe kryptografische Relevanz solcher Algorithmen und NISQ-Technologien vermuten. Es ist aber wichtig, die Entwicklung weiter zu verfolgen.

FAZIT

Die Studie legt dar, dass die Entwicklung von Quantencomputer-Plattformen und -algorithmen stetig Fortschritte macht. Nach derzeitigem Stand wird angenommen, dass es mindestens ein Jahrzehnt dauern wird, bis kryptografische Relevanz erreicht ist. Dieser Zeitraum kann sich aber jederzeit verkürzen, sobald Entwicklungssprünge stattfinden. Aktuelle Veröffentlichungen verschiedener Forschungsgruppen lassen genau solche Sprünge vermuten, wie beispielsweise bei Plattformen, die auf neutralen Atomen basieren. Diese und weitere Veröffentlichungen werden in der nächsten Aktualisierung der Studie, die für Ende dieses Jahres geplant ist, berücksichtigt. Um das Risiko durch potenzielle, besonders einschneidende Entwicklungen abzumildern, arbeitet das BSI für den Hochsicherheitsbereich unter der Annahme, dass ab den 2030-er Jahren ein kryptografisch relevanter Quantencomputer zur Verfügung steht. Entsprechend wird die Migration zu quantensicherer Kryptografie vorangetrieben. Dabei liegt der Fokus besonders auf dem Schutz solcher Informationen, die auch noch in einem Jahrzehnt vertraulich sein müssen, um dem „store now, decrypt later"-Szenario vorzubeugen.

Das Ziel muss aber eine ganzheitlich quantensichere Cybernation Deutschland sein. Dafür ist noch viel zu tun! ■

Die Studie und weitere Informationen finden sich unter:

www.bsi.bund.de/Quanten

www.bsi.bund.de/qcstudie

Cybersicherheit und Digitalisierung im Land verankern

Mit seiner neuen Strategie zeigt das BSI einen Weg auf, wie die Cybernation Deutschland erreicht werden kann

Das Ziel ist ambitioniert, aber alternativlos. Denn es geht ums Ganze. Deutschland muss widerstandsfähig sein und bleiben, um Cyberbedrohungen abzuwehren. Gleichzeitig muss sichergestellt sein, dass Bürgerinnen und Bürger genauso wie Unternehmen digitalen Technologien, die sie nutzen, auch vertrauen können. Deshalb hat das BSI eine Strategie erarbeitet, wie Deutschland Cybernation werden kann: Ein Land, das Cybersicherheit und Digitalisierung erstklassig beherrscht.

Was braucht eine Cybernation? Bürgerinnen und Bürger, die wach und aufmerksam sind. Eine Gesellschaft, die sich der Gefahren des digitalen Fortschritts bewusst ist. Menschen, die nicht bang wie das Kaninchen vor der Schlange stehen, sondern der Realität ins Auge blicken. Die sich darauf verlassen können, dass sich der Staat um die sichere Gestaltung der Digitalisierung kümmert – die gleichzeitig aber in der Lage sind, ihre digitale Umgebung eigenständig zu schützen. Initiativen zum Schutz vor Cyberbedrohungen gehören auf die Tagesordnung. Denn die anhaltende Digitalisierung und die zunehmende Vernetzung vergrößern die Angriffsflächen – und diese werden genutzt.

MASSIVE POLITISCHE DESINFORMATIONSKAMPAGNEN

Der BSI-Bericht zur Lage der IT-Sicherheit in Deutschland im vergangenen Jahr zeichnet ein besorgniserregendes Bild: eine Viertelmillion neue Schadsoftwarevarianten und 21.000 infizierte Systeme tagtäglich, dazu mehr als 2.000 Schwachstellen in Softwareprodukten pro Monat. Der Schaden durch Angriffe auf deutsche Unternehmen belief sich auf mehr als 200 Milliarden Euro. Anfang dieses Jahres registrierte das Auswärtige Amt verstärkt Versuche von ausländischen Akteuren, die Innenpolitik in Deutschland zu beeinflussen. Mit massiven Kampagnen wurde auf Debatten zu außenpolitischen Themen in den Onlinenetzwerken eingewirkt. Russland stand in Verdacht, mit mehr als 50.000 gefälschten Accounts auf der Onlineplattform X und mehr als einer Million deutschsprachiger Tweets Unmut gegen die deutsche Regierungskoalition zu schüren. Häufig tauchte der Vorwurf auf, die Bundesregierung vernachlässige die eigene Bevölkerung, um die Ukraine zu unterstützen. Desinformation wird eingesetzt, um demokratische Gesellschaften zu destabilisieren.

TÄUSCHEND ECHTE KI-FÄLSCHUNGEN

Auch in den USA zeigte man sich alarmiert, als Mitglieder der Demokratischen Partei automatisierte Anrufe erhielten, in denen vermeintlich US-Präsident Joe Biden sie dazu aufforderte, die Vorwahlen zu ignorieren. Die täuschend echt klingende Stimme beweist einmal mehr, wie leistungsstark Fälschungen mithilfe Künstlicher Intelligenz (KI) sind. Auch der Popstar Taylor Swift kann ein Lied davon singen: KI-generierte Nacktbilder von ihr bescherten dem Thema Cyberkriminalität weltweit große Aufmerksamkeit.

GEZIELT GESTÖRTE SATELLITENNAVIGATION

Besonders aufmerksam sind auch Sicherheitsfachleute im Ostseeraum, die seit Monaten gezielte Störungen der Satellitennavigation beobachten. Seit Dezember 2023 wurden laut Bundesverkehrsministerium aus dem deutschen Luftraum Störungen der vom Satellitennavigationssystem „Global Positioning System“ (GPS) ausgestrahlten Navigationssignale gemeldet. Auch in dieser Angelegenheit steht Russland in Verdacht. Die Satellitennavigation wird für die Bestimmung der eigenen Position und zur Routenplanung in Fahrzeugen verwendet. Flugzeuge und Schiffe nutzen Satellitennavigation. Sie ist außerdem für automatisierte Prozesse in der Landwirtschaft relevant.

„Den Herausforderungen in der Cybersicherheit begegnet ein Land nicht auf dem Papier, sondern durch Technologie. Dafür kann Deutschland auf eine exzellente Technologiekompetenz zur Entwicklung von Lösungen zurückgreifen. Es gilt, die Digitalisierung zu beschleunigen, um mit den Entwicklungen unserer Zeit Schritt zu halten!“

Claudia Plattner, BSI-Präsidentin

WARUM DAS ZEITALTER DER POLYKRISEN NACH EINER CYBERSTRATEGIE VERLANGT

Geopolitische Spannungen, wie die drohende Eskalation im Nahostkonflikt und der russische Angriffskrieg auf die Ukraine, weltweite Herausforderungen, wie die Bewältigung des Klimawandels und die Sicherstellung der Energieversorgung, sowie innenpolitische Angelegenheiten, zu denen auch die Auswirkungen der Corona-Pandemie gehören, wirken sich auf die Cybersicherheitslage aus. Die Welt kannte schon immer multiple Krisen, inzwischen hat das Zeitalter der Polykrisen begonnen: Kritische Situationen lassen sich kaum mehr isoliert voneinander betrachten. Deepfakes auf Social-Media-Plattformen werden eingesetzt, um Meinungen zu beeinflussen, Wahlen zu manipulieren oder Gesellschaften zu destabilisieren. „Wir alle sind gefordert, den Gefahren konsequent und mutig entgegenzutreten“, lautet deshalb ein Kerngedanke der Cyberstrategie des BSI.

„Wir wollen mit der Initiative ‚Cybernation Deutschland' gemeinsam erreichen, dass Unternehmen und Betreiber kritischer Infrastrukturen widerstandsfähiger werden und sich noch stärker gegen Cyberangriffe wappnen. Sichere Digitalisierung ist unser gemeinsames Ziel. Denn: Je stärker und resilienter wir als Standort Deutschland sind, desto attraktiver sind wir auch für Wissenschaft, Unternehmen und IT-Fachkräfte. Dabei wollen wir auch für mehr Bewusstsein für Cybersicherheit überall in unserer Gesellschaft sorgen und den digitalen Verbraucherschutz verbessern."

Nancy Faeser, Bundesministerin des Innern und für Heimat

KOMPETENZEN NUTZEN, TECHNIK BEFÄHIGEN

Tagtäglich werden Unternehmen und Institutionen in Deutschland von Cyberkriminellen angegriffen. Besonders beunruhigend ist die hohe Professionalität im Vorgehen: Modernste Technologie wie KI kommt zum Einsatz und die Arbeitsteilung nimmt weiter zu, vor allem bei Ransomware-Attacken und „Cybercrime-as-a-Service", einer perfiden Art krimineller Dienstleistungen. Menschen in Deutschland leben so digital wie nie zuvor. Niemand will auf Onlineshopping oder Onlinebanking, Nachrichtenkonsum und Information im Netz oder Zeitvertreib in sozialen Medien verzichten – deshalb ist es im Interesse aller, dass digitale Angebote sicher sind.

Hier setzt das BSI an und stärkt Staat, Gesellschaft und Wirtschaftsunternehmen bei ihren Initiativen, die Cyberresilienz zu erhöhen. Den Herausforderungen in der Cybersicherheit begegnet ein Land nicht auf dem Papier, sondern durch Technologie. Dafür kann Deutschland auf eine exzellente Technologiekompetenz zur Entwicklung von Lösungen zurückgreifen. Es gilt, die Digitalisierung zu beschleunigen, um mit den Entwicklungen unserer Zeit Schritt zu halten!

CYBERSICHERHEIT FUNKTIONIERT NUR HAND IN HAND

Das Beispiel der GPS-Störungen verdeutlicht die Situation: Satellitensysteme sind unverzichtbar, um die zunehmende Verkehrsdichte und die Automatisierung im Mobilitätssektor zu bewältigen. Expertinnen und Experten analysieren Störungen und lernen daraus für zukünftige Technologieentwicklungen. Die für den Schutz des elektromagnetischen Spektrums zuständige Bundesnetzagentur beobachtet die Lage und tauscht sich mit beteiligten Bundes- und Landesbehörden, mit der Bundeswehr und weiteren Nutzenden des Luftraums aus – denn Cybersicherheit ist eine Gemeinschaftsaufgabe.

GEMEINSCHAFTLICHES HANDELN STÄRKT DIE RESILIENZ

Kooperation ist deshalb ein zentrales Stichwort der BSI-Cyberstrategie: Es bedarf der konsequenten Zusammenarbeit von Politik, Wirtschaft, Wissenschaft und Gesellschaft im Bund wie in den Ländern, damit Deutschland seine Technologiekompetenzen gezielt einsetzen und die digitale Sicherheit erhöhen kann. Wächst Deutschlands Selbstverständnis als Cybernation, kann die nötige Resilienz aufgebaut werden. Das BSI sieht sich in diesem Prozess in vielen Rollen: als Antreiber und Möglichmacher, als Partner und als Helfer, als Architekt und gleichzeitig als tragende Säule in der Sicherheitsarchitektur des Landes. Das BSI weiß, dass die effiziente und effektive Zusammenarbeit aller Akteure und eine funktionierende Koordination der notwendigen Maßnahmen Mammutaufgaben sind.

DIE BSI-CYBERSTRATEGIE AUF EINEN BLICK

Um Deutschland gemeinsam zur Cybernation zu machen, kommt es auf sechs bedeutende Handlungsfelder an:

Das BSI tritt als Promoter der Cybersicherheit auf. Es strebt an, den Schutz kritischer Systeme und sensibler Informationen im Bewusstsein aller Akteure zu verankern. Entscheiderinnen und Entscheider in Deutschland sollen dazu bewegt werden, das Thema regelmäßig und wiederkehrend auf ihre Agenda zu setzen.

BSI KNÜPFT TRAGFÄHIGE NETZWERKE ZU STAKEHOLDERN

Mit wem steht das BSI im Austausch? Auf Bundesebene mit Behörden, Organisationen und Unternehmen. Das BSI erstellt Vorgaben, berät, schlägt konkrete Umsetzungen vor, prüft die Sicherheitsanforderungen, treibt den Einsatz sicherer Technologien voran und koordiniert unmittelbar wirksame Maßnahmen zum Schutz der Informationstechnik. Zudem kooperiert es mit den Behörden auf Bundesebene, die in ihrem Aufgabenbereich an der Cybersicherheit Deutschlands mitwirken, etwa bei der Strafverfolgung, bei Grenzkontrollen, in der militärischen Zusammenarbeit, bei der Gefahrenabwehr und im Zivilschutz.

Auf Landesebene steht das BSI in Kontakt mit den für Cybersicherheit zuständigen Akteuren in allen 16 Bundesländern: Das sind Landesministerinnen und -minister, „Chief Information Security Officer“ (CISO), „Computer Emergency Response Teams“ (CERT), länderübergreifende Genossenschaften mit IT-Aufgaben sowie Landesagenturen oder sonstige staatliche Einrichtungen. Das BSI unterstützt länderübergreifende Initiativen mit Bundesbeteiligung und im Einzelfall – etwa auf Basis einer Kooperationsvereinbarung – auch Länder direkt. Auf der kommunalen Ebene zählen die städtischen Verwaltungen und die kommunalen Spitzenverbände zum BSI-Netzwerk.

„Das Team des BSI stellt sich der Mammutaufgabe, die Cyberresilienz der Unternehmen und Institutionen substanziell zu erhöhen, indem es Verbesserungen aktiv steuernd vorantreibt – immer in dem Bewusstsein, dass den Herausforderungen in der Cybersicherheit nicht auf dem Papier begegnet werden kann, sondern dass sie Tatkraft verlangen.“

Claudia Plattner, BSI-Präsidentin

In der Politik gehören alle parlamentarischen Akteure auf Bundes- und Landesebene sowie Organisationen, Initiativen, Stiftungen und Thinktanks zu den Partnern. Dazu kommen Universitäten, wissenschaftliche Institutionen, Forschungseinrichtungen sowie einzelne Wissenschaftlerinnen und Wissenschaftler. Sie bilden den Kern der nationalen und internationalen BSI-Kooperation mit der Wissenschaft. Diskutiert wird auf fachlich-technischer Ebene, Erkenntnisse werden bilateral und auf Fachkonferenzen ausgetauscht. Man lernt voneinander mit dem gemeinsamen Ziel, Grundlagen der Cybersicherheit zu erforschen und Weiterentwicklungen aktiv und marktfähig zu gestalten.

LEBENDIGES ÖKOSYSTEM FÜR CYBERSICHERHEITSPRODUKTE

Das Team des BSI stellt sich der Mammutaufgabe, die Cyberresilienz der Unternehmen und Institutionen substanziell zu erhöhen, indem es Verbesserungen aktiv steuernd vorantreibt – immer in dem Bewusstsein, dass den Herausforderungen in der Cybersicherheit nicht auf dem Papier begegnet werden kann, sondern dass sie Tatkraft verlangen. Das BSI setzt auf die exzellente Technologiekompetenz in Deutschland zur Entwicklung von Lösungen. Die Cybersicherheit ist dabei ein entscheidender Erfolgsfaktor: Indem Lösungen erarbeitet werden, steigen Sicherheit und Geschwindigkeit bei der Digitalisierung. Von drei Seiten unterstützt durch Politik, Wirtschaft und Wissenschaft entsteht ein lebendiges Ökosystem für Cybersicherheitsprodukte und -services. So ist Deutschland gewappnet und kann auf weitere Herausforderungen effizient und effektiv reagieren.

FORTSCHRITT DANK BSI-WERTSCHÖPFUNGSKETTE

Eine wichtige Voraussetzung für die Cybersicherheit ist die Einschätzung der Sicherheitslage. Durch Forschung und Prüfung im BSI werden notwendige Anforderungen identifiziert und Lösungen auf ihre Tragfähigkeit getestet. Anhand der BSI-Wertschöpfungskette werden Anforderungen und Vorgaben für sichere Produkte und Services sowie für die Sicherheit in Organisationen festgelegt. Zudem stellt das BSI Implementierungshilfen zur Verfügung. Im Rahmen von Zertifizierungen wird geprüft, ob Produkte und Services den Sicherheitsanforderungen entsprechen. Das BSI beurteilt auch die Sicherheit der Bundesverwaltung und der Kritischen Infrastrukturen. Die Ergebnisse der Begutachtungen schaffen Transparenz in Bezug auf die Sicherheitssituation in Deutschland. Mit „Security Operations“ und Support bereitet das BSI auf den Ernst- und Krisenfall vor.

DIE VISION DER CYBERNATION DEUTSCHLAND

Längst haben das BSI und seine Partner mit der Umsetzung erster relevanter Maßnahmen für Cybersicherheit begonnen.

FOLGENDE ZIELE STEHEN IM ZENTRUM DER VISION:

Unternehmen und Institutionen in Deutschland sind resilient gegen Cyberangriffe.

Deutschland ist gut aufgestellt gegen Cyberspionage und -sabotage.

Die Gesellschaft in Deutschland erkennt gezielte Beeinflussung von außen und weiß damit umzugehen.

Die Menschen in Deutschland bewegen sich sicher im Cyberraum.

Deutschland ist ein Vorreiter der sicheren und effizienten Digitalisierung.

Die Menschen vertrauen den digitalen Angeboten des Staates.

Deutschland ist ein attraktiver und innovativer Standort für digitale Technologien und Dienstleistungen.

Mehr Informationen zur Cybernation und zu den strategischen Zielen des BSI gibt es hier:

https://www.bsi.bund.de/dok/cybernation-deutschland

Fundament der Cybernation Deutschland

Neues Nationales IT-Lagezentrum behält die Cybersicherheit rund um die Uhr im Blick

von Sebastian Brück und Christian Eibl, Nationales IT-Lagezentrum, Grundsatz und Meldestelle, Informationsdauerdienst

Das neue Nationale IT-Lagezentrum ist mit modernster Kommunikationstechnik ausgestattet und verfügt im Regelbetrieb über zehn Arbeitsplätze, von denen aus die Spezialistinnen und Spezialisten des BSI die Cybersicherheitslage für Deutschland rund um die Uhr im Blick behalten. Bei der Eröffnung im Februar 2024 starteten Bundesinnenministerin Nancy Faeser und BSI-Präsidentin Claudia Plattner die Initiative „Cybernation Deutschland".

Mit der BSI-Initiative „Cybernation Deutschland" soll Deutschland ein hohes Sicherheitsniveau der Digitalisierung erreichen – das gilt für staatliche Institutionen ebenso wie für die Wirtschaft und die Gesellschaft. Neben der Erhöhung der Cyberresilienz soll die Initiative dazu dienen, insgesamt mehr Bewusstsein für das Thema Cybersicherheit zu schaffen, Cybersicherheit pragmatisch zu gestalten und messbar zu machen, technologische Expertise in Deutschland gezielter zu nutzen und in Deutschland den Markt für Cybersicherheitsprodukte und Dienstleistungen zu stärken.

Diese Herangehensweise ist dringend notwendig, da Unternehmen und Institutionen in Deutschland jeden Tag von Cyberkriminellen angegriffen werden. Von Angriffen mit Ransomware geht dabei momentan die größte Bedrohung aus. Hinzu kommen eine wachsende Professionalisierung auf Täterseite und eine steigende Anzahl von Sicherheitslücken.

Im neuen Nationalen IT-Lagezentrum verfügt das BSI über modernste Infrastruktur, um die Cybersicherheit substanziell zu erhöhen. Die Mitarbeitenden im Lagezentrum tauschen regelmäßig sowohl mit anderen Expertinnen und Experten im BSI – Stichwort: „integrierte Wertschöpfungskette" – als auch mit nationalen und internationalen Partnern Informationen und Bewertungen zur Cybersicherheitslage aus.

RUND UM DIE UHR IM EINSATZ

Das Nationale IT-Lagezentrum beobachtet und bewertet Vorkommnisse der Cybersicherheitslage im 24/7-Betrieb und verfügt so jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland. Mit dieser Übersicht können die BSI-Expertinnen und -Experten bedrohliche Lagen wie Angriffswellen oder potenziell ausnutzbare Schwachstellen frühzeitig feststellen und Handlungsbedarf sowie -optionen sowohl auf staatlicher Ebene als auch in der Wirtschaft zeitnah und kompetent einschätzen.

Innerhalb üblicher Bürozeiten unterstützen BSI-Expertinnen und -Experten für die Kritischen Infrastrukturen (KRITIS) und des Computer Emergency Response Teams des Bundes (CERT-Bund) sowie die Informationssicherheitsoffiziere des Kommandos Cyber- und Informationsraum (KdoCIR) das Nationale IT-Lagezentrum. Außerhalb der Bürozeiten gehen CERT-Bund und KRITIS in Rufbereitschaft. Die Zusammenarbeit mit dem KdoCIR erfolgt über die etablierten Schnittstellen zwischen beiden Behörden.

Zudem ist das Nationale IT-Lagezentrum die zentrale Meldestelle des BSI. Hier laufen diverse gesetzlich oder vertraglich festgeschriebene, aber auch freiwillige Meldestellen zusammen. Pro Jahr gehen im IT-Lagezentrum rund 2.800 Meldungen über 22 Meldestellen ein. Eine aktive Open Source Intelligence (Medienbeobachtung, Social-Media-Analyse, etc.) und eigene Sensoriken ergänzen die Informationsbasis.

SO REAGIERT DIE BSI-SCHALTZENTRALE BEI EINEM CYBERSICHERHEITSVORFALL

Wie kann man sich den Alltag in der Schaltzentrale des BSI vorstellen? Ein Beispiel: Eine Meldung zu einem Sicherheitsvorfall trifft ein, zeitgleich schlagen Monitoringsysteme an. Nach sofortiger Rücksprache mit dem Betroffenen deutet alles auf eine Schadsoftware hin. Folgende Fragen müssen beantwortet werden: Was ist das Ziel der Software? Welche Auswirkungen sind zu erwarten? Wer kann damit noch zum Opfer werden und was bedeutet dies für die Cybersicherheitslage Deutschlands?

Hoher Besuch bei der Eröffnung des neuen Nationalen IT-Lagezentrums: Bundesinnenministerin Nancy Faeser, BSI-Präsidentin Claudia Plattner und der stellvertretnde Inspekteur des Cyber- und Informationsraums (CIR), Generalmajor Jürgen Setzer (v.l.n.r.). Sebastian Brück, Leiter Informationsdauerdienst, führte die Gäste durch die neuen Räumlichkeiten.

Im Nationalen IT-Lagezentrum wird die breite Expertise des BSI gebündelt, von dort aus wird die Reaktion der Cybersicherheitsbehörde des Bundes koordiniert: IT-Spezialistinnen und -Spezialisten aus den unterschiedlichsten Fachrichtungen analysieren gemeinsam die Bedrohungen und entwickeln Gegenmaßnahmen. Da Cyberbedrohungen nicht an Landesgrenzen enden, werden aktuelle Informationen und Bewertungen in etablierten Prozessen auch gemeinsam mit nationalen und internationalen Partnern, wie z. B. unseren NATO-Partnern, ausgetauscht.

AUS DEM IT-LAGEZENTRUM IN DIE FACHABTEILUNGEN

Ist die Erstreaktion vollzogen, fließen die neuen Erkenntnisse in die langfristige Arbeit des BSI ein: Sollen die Ergebnisse in die IT-Grundschutz-Empfehlungen aufgenommen werden? Müssen Technische Richtlinien und Zertifizierungsverfahren angepasst werden? Sind Beratungsprozesse zu ergänzen? Das Nationale IT-Lagezentrum liefert mit seinen kontinuierlichen Erkenntnissen aus der Lagebeobachtung und -bewertung einen wichtigen Beitrag, damit das BSI seine gestaltende Rolle für die Cybersicherheit Deutschlands wahrnehmen kann.

LAGE ERKENNEN – UND ANGEMESSEN REAGIEREN

Während die Erkenntnisse unmittelbar in den Schutz der Regierungsnetze einfließen, gelangen Handlungsempfehlungen über geeignete Verteilmechanismen zeitnah und zielgerichtet an unterschiedliche Zielgruppen. Darunter fallen etwa Warnungen für die breite Öffentlichkeit, geeignete Informationen zum Schutz ihrer Systeme für IT-Profis in Kritischen Infrastrukturen, der Bundesverwaltung und kleineren Unternehmen sowie nicht zuletzt auch Informationen für Verbraucherinnen und Verbraucher. Je nach Bedrohungslage und Betroffenheit nehmen weitere Akteure wie das Mobile Incident Response Team (MIRT) ihre Arbeit auf.

Durch einen intensiven Informationsaustausch im Nationalen Cyber-Abwehrzentrum werden auch anderen Behörden zeitgerecht unterrichtet und Maßnahmen abgestimmt.

REAKTION AUF KRISEN

In besonders schweren Fällen wächst das IT-Lagezentrum zum Nationalen IT-Krisenreaktionszentrum auf. Dort arbeiten Spezialistinnen und Spezialisten verschiedener Fachgebiete eng zusammen, um in einer Krisensituation zügig wieder den Normalzustand herbeiführen zu können.

Im Ernstfall können dann durch die neue Infrastruktur bis zu 100 IT-Sicherheitsfachkräfte orchestriert zusammenarbeiten. Um die für den Betrieb des Lagezentrums erforderlichen Räume und Systeme miteinander zu vernetzen, wurden ca. 19.000 Meter Netzwerkkabel verlegt. Das entspricht der Länge eines Autokorsos über alle BSI-Liegenschaften auf dem Gebiet der Bundesstadt Bonn.

FAZIT UND NÄCHSTE SCHRITTE

Mit dem neuen Nationalen IT-Lagezentrum ist die Infrastruktur vorhanden, um die Cybersicherheit in Deutschland substanziell zu erhöhen. Mit dem BSI als Zentralstelle im Bund-Länder-Verhältnis würde sich das nationale Lagebild weiter vereinheitlichen und präzisieren lassen. Von einem Ad-hoc-Bedrohungslagebild und zentralen Sensoriken profitierten auch Länder und Kommunen, um Gefahren besser zu antizipieren. Dafür können im neuen Lagezentrum die Fäden zusammenlaufen, um Deutschland auch in der Fläche gegen Gefahren aus dem Cyberraum abzusichern. ■

Cybersicherheit in Landkreisen, Städten und Gemeinden gemeinsam ausbauen

Das BSI bringt Bund, Länder und den kommunalen Sektor an einen Tisch, um gemeinsam Strategien zu entwickeln, wie das Cybersicherheitsniveau in Kommunen erhöht werden kann

von Stefanie Euler, Referat Informationssicherheitsberatung für Länder und Kommunen

Kommunen geraten verstärkt ins Visier von Cyberkriminellen, das haben zahlreiche Angriffe in jüngster Zeit ebenso erschreckend wie eindrucksvoll bewiesen. Solche Angriffe haben regelmäßig weitreichende Folgen für die Kommunalverwaltungen – und damit für die Bürgerinnen und Bürger. Das BSI forciert darum die Zusammenarbeit zwischen Bund, Ländern, Kommunen, Verbänden und Dienstleistern. Denn Cybersicherheit ist eine Gemeinschaftsaufgabe, die alle zusammen angehen müssen.

Die Cybersicherheitslage in Deutschland ist besorgniserregend. Die Schäden für Wirtschaft, Verwaltung und Gesellschaft aufgrund von Cyberattacken gehen in die Milliarden Euro. Insbesondere Angriffe mit sogenannter Ransomware sind seit mehreren Jahren weitverbreitet, stellen sie doch ein lukratives Geschäftsmodell für Cyberkriminelle dar. Hinzu kommen eine wachsende Professionalisierung auf Täterseite und eine steigende Anzahl von Sicherheitslücken. Bei den Angriffen kann es jeden treffen. So beobachtet das BSI beispielsweise bei Cyberangriffen mit Ransomware eine Verlagerung der Attacken: Inzwischen sind nicht mehr nur große, zahlungskräftige Unternehmen das Ziel, sondern zunehmend auch kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen.

DURCHSCHNITTLICH ZWEI ANGRIFFE IM MONAT AUF KOMMUNEN

Mehr als zwei erfolgreiche Ransomware-Angriffe auf Kommunalverwaltungen oder kommunale Betriebe wurden im Durchschnitt in jedem Monat bekannt.

Das Beispiel eines kommunalen IT-Dienstleisters, der im vergangenen Jahr Opfer eines Cyberangriffs wurde, zeigt die Verwundbarkeit: Er entdeckte verschlüsselte Daten auf Servern und meldete den Angriff. Vorsorglich wurde die Mehrheit der IT-Systeme heruntergefahren – mit der Folge, dass mehr als hundert kommunale Verwaltungen nicht oder nur teilweise erreichbar waren. Auch die Webseiten der Verwaltungen waren betroffen. Fällt also ein zentraler IT-Dienstleister aus, wirkt sich das auf viele Kommunen und damit auch auf die breite Bevölkerung aus.

KOMMUNEN DESHALB BESONDERS SCHÜTZEN

Die Aufgabe, sich gegen Cyberangriffe zu wappnen, muss darum ganz oben auf der Agenda der kommunalen Entscheidungsträger stehen. Aber auch der Bund und die Länder müssen die Kommunen unterstützen – ist der Schutz der Verwaltung doch eine gemeinsame Aufgabe aller Akteure, die nur gemeinsam gelingen kann.

Individuelle Beratungen für Kommunen sind jedoch aufgrund ihrer Vielzahl nicht leistbar. Das BSI arbeitet daher eng mit zahlreichen engagierten Multiplikatoren auf kommunaler Ebene zusammen. Kommunen können auf Handreichungen und Empfehlungen zu bestimmten Themen zurückgreifen, auch auf spezifische Hilfsdokumente und Arbeitshilfen – wobei alle Unterstützungsangebote praxisnah und skalierbar sind. Sie stärken Verantwortliche dabei, den Einstieg in die Informationssicherheit zu finden und ihre Systeme und Netze wirksam zu schützen.

Ein weiteres Werkzeug, um Informationssicherheit möglichst effizient in Kommunalverwaltungen zu implementieren, sind sogenannte IT-Grundschutz-Profile. Mit diesen Schablonen für Informationssicherheit können Unternehmen und Behörden Profile für Anwendungsfälle erstellen und im Anschluss weiteren Interessierten zur Verfügung stellen. Anwendende, die ähnliche Sicherheitsanforderungen haben, können anhand dieser Vorlage ressourcenschonend das Sicherheitsniveau ihrer Institution überprüfen. Das BSI begleitet Vertreterinnen und Vertreter aus den Ländern und Kommunen u. a. bei der Entwicklung und Bereitstellung dieser IT-Grundschutz-Profile.

Außerdem führt das BSI unterschiedliche Veranstaltungen für die Zielgruppe Kommunen durch. Beispielsweise hat das BSI das Format „Roadshow Kommunen“ konzipiert und gemeinsam mit einigen Bundesländern durchgeführt. Hierbei handelt es sich um eine virtuelle Veranstaltungsreihe, die das Cybersicherheitsniveau im kommunalen Umfeld erhöhen soll.

Auch über Kooperationsvereinbarungen zwischen Ländern und dem BSI wird die Unterstützung der kommunalen Ebene adressiert. Um gemeinsam die Cyber- und Informationssicherheit auf ein höheres Niveau zu heben, hat das BSI bisher mit sechs Ländern Kooperationsvereinbarungen abgeschlossen. Die Vertragspartner unterstützen sich im Zuge der Kooperationsvereinbarungen untereinander, um so die Informationssicherheit effizient und effektiv zu erhöhen. Zu den Kooperationsbedarfen gehören beispielsweise: Austausch zu Cybersicherheitsinformationen, Warnungen, Hospitationen, Unterstützung bei Vorfallsmeldungen, Vorträge, um für das Thema Cybersicherheit zu sensibilisieren, oder auch gemeinsame Informationsveranstaltungen für Bürgerinnen und Bürger.

WAS KOMMUNEN BRAUCHEN

Grundlage für die verschiedenen Angebote ist der praktische Bedarf der Kommunalverwaltungen und wie man diesem begegnen kann. So thematisierte eine „BSI im Dialog“-Veranstaltung, die im Februar 2024 in Berlin stattfand, die Cybersicherheit in Kommunen unter der Leitfrage „Wie kann grundsätzlich zur Stärkung der Kommunen im Bereich der Cyber- und Informationssicherheit beigetragen werden?“. Das BSI hatte dazu Vertreterinnen und Vertreter von Bund, Ländern und Kommunen sowie Dienstleistern und Verbänden eingeladen, zu diskutierten und gemeinsam Handlungsstränge mit zum Teil konkreten Maßnahmen zu erarbeiten – immer mit dem Ziel, die Cybersicherheit in Kommunen schnell und effektiv zu erhöhen.

Dabei wurden mehrere konkrete Handlungsstränge identifiziert, die nun entweder durch das BSI oder einzelne Teilnehmende weiterverfolgt werden. Folgende Themen standen dabei im Fokus: die Verbesserung der Vernetzung, Möglichkeiten der IT-Bündelung, die Schaffung eines rechtlichen Rahmens in den Ländern, die Bereitstellung von ausreichenden Ressourcen, mögliche zentrale Services, die Durchführung von Cybersicherheitsübungen, die Etablierung von Standards und die Trendthemen KI und Cloud.

Als Fazit dieses Dialogs lässt sich aus Sicht des BSI festhalten: Die aktuellen Angebote u. a. der Informationssicherheitsberatung für Länder und Kommunen des BSI sind zielführend, sie sollten weiterverfolgt und möglichst ausgebaut werden. Dazu gehören auch die Checklisten aus dem Projekt „Weg in die Basis-Absicherung“ (WiBA), die Kommunen den Einstieg in den IT-Grundschutz vereinfachen und es ermöglichen, effektive Sicherheitsmaßnahmen ressourcenschonend umzusetzen. Auch die bisherigen Austauschformate sollen im Sinne der Vernetzung und des Wissensaustauschs fortgesetzt werden. So sollen insbesondere das „BSI im Dialog“-Format zwischen Bund, Ländern und Kommunen fortgeführt, die „Roadshows Kommunen“ verstetigt und zusätzliche ähnliche Dialog- und Informationsformate durch das BSI, die Länder und kommunale Spitzenverbände konzipiert werden.

BUND-LÄNDER-ZUSAMMENARBEIT AUSBAUEN

Der Austausch zwischen Bund, Ländern und Kommunen zeigt: Wir sind auf dem richtigen Weg, aber es gibt noch viel zu tun, um den steigenden Angriffen begegnen und somit ein verlässliches und nachvollziehbares Verwaltungshandeln in Städten, Kreisen und Gemeinden sicherstellen zu können.

Neben organisatorischen und technischen Maßnahmen sind dabei auch die rechtlichen Möglichkeiten weiter auszubauen. Derzeit werden die rechtlichen Rahmen von Bund und Ländern bereits voll ausgeschöpft. Um der steigenden Bedrohungslage Rechnung zu tragen, sollten weitere (verfassungs-)rechtliche Möglichkeiten geschaffen werden, damit Bund, Länder und Kommunen schnell, effizient und damit effektiv handeln können. Hierfür bedarf es u. a. der Möglichkeit, sich in konkreten Vorfällen zu unterstützen, Arbeitsteilung zu betreiben und ein gemeinsames Lagebild zu schaffen. Denn eins ist klar: Nur gemeinsam sind wir in der Lage, der organisierten Kriminalität und gezielten Angriffen begegnen zu können, um so eine erfolgreiche Digitalisierung und letztendlich eine kommunale Daseinsvorsorge zu gewährleisten. ■

Informationssicherheit von Anwendern für Anwender: Bereitstellung von IT-Grundschutz-Profilen:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Profile/it-grundschutz-profile_node.html

Fünf Jahre Cybersicherheit in Freital

Toller Teamspirit und sinnhafte Aufgaben am zweiten Dienstsitz des BSI

von Julia Wiebe, Referat Cyberluftsicherheit Grundsatz

Im Juli 2019 erfolgte der offizielle Startschuss für die Eröffnung des zweiten BSI-Standorts im sächsischen Freital. Heute – fünf Jahre später – arbeiten bereits mehr als 170 Kolleginnen und Kollegen am Standort zwischen Elbtal und Osterzgebirge mit daran, die Cybernation Deutschland zu bauen.

Prof. Thomas Popp, Staatssekretär für digitale Verwaltung und Verwaltungsmodernisierung sowie CIO Freistaat Sachsen

Der BSI-Standort in Freital stärkt seit 2019 die Cybersicherheit im Freistaat Sachsen. Dafür sind wir sehr dankbar.

Als Bundesland, das den Hochtechnologie-Cluster Silicon Saxony im Raum Dresden beherbergt, passt der BSI-Standort mit seiner Profilierung auf die Mobilfunktechnologien der nächsten Generation hervorragend in das bestehende Gefüge aus Lehre, Forschung und Wirtschaft – unter anderem mit dem Institut für Nachrichtentechnik an der TU Dresden, dem Barkhausen-Institut und den Forschungseinrichtungen wie dem Tech Innovation Center von Vodafone.

Sicherheit ist auch eine Grundvoraussetzung für eine gelingende Digitalisierung der Verwaltung. Um gegenüber den Gefährdungen aus dem Cyberraum gewappnet zu sein und im Ernstfall schnell wieder arbeitsfähig zu werden, müssen wir die Zusammenarbeit aller Ebenen intensivieren. Das tun wir in Sachsen als Staatsverwaltung mit den Kommunen durch eine gemeinsame integrierte IT-Sicherheitsarchitektur. Eine intensive Zusammenarbeit ist aber auch mit dem Bund notwendig. Ich freue mich daher, dass wir im November des letzten Jahres eine Kooperationsvereinbarung mit dem BSI unterzeichnet haben. Wir wirken bei der Cyberabwehr zusammen, unterstützen uns bei IT-Sicherheitsvorfällen und klären gemeinsam die Bürgerinnen und Bürger zum Thema Cyber- und Informationssicherheit weiter auf. Bei der letztjährigen sächsischen Roadshow zur Cybersicherheit unter dem Motto ‚Digital? Aber sicher!', an der über 3.000 Menschen in 13 sächsischen Städten teilnahmen, konnten wir das BSI als Partner gewinnen, der mit seinen Inhalten das Programm bereicherte.

Besonders hervorheben möchte ich auch die enge Zusammenarbeit beim Schutz der Kulturhauptstadt Europas Chemnitz 2025. Im kommenden Jahr wird ganz Europa auf Chemnitz und die Kulturregion schauen. Das wird ein besonderes Fest. Sicherheitsvorfälle sollen draußen bleiben.

Ich freue mich auf die weitere Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik.
Der Schwerpunkt der Arbeit, die in Freital geleistet wird, liegt u. a. in der Entwicklung von sicherem 5G/6G, im Digitalen Verbraucherschutz und in der Cybersicherheit der zivilen Luftfahrt. Drei Fachexpertinnen und Fachexperten stellen exemplarisch das breite Aufgabenspektrum am Standort Freital dar.

- **30.04.2024:** Offizielle Schlüsselübergabe für renovierte Liegenschaft
- **15.12.2023:** Einrichtung des Fachbereichs „Cyberluftsicherheit“ für die zivile Luftfahrt
- **30.08.2023:** Eröffnung 5G/6G Security LAB (TEMIS)
- **01.12.2022:** Start des Inhouse-Betriebs des BSI-Service-Centers
- **01.01.2022:** 100 Mitarbeitende am Standort Freital
- **12.2021:** Einführung des IT-Sicherheitskennzeichens
- **16.06.2021:** Erste Veröffentlichung des Berichts zum Digitalen Verbraucherschutz
- **11.07.2019:** Unterzeichnung der Absichtserklärung

„Es herrscht ein toller Teamspirit“

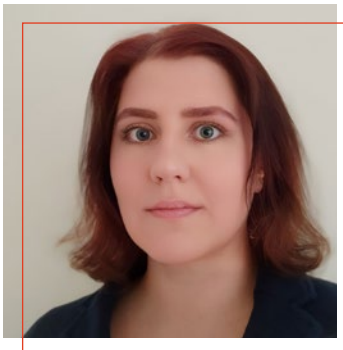
Auf der Suche nach neuen beruflichen Herausforderungen habe ich vor einem Jahr die Stellenanzeige des BSI für eine Stelle im Geschäftszimmer der Abteilung Cybersicherheit für Wirtschaft und Gesellschaft entdeckt. Es gibt viele Punkte, warum ich gerne zur Arbeit komme: In unserer Abteilung geht es um gesellschaftliche und wirtschaftliche Aspekte der Cybersicherheit, das ist interessant und niemals langweilig. Für mich persönlich sind die Chancen zur Weiterbildung sowie die Familienfreundlichkeit absolute Pluspunkte. Nach meinem ersten Jahr im #TeamBSI bin ich froh, den Schritt nach Freital gewagt zu haben. Wir haben im BSI nicht nur zahlreiche fachliche Themen, sondern auch viele Gestaltungsmöglichkeiten, uns einzubringen, etwa wenn es um die Kultur des Miteinanders und den Zusammenhalt unter den Kolleginnen und Kollegen geht. Zum Beispiel bei den regelmäßigen Veranstaltungen zum Teambuilding wie dem Sommerfest oder Abteilungsveranstaltungen.

Kristin Lindner, Abteilung Cybersicherheit für Wirtschaft und Gesellschaft

„Von unserer Arbeit profitiert die Gesellschaft“

Schon während meines Masterstudiums Public Administration begeisterte ich mich für die Themen Verwaltungsdigitalisierung und eGovernment. Die Eröffnung des BSI-Standorts in Freital bot mir die perfekte Gelegenheit, mich stärker auf Projekte an der Schnittstelle von Technik und Verwaltung zu konzentrieren. Als Referent bin ich hier für das freiwillige IT-Sicherheitskennzeichen des BSI zuständig. Gemeinsam mit meinen Kolleginnen und Kollegen arbeite ich daran, die Cybersicherheit von Verbraucherprodukten transparenter zu gestalten und Herstellern einen Anreiz für die sichere Gestaltung ihrer digitalen Produkte zu geben. Unser Beitrag zur Sicherheit in der digitalen Welt, der gesellschaftliche Nutzen unserer Arbeit und mein tolles Team motivieren mich tagtäglich für meinen Job im #TeamBSI.

Paul Trinks, Referat Erteilung von IT-Sicherheitskennzeichen



„Wir haben gute Aufstiegsmöglichkeiten“

Vor drei Jahren wagte ich den Schritt in den öffentlichen Dienst und habe ihn bis heute nicht bereut. Angefangen im BSI habe ich als Referentin bei der Informationssicherheitsberatung. In dieser Position konnte ich von Beginn an Verantwortung übernehmen und u. a. digitale Tools in meinem Fachbereich einführen. Besonders begeistert bin ich von der offenen Kultur und dem starken Zusammenhalt im BSI. Wir alle verfolgen das gleiche Ziel: einen gesellschaftlichen Mehrwert leisten. Das BSI fördert zudem die persönliche und berufliche Weiterentwicklung der Mitarbeitenden. Neben einem umfangreichen Schulungsangebot werden interne Aufstiegsmöglichkeiten geboten. Diese habe ich genutzt und seit März 2024 die Leitung eines neu gegründeten Referats übernommen. Gemeinsam mit meinem Team leiste ich aktiv einen Beitrag dazu, dass die Cybersicherheit in der zivilen Luftfahrt nachhaltig gestärkt wird und Fliegen somit sicher bleibt.

Sandra Teichert, Referat Cyberluftsicherheit Grundsatz

BSI
20. Deutscher
IT-Sicherheitskongress

Brennglas für Cybersicherheit:
20 Jahre Deutscher IT-Sicherheitskongress

Zum 20. Mal organisierte das BSI die hochkarätige Fachveranstaltung, auf der Verantwortliche aus Verwaltung, Wirtschaft, Wissenschaft und Gesellschaft aktuelle Themen und Fragestellungen der Cybersicherheit diskutieren. Anlässlich dieses Jubiläums hat die BSI-Magazin-Redaktion mit dem ehemaligen BSI-Präsidenten Michael Hange gesprochen. Er war im Gründungsstab des BSI und hat von Tag eins an bis zu seinem Ausscheiden im Jahr 2015 an allen IT-Sicherheitskongressen teilgenommen. Selbst im Ruhestand lässt er es sich nicht nehmen, einige Vorträge des Onlinekongresses zu verfolgen.

Herr Hange, wie kam es damals zum ersten IT-Sicherheitskongress? Was war das Ziel, wer die treibende Kraft im BSI, das zum damaligen Zeitpunkt noch eine recht überschaubare Anzahl von Mitarbeiterinnen und Mitarbeitern hatte?

Michael Hange: Der erste Deutsche IT-Sicherheitskongress fand 1990 im Vorfeld der Gründung des BSI und vor dem Hintergrund der deutschen Wiedervereinigung, für mich im Gründungsstab des BSI, in einer sehr spannenden Zeit statt. So nahmen auch Vertreter des zentralen Chiffrierorgans der DDR am Kongress teil. Das BSI wurde erst 1991 mit Arbeitsbereichen aus unterschiedlichen Sicherheitsbehörden aus der Taufe gehoben. Gemeinsames Ziel des Bundesinnenministeriums und des Gründungspräsidenten Otto Leiberich war es, mit dem Kongress bereits 1990 das künftige BSI und seine Themen, die bis dahin nur Eingeweihten bekannt waren, erstmalig einem größeren Fachpublikum vorzustellen. Das BSI hat sich mit Beteiligung von externen Vortragenden als neue technische Behörde vorgestellt, die sich nicht nur auf die Verwaltung ausgerichtet hat, sondern explizit auch die Wirtschaft sowie Bürgerinnen und Bürger einbezog. Aufgrund des parlamentarischen Gesetzgebungsverfahrens für die Gründung des BSI sollte die Behörde als vertrauensvoller Partner in der Öffentlichkeit bekannter werden.

Sind die Themen von damals auch noch die Themen von heute?

Hange: Es bestand sicherlich bei jedem IT-Sicherheitskongress der Anspruch, „am Puls der Zeit“ aktuelle Fachthemen aufzugreifen. Der Wandel der Themen war stets bestimmt durch die rasante technologische Entwicklung und die sich verschärfende Bedrohungslage vom Goldfischteich in den Neunzigern zum heutigen Haifischbecken. Beim ersten IT-Sicherheitskongress stand neben der Kryptografie die Zertifizierung nach internationalen Standards für die Hersteller von IT-Produkten besonders im Fokus. Wegen des damit verbundenen Eingriffs in den Wettbewerb musste für die Zertifizierung eine rechtliche Grundlage im BSI-Gesetz geschaffen werden. Die Vorstellung des ersten IT-Grundschutzhandbuches auf dem Kongress 1992 zählt sicher zu den thematischen Meilensteinen in der Fortentwicklung der Veranstaltung. Mit dem Grundschutzhandbuch wurde über die Bundesverwaltung hinaus auch in der Wirtschaft ein Standard für das IT-Sicherheitsmanagement gesetzt. Der Loveletter-Virus sorgte im Jahr 2000 dafür, dass das Thema Internetsicherheit beim Einsatz im privaten Bereich stärker in das Kongressprogramm aufgenommen wurde. Der Kongress war zugleich ein Forum für Diskussionen, die z. B. im Vorfeld der Einführung gesetzlicher Initiativen zur IT-Sicherheit – wie bei den hoheitlichen Dokumenten – geführt wurden. Im Laufe der Jahre wurden neben der technischen Fach-Community immer differenzierter unterschiedliche Zielgruppen angesprochen und sensibilisiert. Zudem wurde nachhaltig die Zusammenarbeit der relevanten Stakeholder gefördert.

Ein Zitat aus dem Tagungsband von 2003 lautet „verteilte Kräfte für ein gemeinsames Ziel zu bündeln“ – der aktuelle IT-Sicherheitskongress trägt das Motto „Kooperation gewinnt“: Warum sind Kooperation und Netzwerken für die Informationssicherheit bis heute so wichtig?

Hange: Kooperation und Informationsaustausch sind in der Cybersicherheit unerlässlich. Der IT-Sicherheitskongress ist

„Der IT-Sicherheitskongress ist bis heute als Plattform für einen Austausch über die Breite von IT-Sicherheitsthemen konzipiert – und das mit dem Anspruch, bei jeder Ausgabe auf dem neuesten Stand der Erkenntnisse zu sein.“

bis heute als Plattform für einen Austausch über die Breite von IT-Sicherheitsthemen konzipiert – und das mit dem Anspruch, bei jeder Ausgabe auf dem neuesten Stand der Erkenntnisse zu sein. Das BSI bringt sich mit fachlicher Expertise ein und legt zugleich Wert auf die Mitwirkung von Fachleuten aus Wissenschaft, Wirtschaft und Verwaltung, damit sie ihre aktuellen Lösungen vorstellen. Das heutige Onlineformat hat den Vorteil, dass inzwischen mehrere Tausend Interessierte kostenfrei die Vorträge verfolgen können.

Welche Rolle spielt der Beirat für den Kongress?

Hange: Mit Fachleuten aus Wissenschaft, Wirtschaft und Verwaltung steht der Beirat für die Unabhängigkeit der Kongressinhalte, einzelne Beiratsmitglieder bringen bereits seit Jahrzehnten ihre Expertise in das Programm ein. Der Kongressbeirat legt gemeinsam mit Verantwortlichen aus dem BSI das Programm fest, bewertet und wählt die eingereichten Vorträge aus. Bereits auf dem ersten Kongress wurde deutlich, dass kein BSI-zentriertes Meinungsbild vermittelt wird, sondern das Fachwissen aus der Fachcommunity die Veranstaltung prägt.

Verraten Sie uns ein Highlight aus den ersten Jahren?

Hange: Ich erinnere mich noch gut an meinen ersten Vortrag, den ich beim IT-Sicherheitskongress im Jahr 1991 gehalten habe. Es war ein Vortrag zum Thema Kryptologie vor einem Publikum, das teilweise keine spezielle Kenntnis der Materie hatte. In der Vorbereitung wurde mir natürlich bewusst, dass es weniger auf das Vermitteln der Kryptologie in der Tiefe ankommt als um einen Vortrag mit verständlichen Botschaften zu kryptografischen Konzepten und deren Einsetzbarkeit – auch für normale IT-Anwendende. Es war eine echte Herausforderung, den üblichen „kryptischen“ Jargon mit vielen Fachbegriffen zu vermeiden. Das ist sicher bis heute für jeden Vortragenden eine Herausforderung und man lernt es dann in der Praxis.

Was ist das Erfolgsgeheimnis des Deutschen IT-Sicherheitskongresses?

Hange: Zum einen die gute fachliche Vorbereitung der Vortragsthemen und -slots. Die Themenauswahl ist wie ein Brennglas auf die aktuellen und drängenden Fragestellungen und Probleme in der IT- und Cybersicherheit. Zum anderen die qualifizierte Organisation des Kongresses, das wussten besonders die Aussteller zu schätzen. Darüber hinaus ist auch Networking ein entscheidender Faktor des Kongresses. Trafen sich die Teilnehmenden ehemals noch persönlich in der Stadthalle Bad Godesberg, so ist der Kongress inzwischen das größte digitale Klassentreffen zur Cybersicherheit in Deutschland.

Was wünschen Sie dem Deutschen IT-Sicherheitskongress?

Hange: Ich wünsche dem BSI, dass es auch mit den kommenden Ausgaben des Kongresses weiterhin die relevanten Themen für die unterschiedlichsten Zielgruppen adressiert und den erfolgreichen kooperativen Ansatz weiterverfolgt.

Sie sind schon länger im Ruhestand: Verfolgen Sie den Kongress online?

Hange: Der Kongress hat sich mit dem Live-Format sicherlich verändert, aber ich finde ihn nach wie vor sehr spannend. Inzwischen bin ich ja auch schon einige Jahre aus dem Tagesgeschäft raus. Ich verfolge aber weiterhin als IT-Anwender mit Interesse einzelne Vorträge bei dem Onlinkongress. ■

BSI-Marktaufsicht – für mehr IT-Sicherheit am Verbrauchermarkt

Blick hinter die Kulissen: Wie sich die Zusammenarbeit der BSI-Marktaufsicht mit den Herstellern gekennzeichneter Produkte gestaltet

von Inke Gelfert und Daisy Kunze, Referat Marktaufsicht über zertifizierte Dienstleister und Produkte

Was tun, wenn Sicherheitslücken bei einem Produkt bekannt werden? Wie läuft eine anlasslose technische Konformitätsüberprüfung? Die BSI-Marktaufsicht gewährt Einblicke in die Abläufe rund um das neue IT-Sicherheitskennzeichen, mit dem Hersteller und Dienstanbieter ihre IT-Produkte auszeichnen. Sie sichern damit zu, dass bestimmte Sicherheitseigenschaften vorhanden sind.

Bereits vor der Beantragung des IT-Sicherheitskennzeichens muss ein Hersteller sein Produkt auf Konformität mit den Sicherheitsanforderungen des BSI testen. Dazu liefert er wesentliche technische Angaben zum Produkt und beschreibt detailliert, welche Methoden und Verfahren er bei der Konformitätsprüfung angewendet hat. Auf dieser Basis beurteilt das BSI, ob die Angaben ausreichend belegt und aktuelle Sicherheitslücken bekannt sind. Da sich die Sicherheitsmerkmale von IT-Produkten im Lauf der Zeit verändern können, prüft das BSI die Produkte aber nicht zu einem Stichtag, sondern beaufsichtigt sie über die gesamte Laufzeit des Kennzeichens durch die BSI-Marktaufsicht. Der effiziente Antragsprozess in Kombination mit der nachgelagerten Marktaufsicht fördert das Vertrauen in das IT-Sicherheitskennzeichen und wird den schnelllebigen Produktzyklen am Verbrauchermarkt gerecht.

Nach der offiziellen Übergabe des IT-Sicherheitskennzeichens an den Antragsteller beginnt die Arbeit der BSI-Marktaufsicht. Sie prüft während der Laufzeit, ob die in der Herstellererklärung zugesicherten Konformitätsangaben bei den gekennzeichneten Produkten eingehalten werden. Das geschieht sowohl anlasslos stichprobenartig als auch anlassbezogen.

EIN IT-SICHERHEITSKENNZEICHEN WURDE ZUR NUTZUNG FREIGEGEBEN – UND NUN?

Für den Zeitraum der Bewilligung erklärt sich der Hersteller bereit, das BSI über mögliche Schwachstellen seiner Produkte zu informieren, Sicherheitsupdates bereitzustellen und die geltenden Sicherheitsanforderungen einzuhalten. Die Marktaufsicht des BSI überwacht diese Sicherheitseigenschaften während der Dauer der Freigabe. Sie überprüft die Produkte auf deren Konformität, reagiert auf Schwachstellenmeldungen und pflegt die Sicherheitsinformationen der Produkte auf der BSI-Website ein. Die Marktaufsicht kann Antragsunterlagen, technische Unterlagen und Herstellerdokumente heranziehen oder Testkäufe durchführen, um die Produkte technisch zu prüfen.

WIE LÄUFT EINE ANLASSLOSE ÜBERPRÜFUNG AB?

Die Marktaufsicht nimmt anlasslos stichprobenartig ausgewählte Produkte genauer unter die Lupe. Dabei erfolgt eine erste technische Vorprüfung entweder durch das BSI oder durch anerkannte Prüfstellen.

Wesentliche Punkte einer anlasslosen Überprüfung sind:

- Kontrolle der Konformität des Produkts mit den zugrunde liegenden IT-Sicherheitsanforderungen, wie etwa den Standards für sichere Breitbandrouter, für sicheren E-Mail-Transport und dem ETSI-Standard für Consumer Internet of Things (IoT)

- Prüfung der Einhaltung der Herstellerpflichten bei Sicherheitslücken nach Meldungen an das BSI

Zusätzlich können gekennzeichnete Produkte einer Tiefenprüfung unterzogen werden. Dabei werden die Testobjekte gezielt in Bezug auf die geforderten Standards für die IT-Sicherheit untersucht. Dies kann beispielsweise auch Penetrationstests oder Schnittstellenprüfungen umfassen, um mögliche Nichtkonformitäten aufzudecken. Die Erkenntnisse aus der Tiefenprüfung werden im Nachgang mit den Kennzeicheninhabern besprochen.

WAS KÖNNEN AUSLÖSER EINER ANLASSBEZOGENEN PRÜFUNG SEIN?

Schwachstellen im Produkt oder in den verwendeten Technologien können Anlass für eine Untersuchung bieten. Manchmal gewinnen Hersteller eigene Erkenntnisse und melden sich oder es gibt Hinweise von Dritten. Im Lagezentrum des BSI laufen verschiedene Sicherheitsinformationen zusammen. Liefern die Erkenntnisquellen sicherheitsrelevante Treffer zu gekennzeichneten Produkten, prüft die Marktaufsicht in Zusammenarbeit mit anderen BSI-Kolleginnen und -Kollegen das mögliche Bedrohungsrisiko.

WAS PASSIERT NACH EINEM SCHWACHSTELLENFUND?

Wenn eine Schwachstelle gefunden wurde, kontaktiert die Marktaufsicht die jeweiligen Hersteller und Dienstanbieter. Häufig ergibt sich ein enger Austausch, der zur zügigen Bereitstellung des notwendigen Updates führt. Nach den bisherigen Erfahrungen sind die Kennzeicheninhaber sehr darum bemüht, die Sicherheit ihrer Produkte aufrechtzuerhalten.

WELCHE BISHERIGEN ANLÄSSE HABEN BEISPIELSWEISE EINE SOLCHE ANLASSBEZOGENE ÜBERPRÜFUNG INITIIERT?

Ein Anlass, um mit den E-Mail-Dienstanbietern Kontakt aufzunehmen, war z. B. die Schwachstelle „Simple Mail Transfer Protocol (SMTP) Smuggling“. Bei dieser machen es sich Angreifer zunutze, dass verschiedene SMTP-Implementierungen die Kennzeichnung des Endes einer E-Mail-Nachricht unterschiedlich interpretieren. So können gefälschte E-Mails versendet (Spoofing) und sogar Authentifizierungsmechanismen umgangen werden. Auch wirken Warnungen, wie z. B. eine Spam-Markierung in der Betreffzeile, nicht mehr.

Ein weiterer Anlass, als Marktaufsicht tätig zu werden, war die Terrapin-Sicherheitslücke. Diese kann bei Routern verschlüsselte Secure-Shell-(SSH-)Verbindungen schwächen, sodass ein Angreifer per Man-in-the-Middle-Attacke Daten aus einer abgesicherten SSH-Verbindung löschen könnte, um die Sicherheit der Verbindung herabzusetzen.

Die BSI-Marktaufsicht hat im gemeinsamen Austausch mit den Herstellern geprüft, ob die gekennzeichneten Produkte tatsächlich betroffen waren. War dies der Fall, wurde die Schwachstelle zügig vom Hersteller behoben.

WIE WERDEN VERBRAUCHERINNEN UND VERBRAUCHER INFORMIERT?

Nach Bereitstellung der Updates aktualisiert das BSI die jeweilige Produktinformationsseite für Verbraucherinnen und Verbraucher. Der schnellste Weg dorthin ist das Scannen des QR-Codes auf dem IT-Sicherheitskennzeichen. Die Produktinformationsseite beinhaltet verbraucherfreundlich aufbereitete Informationen über die Sicherheitseigenschaften des Produkts oder bekannt gewordene Schwachstellen. ■

Weitere Informationen:

www.bsi.bund.de/it-sik/hersteller

Für ein gesundes #TeamBSI

Beim BSI setzen wir auf Prävention – bei der Cybersicherheit ebenso wie bei der Gesundheit unserer Mitarbeitenden

von Kirsten Kampmann und Miriam List, Referat Personalentwicklung

Im BSI steht die körperliche und mentale Gesundheit der Mitarbeitenden im Fokus. Unser umfassendes Gesundheitsmanagement geht weit über die bewegte Pause hinaus – wir verfolgen einen ganzheitlichen Ansatz und verzahnen Maßnahmen auf vielen Ebenen. Unser Ziel ist, sowohl die Gesundheit als auch die Zufriedenheit und Motivation der Mitarbeitenden zu fördern.

Die vielfältigen Anforderungen und die Schnelllebigkeit der heutigen Arbeitswelt sowie im Privatleben stellen auch eine Herausforderung für die Gesundheit dar. Daher setzen wir im BSI mit dem Motto Gesundes #TeamBSI auf ein ganzheitliches Gesundheitsmanagement, das mehr ist als die Teilnahme am Firmenlauf. Die Gesundheit steht für uns an erster Stelle, denn nur mit gesunden Mitarbeitenden können wir die Cybersicherheit in Deutschland voranbringen. Im BSI werden mentale und körperliche Gesundheit auf allen Ebenen und in allen Prozessen mitbedacht – etwa bei der Personalentwicklung, die Strategien und Maßnahmen in den Bereichen Gesundheitsmanagement, Führung, lebenslanges Lernen und interne Zusammenarbeit verzahnt. Denn motivierte Mitarbeitende, die sich vom Arbeitgeber BSI wertgeschätzt fühlen, sind leistungsstark und erhöhen das Innovationspotenzial.

BETEILIGUNG ALLER MITARBEITENDEN: DER SCHLÜSSEL ZU MASSGESCHNEIDERTEN LÖSUNGEN

Im BSI fördern wir die Partizipation der Beschäftigten und wechselseitige Kommunikation. Wie auch bei unserer Aufgabe, Staat, Wirtschaft und Gesellschaft für Cybersicherheit zu sensibilisieren und gleichzeitig zu stärken, setzen wir im Gesundheitsmanagement auf das Prinzip Prävention, Detektion und Reaktion. Deshalb befragen wir alle Mitarbeitenden regelmäßig zu Themen, die einen besonderen Einfluss auf die Gesundheit im Arbeitskontext haben. Dabei geht es um Führung, soziale Beziehungen, Zugehörigkeitsgefühl und sinnstiftende Arbeitsaufgaben. Wir erfassen die Einschätzungen der Mitarbeitenden systematisch und können dadurch Verbesserungspotenziale sichtbar machen. Verbesserungsmaßnahmen werden – teilweise auch abteilungsspezifisch – umgesetzt. Jedoch dienen nicht nur diese Handlungsfelder als wichtiges Fundament. Die Befragungen zeigen auch Stärken und Ressourcen im BSI auf, die wir für die Gestaltung eines gesunden Arbeitsumfeldes nutzen. Diese Form der Einbeziehung der Beschäftigten ermöglicht es uns, die Arbeitsbedingungen kontinuierlich zu verbessern und somit zu einem gesunden #TeamBSI beizutragen.

„Wir legen im BSI großen Wert auf eine Kultur der Wertschätzung und Partizipation. Denn nur in einem Umfeld, das auf gegenseitigem Respekt und Verständnis basiert, können wir langfristig das Wohlbefinden und die Leistungsfähigkeit unseres Teams fördern. Gesundheit ist mehr als nur das Fehlen von Krankheit – sie ist ein ganzheitlicher Zustand auf mentaler, körperlicher und sozialer Ebene. Im betrieblichen Gesundheitmanagement unterstützen wir dies durch die Gestaltung von gesunden Rahmenbedingungen und geben Impulse zur bewussten Auseinandersetzung mit der eigenen Gesundheit.“

Kirsten Kampmann, Gesundheitsmanagement

„Resilienz stärken ist nicht nur in der IT-Welt von Bedeutung, sondern auch in Bezug auf die Gesundheit unserer Mitarbeitenden.“

Claudia Plattner, BSI-Präsidentin

In einer Kurzumfrage, der Pulsbefragung, haben wir beispielsweise um eine Einschätzung zu der eigenen psychischen Gesundheit in der digitalen Zusammenarbeit gebeten. Erfreuliches Ergebnis: Besonders die Vereinbarkeit von Beruf und Privatleben wird von 85 Prozent der Mitarbeitenden als positiv bewertet. Die Vermutung, aufgrund der digitalen Arbeitsweise entstehe ein Gefühl der sozialen Isolation, hat sich glücklicherweise nicht bewahrheitet – Teamzusammenhalt und soziale Interaktionen sind nicht nur auf persönliche Begegnungen beschränkt. Gleichzeitig wurde aber auch deutlich, dass die hybride Arbeitswelt mit neuen Herausforderungen verbunden ist. Darauf reagieren wir mit verschiedenen Ansätzen in der Zusammenarbeit.

Selbstverständlich und unerlässlich ist für uns die aktive Beteiligung der Führungskräfte. Sie sind ein großer Stellhebel und haben aufgrund ihrer Wirkungsbreite einen großen Einfluss – insbesondere die oberste Leitungsebene. So treffen sich beispielsweise alle Abteilungsleitungen zweimal im Jahr, um über gesundheitsrelevante Aktivitäten und Prozesse zu beraten und konkrete Maßnahmen zu beschließen.

VIELFÄLTIGE MASSNAHMEN ZUR GESUNDHEITSFÖRDERUNG

Neben den strukturellen Ansätzen im Gesundheitsmanagement ist uns ein gesundes Arbeitsumfeld wichtig. Uns sind auch die Stärkung des individuellen Gesundheitsbewusstseins und die Unterstützung von gesunden Arbeits- und Verhaltensweisen ein Anliegen.

Aufgrund unserer überwiegend sitzenden Tätigkeit ist es wichtig, Bewegung in den Alltag zu integrieren. Dafür haben wir verschiedene Angebote:

- **digitale bewegte Pause**
- **elektrisch höhenverstellbare Schreibtische**
- **jährliche Teilnahme an den Firmenläufen in Bonn, Dresden und Saarbrücken**
- **jährliche Schritte-Challenge**
- **Kooperation mit einem Gesundheitsanbieter**

Ergänzend zu den sportlichen Angeboten organisieren wir informative Impulsvorträge zu verschiedenen Gesundheitsthemen. Neben dem Präventionsgedanken geht es uns auch um Wissensvermittlung und Kompetenzerweiterung in den Bereichen:

- **mentale Gesundheit (z. B. Umgang mit Stress)**
- **gesunde Ernährung**
- **Vereinbarkeit von Beruf und Familie**

Zur Prävention zählt auch die kostenfreie Grippeschutzimpfung an unseren Standorten. Damit schützen wir die Gesundheit unserer Mitarbeitenden und beugen Krankheitsausfällen vor. Neben allen strukturellen und organisationsübergreifenden Maßnahmen dürfen die individuellen Bedürfnisse und Herausforderungen der einzelnen Mitarbeitenden nicht zu kurz kommen. Bei persönlichen Angelegenheiten oder in schwierigen Lebenssituationen bietet unsere Sozialberaterin vom Bundesministerium des Innern und für Heimat allen Mitarbeitenden ein offenes Ohr und kann kompetent beraten. Auch das betriebliche Eingliederungsmanagement bietet individuelle Hilfestellung nach einer längeren Erkrankung an.

„Das Angebot der Sozialberatung und das betriebliche Eingliederungsmanagement greifen die individuellen Bedürfnisse der Beschäftigten auf. Dabei wird auf die besondere Situation der betroffenen Person eingegangen und gemeinsam Lösungsansätze erarbeitet.

Diese individuellen Gespräche liefern uns gleichzeitig wertvolle Erkenntnisse für die gesamte Organisation. So können wir diese bündeln und mit anderen Themenbereichen, wie z. B. dem Arbeitsschutz oder der Führungskräfteentwicklung, verzahnen."

Miriam List, Gesundheitsmanagement

„Wir alle wissen gute Gesundheit oft erst dann zu würdigen, wenn sie beeinträchtigt ist. Gesundheit ist ein hohes Gut, das wir schützen sollten! Nicht nur lebt es sich privat gesund besser, sondern Gesundheit wirkt sich auch positiv auf unsere Leistungsfähigkeit aus!"

Sandro Amendola, Abteilungsleiter SZ

EIN GESUNDES #TEAMBSI IST AUCH EIN LEISTUNGSFÄHIGES UND INNOVATIVES #TEAM BSI

Wir betrachten das Gesundheitsmanagement als eine Investition in die Entwicklung unserer Mitarbeitenden und somit in den langfristigen Erfolg des BSI. Mitarbeitende gezielt einbinden, vielfältige Gesundheitsmaßnahmen implementieren und eine gesunde Zusammenarbeit aktiv fördern, das sind die höchsten Ziele der Personalentwicklung. So schaffen wir ein Arbeitsumfeld, in dem sich alle wohlfühlen und somit ihr volles Potenzial entfalten können. Gesunde und motivierte Mitarbeitende sind nicht nur produktiver und innovativer, sondern auch leistungsfähiger und zufriedener. Das BSI bleibt am Puls der Zeit, um die Bedürfnisse des #TeamBSI zu verstehen und die Arbeitsbedingungen kontinuierlich zu optimieren. Gemeinsam gestalten wir eine gesunde und erfolgreiche Zukunft – denn Gesundheit ist nicht nur ein Versprechen, sondern unsere gelebte Realität.

Gesundes #TeamBSI: Gemeinsam stark für eine gesunde Zukunft! ■

Weitere Informationen:

https://www.bsi.bund.de/DE/Karriere/Arbeiten-im-BSI/Einblicke/Ein-Tag-im-BSI/Tagesablaeufe/Kirsten_Kampmann/Kirsten_Kampmann_node.html

Vor mir liegen viele Aufgaben. Hinter mir steht ein ganzes Team.

Ihr wollt mit eurem Team aufs Ganze gehen?
Dann seid ihr bei uns genau richtig. Kommt ins **#TeamBSI.**

Bundesamt
für Sicherheit in der
Informationstechnik

Mehr Infos auf:

www.team-bsi.de

30 Jahre IT-Grundschutz: 30 Jahre Informationssicherheit

Ein kleiner Blick zurück, ein großer nach vorne in die Zukunft

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

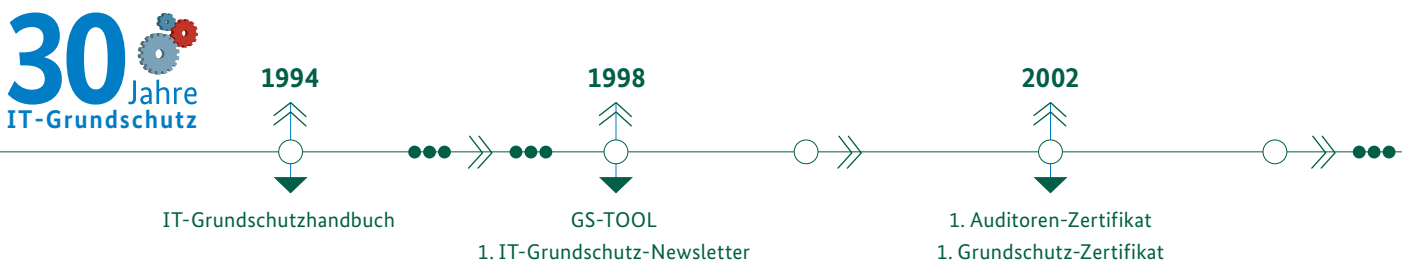
Vor 30 Jahren hat das BSI erstmals IT-Sicherheitsempfehlungen unter dem Namen „IT-Grundschutz“ veröffentlicht – ein Meilenstein in der Geschichte der Informationssicherheit. Der IT-Grundschutz bleibt dem eigenen Leitgedanken folgend dynamisch: Informationssicherheit ist kein Status, sondern ein Prozess. Wir werfen einen kurzen Blick in die Vergangenheit, bevor es in die Zukunft geht.

Drei Jahrzehnte sind schon in der analogen Welt eine lange Zeit – in der digitalen sind sie eine Ewigkeit. Dementsprechend viele Veränderungen kennt der IT-Grundschutz, seit im Jahr 1994 die erste Ausgabe des IT-Grundschutzhandbuches herauskam. Der IT-Grundschutz zeigt sich von jeher dynamisch, ob in seinen Anfängen, als das Internet zum Massenphänomen wurde, oder heute, wenn es um die fortschreitende Entwicklung der Digitalisierung in Behörden und Unternehmen geht, wenn sich Teilbereiche wie etwa die Künstliche Intelligenz (KI) rapide weiterentwickeln, und vor allem, wenn die Vision einer Cybernation Deutschland Realität werden soll. Der IT-Grundschutz hat sich als national und international anerkannter Standard im Bereich Informationssicherheit etabliert.

Der Grundgedanke war von Anfang an, IT-Sicherheitsempfehlungen möglichst praxisnah und flexibel zu gestalten. Anwendende erhielten mit einem modularen Baukastenkonzept Hilfe zur Selbsthilfe. Los ging es mit einer FAQ-Liste und 15 Pilot-IT-Grundschutz-Bausteinen. In diesen Bausteinen werden jeweils für einen bestimmten Aspekt der Informationssicherheit (z. B. zum Einsatz von Servern) typische Gefährdungen und in den Anfängen des IT-Grundschutzes Sicherheitsmaßnahmen und ab dem IT-Grundschutz-Kompendium Anforderungen beschrieben. Über die Jahre ist daraus eine umfassende und aktuelle Zusammenstellung von Methoden, Empfehlungen und Standards geworden. Kommunen sowie Landes- und Bundesbehörden arbeiten ebenso damit wie lokale Handwerksbetriebe, Mittelständler und DAX-Konzerne.

Darüber hinaus wurde die Möglichkeit geschaffen, mithilfe von Zertifikaten und Testaten Informationssicherheit gegenüber Kundinnen und Kunden, Dienstleistern und Mitarbeitenden nachzuweisen. Ein ISO 27001-Zertifikat nach IT-Grundschutz belegt bis heute den hohen Stellenwert der Informationssicherheit in einer Institution.

Praxisnähe und Flexibilität sind gegenwärtig grundlegende Elemente des IT-Grundschutzes und werden es auch in Zukunft sein. Allein das Entwicklungstempo in der Informationssicherheit erfordert, dass der IT-Grundschutz kontinuierlich aktualisiert wird. Der folgende Aus- und Überblick stellt die aktuell wichtigsten Projekte und Vorhaben vor.



Über den IT-Grundschutz

Der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist ein bewährtes Verfahren, um das Niveau der Informationssicherheit in Behörden und Unternehmen jeder Größenordnung zu erhöhen. Die Angebote des IT-Grundschutzes gelten in Verwaltung und Wirtschaft als Maßstab, wenn es um die Absicherung von Informationen und den Aufbau eines Managementsystems für Informationssicherheit (ISMS) geht. Ein systematisches Vorgehen ermöglicht es, notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards liefern hierzu bewährte Vorgehensweisen. Das IT-Grundschutz-Kompendium formuliert mit den IT-Grundschutz-Bausteinen konkrete Anforderungen.

VERÖFFENTLICHUNG DES SCHULUNGSKONZEPTES BCM-PRAKTIKER

Ob ein Rechenzentrum ausfällt, eine Produktionsstätte infolge eines Naturereignisses zerstört wird oder ob es eine Cyberattacke auf die gesamte IT-Infrastruktur gibt – Behörden und Unternehmen sind einer stetig wachsenden Zahl an potenziellen Gefahren ausgesetzt, die zu einer existenzbedrohenden Unterbrechung des Geschäftsbetriebes führen können.

Wie kann man sich schützen? Unter anderem gewinnt das Business Continuity Management (BCM) zunehmend an Bedeutung. BCM ist neben dem Informationssicherheits- und Krisenmanagement das Werkzeug für organisatorische Resilienz. Vielen Anwenderinnen und Anwendern fällt es jedoch noch schwer, ein passendes Business-Continuity-Management-System (BCMS) zu planen und strukturiert aufzubauen. Der Bedarf an qualifiziertem Personal, das eine Implementierung kompetent mit Empfehlungen und konkreten Maßnahmen begleiten kann, ist hoch.

Das BSI hat die Antwort auf diesen Bedarf: 2023 wurde der modernisierte BSI-Standard 200-4 BCM vorgestellt. Basierend darauf hat das BSI ein neues Schulungskonzept zum BCM-Praktiker entwickelt. Seit Anfang des Jahres 2024 kann die Schulung bei kooperierenden Schulungsanbietern belegt werden.

Die Schulung BCM-Praktiker stellt eine Ergänzung zum IT-Grundschutz-Praktiker und -Berater dar und richtet sich an Business-Continuity-Beauftragte (BC-Beauftragte) und BC-Interessierte. Sie vermittelt grundlegende Kenntnisse des gesamten BCMS-Prozesses nach dem BSI-Standard 200-4 und wird ergänzt durch praktische Beispiele und Erläuterungen.

Weitere Informationen:

https://www.bsi.bund.de/dok/BCM-Praktiker

2003

Leitfaden IT-Sicherheit – IT-Grundschutz kompakt
1. IT-Grundschutz-Tag
Webkurs IT-Grundschutz
IT-Grundschutz als Basis für Informationssicherheit in Estland

2005

BSI-Standards und IT-Grundschutz-Kataloge
Webkurs GSTOOL
1. ISO 27001-Zertifikat auf der Basis von IT-Grundschutz

2008

BSI-Standard 100-4

2009

Webkurs Notfallmanagement

30 Jahre IT-Grundschutz

„Was auch immer im Bereich der Digitalisierung und Informationstechnik passieren mag, der IT-Grundschutz wird dynamisch bleiben und darauf reagieren.“

Holger Schildt, seit 2017 Referatsleiter von SZ 13

REDUZIERUNG VON DOKUMENTATIONSAUFWÄNDEN

In 2023 wurde ein Projekt zu den Dokumentationsaufwänden bei der Etablierung eines Managementsystems für Informationssicherheit (ISMS) im IT-Grundschutz durchgeführt. Ziel ist es, die Dokumentationsaufwände zukünftig auf das notwendige Minimum zu reduzieren. Dazu wurden die derzeit geforderten Aufwände im Hinblick auf ihre Notwendigkeit überprüft. Gleichzeitig wurden die bisherigen Vorgaben zur Dokumentation harmonisiert, um zukünftig mehr Klarheit für die Umsetzung unter Beibehaltung der Freiheit in der tatsächlichen Ausgestaltung zu ermöglichen.

Bereits in 2024 werden den Anwendenden erste aus dem Projekt entwickelte Hilfsmittel zur Verfügung gestellt. Somit wird eine erste Reduzierung der Dokumentationsaufwände im IT-Grundschutz zeitnah möglich sein.

SPANNUNGSFELD KONTINUITÄT UND WANDLUNGSFÄHIGKEIT: EIN AUSBLICK

Der IT-Grundschutz wird fortlaufend weiterentwickelt, sowohl um mit der technischen Weiterentwicklung mitzuhalten als auch um den Bedürfnissen der Anwendenden Rechnung zu tragen. Schließlich ist es ein Ziel des BSI, die Resilienz von Unternehmen und Behörden zu erhöhen und Informationssicherheit pragmatisch zu gestalten. Dabei bewegt sich der IT-Grundschutz in einem interessanten Spannungsfeld. Denn einerseits ist Kontinuität in der Gestaltung ganzheitlicher, prozessualer Informationssicherheit unerlässlich. Andererseits erfordert die sprunghafte Weiterentwicklung im digitalen Bereich auch vom IT-Grundschutz eine hohe Wandlungsfähigkeit. Zudem wünschen sich viele Anwendende weitere Vereinfachungen – ein anspruchsvoll umzusetzender Wunsch für ein komplexes Thema. Wer ganzheitliche Informationssicherheit anstrebt, z. B. durch den Aufbau eines vollumfänglichen ISMS, hat einen zeit- und ressourcenaufwendigen Prozess zu bewältigen.

2012

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

2016

IT-Grundschutz-Kataloge umfassen
100 Bausteine

2017

BSI-Standards 200-1, 200-2 und 200-3
IT-Grundschutz-Kompendium
1. IT-Grundschutz-Profil

Fakten zum IT-Grundschutz

- Der erste IT-Grundschutz bestand aus einer FAQ-Liste.
- 2017 wurden die Ergebnisse einer grundlegenden Modernisierung des IT-Grundschutzes vorgestellt. Die Inhalte wurden fokussiert und verschlankt, neue Themen, Vorgehensweisen und IT-Trends wurden aufgenommen.
- Die aktuelle Version des IT-Grundschutzes enthält vier BSI-Standards und 111 IT-Grundschutz-Bausteine im IT-Grundschutz-Kompendium.
- 35.985 Abonnenten beziehen den IT-Grundschutz-Newsletter und 14.680 Abonnenten erhalten durch den BCM-Newsletter Informationen über aktuelle Neuheiten.
- Aktuell sind auf der BSI-Website 19 IT-Grundschutz-Profile zu unterschiedlichen Anwendungsszenarien verfügbar.
- Das BSI hat Schulungskonzepte für den IT-Grundschutz-Praktiker, den IT-Grundschutz-Berater und den BCM-Praktiker entwickelt.

All das sind Herausforderungen, denen sich der IT-Grundschutz auch in Zukunft stellt. Der IT-Grundschutz wird agil weiterentwickelt mit den Zielen, den Umfang und die bei der Umsetzung entstehenden Dokumentationsaufwände auf das notwendige Mindestmaß zu reduzieren, eine Priorisierung der Anforderungen vorzunehmen sowie die Anwendung von Automatisierungstools weitestgehend zu ermöglichen. Die erste Version des weiterentwickelten IT-Grundschutzes wird in der Einführung eines Nachfolgers des IT-Grundschutz-Kompendiums bestehen. Parallel zu dieser Überarbeitung wird die Edition 2023 des IT-Grundschutz-Kompendiums je nach Bedarf und Notwendigkeit weiter gepflegt und gegebenenfalls um neue Bausteine ergänzt. Die Pilotierung des weiterentwickelten IT-Grundschutz-Kompendiums ist für Ende 2024/Anfang 2025 geplant. In einer mehrjährigen Übergangszeit werden der aktuelle IT-Grundschutz und Versionen des weiterentwickelten IT-Grundschutzes nebeneinander bestehen und anwendbar bleiben. Die erfolgreiche Umsetzung von IT-Grundschutz soll auch messbar werden, zudem sind stärkere Synergien mit weiteren BSI-Vorgaben geplant.

Gleichzeitig werden gewonnene Erkenntnisse aus den vergangenen Projekten in die Weiterentwicklung einfließen. Erfahrungswerte aus der Projektgruppe „Wege in die Basis-Absicherung“ zeigen z. B., dass es zum einen ein erfreuliches Interesse an Informationssicherheit gibt, zum anderen jedoch auch der Bedarf besteht, die Praxisorientierung des IT-Grundschutzes weiter zu erhöhen. ■

Sie wollen über aktuelle Neuigkeiten aus dem IT-Grundschutz informiert werden? Dann abonnieren Sie unseren IT-Grundschutz-Newsletter:

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

2018

Online-Kurs zum modernisierten IT-Grundschutz
1. ISO 27001-Zertifikat auf der Basis von IT-Grundschutz nach dem IT-Grundschutz-Kompendium

2019

Testat nach der Basis-Absicherung
IT-Grundschutz-Praktiker und -Berater

2023

BSI-Standard 200-4

2024

BCM-Praktiker

Mobiles Arbeiten auch in Zukunft sicher

Moderne Plattformlösungen ermöglichen ein lebendiges App-Ökosystem für Verschlusssachen

von Lars Bruchhaus, Jan Metzke und Yvonne Omlor, Referat Produkte und Systeme für Verschlusssachen (VS-IT)

Wer wollte darauf verzichten? Mobiles Arbeiten hat die Arbeitswelt in vielen Branchen revolutioniert – Mitarbeitende entscheiden oft selbst, wie, wann und wo sie arbeiten. Mobile Anwendungen machen's möglich. Allerdings müssen auch beim flexiblen Arbeiten Vertraulichkeit, Verfügbarkeit und Integrität gewährleistet sein. In Zukunft werden Plattformlösungen und App-Ökosysteme noch mehr Flexibilität erlauben und die Funktionspalette signifikant erweitern.

Die mobile Kommunikation gehört zu den besonders innovativen und sich rasant entwickelnden Bereichen der IT-Branche. „New Normal" heißt, es wird erwartet, dass die Arbeit überall und jederzeit erledigt werden kann. Das gelingt mit mobilen Endgeräten, die dank einfach zu installierender Apps und aufgrund ihrer Leistungsfähigkeit zu universellen Werkzeugen geworden sind.

Diese Entwicklung birgt jedoch auch Risiken: Gehen mobile Geräte verloren oder werden sogar gestohlen, sind potenziell vertrauliche Daten gefährdet. Auch Missbrauch und Manipulation der Geräte sind ein Risiko, z. B. wenn Nutzende unbemerkt überwacht werden.

SICHER MOBIL IN DER BUNDESVERWALTUNG

Das BSI arbeitet seit vielen Jahren mit verschiedenen Herstellern an Lösungen für die Bundesverwaltung zum sicheren mobilen Arbeiten, einschließlich mit Verschlusssachen bis zum Einstufungsgrad VS – NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD). Bei diesen Lösungen wird der klassische sicherheitstechnische Dreiklang umgesetzt: „Data at Rest" – sichere Speicherung auf den Endgeräten, „Data in Use" – Sicherheit bei der Arbeit mit den Daten und „Data in Transit" – sichere Anbindung ans Backend. Mit einem Mobile Device Management werden die Endgeräte verwaltet und sicher konfiguriert.

Obwohl mobile Betriebssysteme oft über gute Sicherheitsmechanismen verfügen, sind diese aufgrund der Komplexität der Systeme und der hohen Entwicklungsdynamik ohne eine enge Zusammenarbeit mit den Herstellern schwer zu bewerten. Daher waren Hersteller sicherer mobiler Lösungen bisher häufig gezwungen, eigene Sicherheitsmechanismen für Produkte wie SecurePIM Government SDS oder SecuSUITE for Samsung Knox zu entwickeln. Auf diese Weise lässt sich ein hohes, nachweisbares Sicherheitsniveau erreichen, funktionale Erweiterungen stellen sich jedoch oft als aufwendig und schwierig umsetzbar heraus.

Deshalb hat das BSI in den vergangenen Jahren die Zusammenarbeit mit den Herstellern Apple und Samsung ausgebaut und native Sicherheitsfunktionen in den Plattformen iOS/iPadOS und Samsung Knox evaluiert. Diese überprüfte Plattformsicherheit ist die Basis für die Lösungen „indigo" und perspektivisch „Knox Platform for Enterprise Knox Native Solution" (Knox Native).

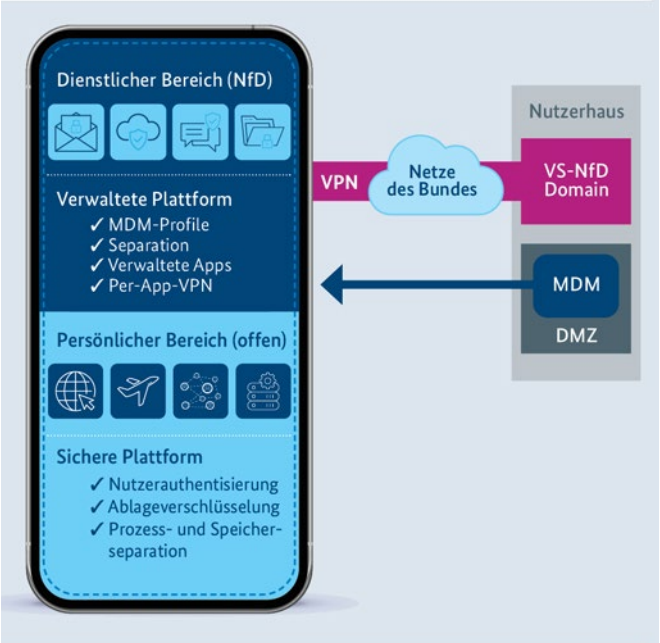


Abbildung 1: Sichere mobile Plattform: Zielarchitektur

PLATTFORMLÖSUNGEN: INDIGO UND KNOX NATIVE

Native Sicherheitsfunktionen bilden das Fundament für die Lösungen indigo und Knox Native. Beide ermöglichen bereits einen abgesicherten Zugriff auf E-Mails, Kalender und Kontakte auf VS-NfD-Niveau über die vorinstallierten nativen Apps. Darüber hinaus bietet indigo eine VS-NfD-konforme S/MIME-Verschlüsselung und Knox Native Zugriff auf Notizen. Die zugrunde liegende Verschlüsselung basiert bei indigo auf dem nativ verbauten Sicherheitsanker von Apple, der Secure Enclave, während Knox Native auf ein gemeinsam mit dem BSI entwickeltes Java Card Applet setzt, das im zertifizierten embedded Secure Element von Samsung ausgeführt wird. Die Trennung zwischen persönlichen und dienstlichen Apps wird ermöglicht durch die Separationsmechanismen des Betriebssystems sowie eine evaluierte, native VPN-Technologie (Abb. 1).

Die nativen Sicherheitsfunktionen schonen nicht nur das interne Netz und verbessern die Akkulaufzeit. Sie schaffen auch ein Erlebnis, wie Nutzende es von ihren privaten Endgeräten kennen. Durch ihre Skalierbarkeit bilden native Sicherheitsfunktionen außerdem die Basis eines lebendigen Ökosystems, das sukzessive und kontinuierlich den Funktionsumfang der mobilen Lösungen durch die dynamische Aufnahme zusätzlicher sicherer Apps erweitert.

AUSBLICK: AUFBAU EINES APP-ÖKOSYSTEMS

Mit TrustOwl & SecuFOX als Intranet-Browser und SecuOFFICE & TrustDok für die Dokumentenverarbeitung sind erste Apps verfügbar, die sich auf die nativen Sicherheitsmechanismen der indigo-Plattform stützen. Zusätzlich stehen Nutzenden der freigegebenen indigo-Lösung die Apps Wire und SecuVOICE für sichere Kommunikation zur Verfügung. Auch die parallele Weiternutzung bisheriger Lösungen wie etwa SecurePIM im Sinne einer sanften Migration ist möglich.

Durch Nutzung geprüfter Sicherheitsfunktionen können zukünftig auch weitere bereits verfügbare Apps und Eigenentwicklungen für die Bundesverwaltung bereitgestellt werden. Hierzu entwickelt das BSI mit einer Prüfstelle einen leicht zugänglichen Prozess (Abb. 2). Sowohl die bereits existierenden Apps als auch die Eigenentwicklungen werden einer Prüfung unterzogen. Dabei wird die korrekte Nutzung der bereits evaluierten Sicherheitsfunktionen nachgewiesen. Zusätzlich werden valide Prozesse zur Fehlerbehebung und zum Lifecycle sichergestellt. Nach erfolgreicher Prüfung können die Apps in den Plattformlösungen genutzt werden.

Der modulare Aufbau des Ökosystems erlaubt die kontinuierliche Weiterentwicklung. Zukünftige Apps können einfach integriert werden, ohne dass umfangreiche Neuentwicklungen für die Plattform erforderlich sind. Damit kann die Bundesverwaltung auch in Zukunft von innovativen, bedarfsgerechten Lösungen für die sichere, mobile Arbeit profitieren und gleichzeitig einen hohen Schutz ihrer Daten gewährleisten. ■

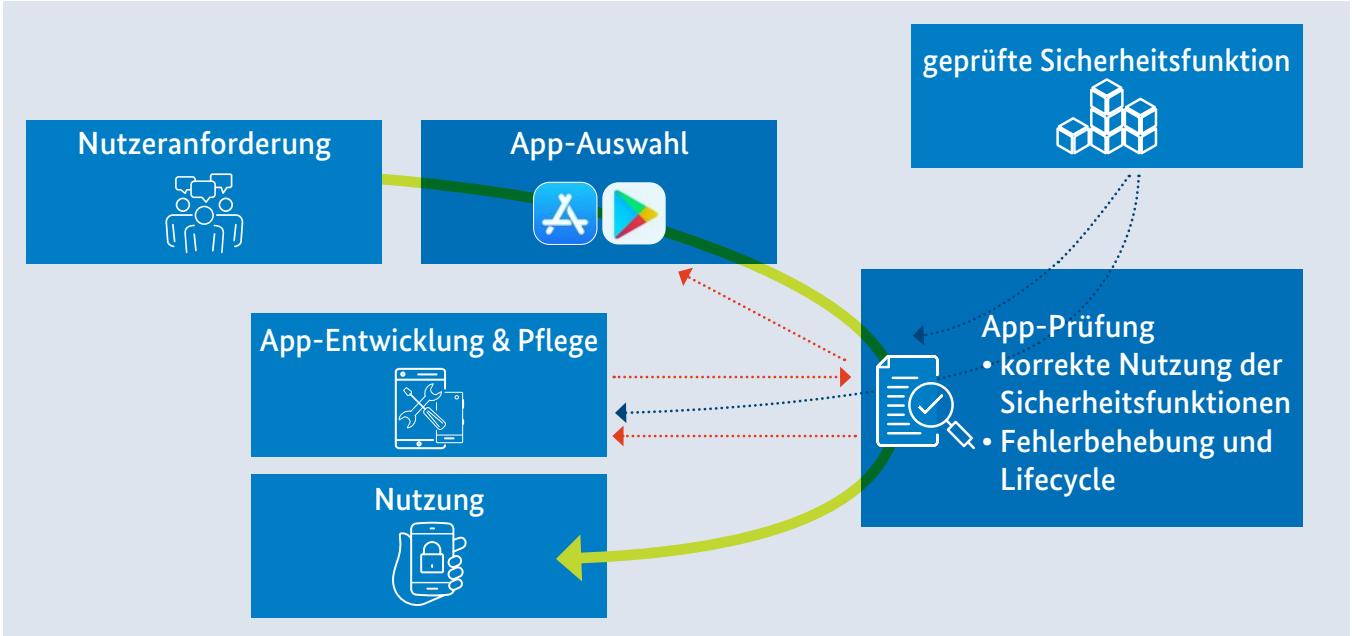


Abbildung 2: Aufnahme von Apps ins Ökosystem

Ein wichtiger Meilenstein für das Smart Grid

Mit der neuen Technischen Richtlinie (TR) Kommunikationsadapter bringt das BSI die Transformation des Energienetzes zu einem sicheren Smart Grid voran

von Michael Brehm und Dr. Andreas Resch, Referat Cybersicherheit für die Digitalisierung der Energiewirtschaft

Das BSI hat mit der Veröffentlichung der TR-03109-5 Kommunikationsadapter einen Meilenstein für die sichere kommunikative Anbindung von technischen Einrichtungen an die Kommunikationseinheit Smart-Meter-Gateway (SMGW) erreicht. Damit besteht die Möglichkeit, Steuerungs- und Submetereinrichtungen sicher und interoperabel anzubinden.

Die Energiewende führt zu einer stark steigenden Zahl von dezentralen Erzeugungsanlagen im Stromnetz. Nicht nur Photovoltaikanlagen (PV) und Stromspeicher mit Wechselrichter liegen im Trend, sondern auch lastvariable Verbrauchseinrichtungen wie etwa Wärmepumpen oder E-Ladestationen. Im Sinne der Netzstabilität ist es wichtig, Erzeugung und Verbrauch flexibel aufeinander abzustimmen. Im Smart Grid, dem intelligenten Stromnetz, vernetzen sich Akteure des Energiesystems digital – von der Erzeugung über den Transport, die Speicherung und die Verteilung bis hin zum Verbrauch. Vor dem Hintergrund einer hohen Bedrohungslage ist daher der Schutz der kommunikativen Anbindung aller Akteure vor Cyberangriffen wichtiger denn je.

Mit der im Dezember 2023 veröffentlichten TR Kommunikationsadapter wurde nun die Grundlage für die sichere Integration von Erzeugungs- und Verbrauchsanlagen in das Smart Grid erarbeitet. Sie ermöglicht neben der Anbindung dieser Anlagen auch die Erfassung von Verbrauchsmessgeräten über die sichere SMGW-Infrastruktur.

ANSCHLUSS VON GERÄTEN AN SMGW NUR MIT BSI-VORGABEN MÖGLICH

Das SMGW ist die Kommunikationseinheit des intelligenten Messsystems (iMSys). Es verbindet die Backendsysteme im Wide-Area-Netzwerk (WAN) mit den lokal installierten Messeinrichtungen im Lokalen Metrologischen Netzwerk (LMN) und auch mit den technischen Einrichtungen im Home-Area-Netzwerk (HAN mit HAN-CLS und HAN-CON). Grundsätzlich können technische Einrichtungen nur dann mit dem SMGW verbunden werden, wenn sie die Interoperabilitäts- und IT-Sicherheitsanforderungen des BSI erfüllen. Die TR formuliert Mindestanforderungen an die Komponenten im HAN-CLS (sogenannte CLS-Komponenten), die den Funktionsumfang eines Kommunikationsadapters implementieren. Technische Einrichtungen können Verbrauchs- und Erzeugungseinrichtungen sein, aber auch Steuerungseinrichtungen zur Anbindung von Neu- und Bestandsanlagen oder Produkte zur Fernauslesung von Sensoren.

Abbildung 1: Systemarchitektur des intelligenten Messsystems mit SMGW und dem neuen CLS-Kommunikationsadapter. WAN: Wide-Area-Netzwerk für den Fernzugriff, LMN: Lokales Metrologisches Netz für Messeinrichtungen, HAN-CON: Home-Area-Netzwerk (HAN) für den Zugang des Letztverbrauchers, HAN-CLS: HAN für weitere technische Einrichtungen.

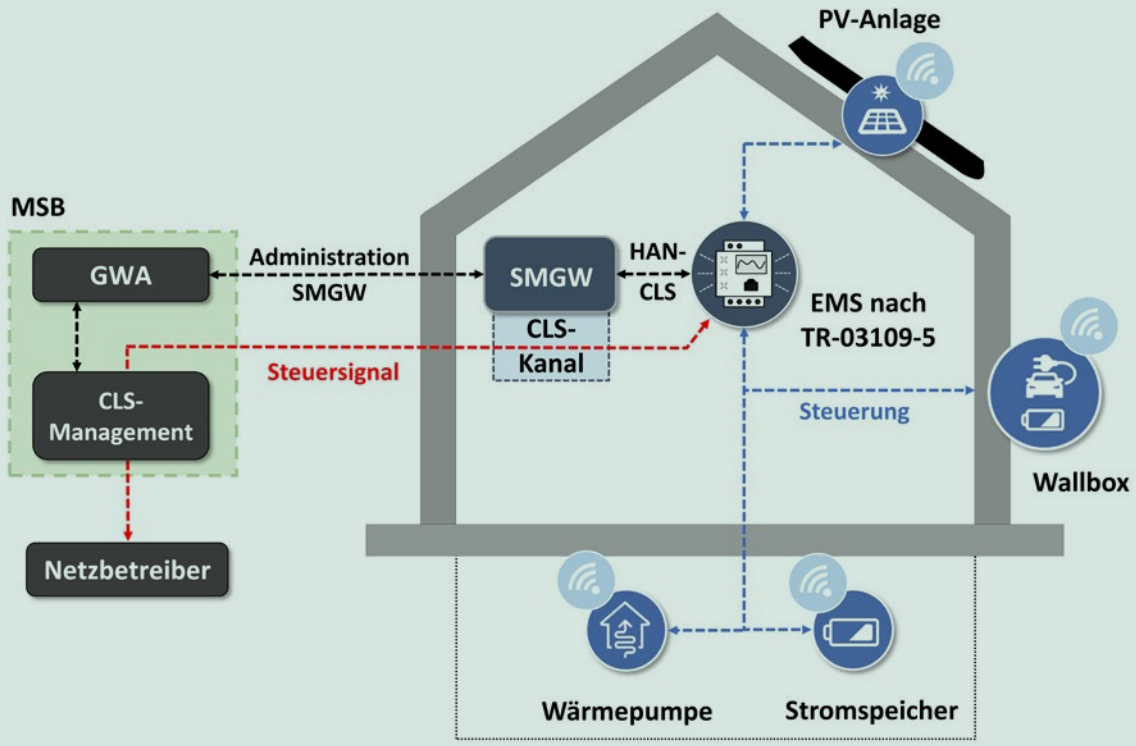


Abbildung 2: Beispiel für die Umsetzung der netzorientierten Steuerung über iMSys mit SMGW und EMS. GWA: Gatew-Ayadministrator; MSB: Messstellenbetreiber; EMS: Energiemanagementsystem als CLS-Komponente nach TR-03109-5. Rote Pfeile: logischer Signalweg; schwarze Pfeile: physischer Signalweg.

BEISPIELE FÜR DIE SICHERE ANWENDUNG

Das Messstellenbetriebsgesetz verlangt ab 2025, dass Verbrauchseinrichtungen und Erzeugungsanlagen sicher und interoperabel über das SMGW gesteuert werden können. Die Abbildung 2 verdeutlicht, wie das Energiemanagementsystem (EMS) das Steuersignal eines Netzbetreibers über den CLS-Kanal des SMGW sicher entgegennimmt. Es wertet es aus und steuert die angeschlossenen Einrichtungen – genau so, wie die Vorgaben und hinterlegten Parameter des Netzbetreibers es verlangen. Als CLS-Komponente ist es durch das BSI zertifiziert.

MINDESTANFORDERUNGEN DER TR KOMMUNIKATIONSADAPTER

Die TR definiert Sicherheitsziele und stellt Mindestanforderungen an die Sicherheitsleistung der CLS-Komponenten. Es geht vor allem um

- Interoperabilitätsanforderungen,
- die Nutzung des CLS-Kanals,
- die Durchführung von Firmware-Updates und
- das Führen einer Systemzeit.

Zur Verwendung des CLS-Kanals ist es notwendig, eine TLS-Verbindung mit dem SMGW herzustellen. Um eine möglichst einfache Inbetriebnahme zu ermöglichen, müssen die CLS-Komponenten in der Lage sein, sich automatisch in das HAN-CLS-Netzwerk einzufügen und die Dienste des SMGW zu nutzen.

Sollten nicht durch SMGW abgesicherte Verbindungen in weitere Netze bestehen, sind die CLS-Komponenten nicht vollumfänglich geschützt. Die Anforderungen an die IT-Sicherheit sollen vor allem mögliche Angriffe auf die CLS-Komponente abwehren.

ZERTIFIZIERUNGSANTRÄGE KÖNNEN GESTELLT WERDEN

Die TR bildet die Grundlage für die Durchführung von Zertifizierungsverfahren nach Technischer Richtlinie sowie für die Beschleunigte Sicherheitszertifizierung (BSZ) des BSI.

Für den Prüfbereich nach Technischer Richtlinie wurden eine Testspezifikation und ein Produktzertifizierungsprogramm erstellt, sodass Hersteller nun entsprechende Zertifizierungsanträge stellen können.

Um die Zertifizierung im neuen BSZ-Geltungsbereich „Komponenten im HAN des SMGW“ (AIS-B SMGW HAN) etablieren zu können, müssen die Grundlagen in zwei Pilotverfahren evaluiert und geprüft werden. Dafür hatten sich zahlreiche Hersteller mit ihren Produkten beworben. Es ist geplant, nach Abschluss der Pilotverfahren den Prüfbereich ab der zweiten Jahreshälfte für alle Hersteller zu öffnen.

HOHE AKZEPTANZ UND STARKER RÜCKHALT IN DER BRANCHE

Die TR Kommunikationsadapter erfährt eine hohe Akzeptanz und starken Rückhalt durch die Energiewirtschaft. Das wurde bei der abschließenden Anhörung im Ausschuss Gateway-Standardisierung deutlich. Zuvor hatte das BSI die Branche in mehreren Kommentierungsphasen in die Entwicklung der TR eingebunden und wertvolles Feedback erhalten. Die Richtlinie gilt als Wegbereiter für wichtige Anwendungsfälle der Energiewirtschaft. Das BSI gestaltet damit aktiv die Sicherheit im Smart Grid und trägt direkt zum Gelingen der Digitalisierung der Energiewirtschaft bei. ■

Portalverbund: Cybersicherheit rund um das Onlinezugangsgesetz

Verwaltungsdigitalisierung konsequent, pragmatisch und sicher voranbringen

von Michael Bauer und Dr. Thorsten Limböck, Referat eID-Lösungen für die digitale Verwaltung, und Erik Mann und Eva Stützer, Referat Cybersicherheit bei der Umsetzung des Onlinezugangsgesetzes

2017 trat das „Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen – Onlinezugangsgesetz (OZG)“[1] in Kraft. Es verpflichtet Bund und Länder, ihre Verwaltungsleistungen elektronisch über Verwaltungsportale verfügbar zu machen. Ein erster Blick in die Arbeitsfassung der Technischen Richtlinie BSI TR 03172 macht deutlich, wie IT-Sicherheit dabei gewährleistet werden soll.

Das Zusammenspiel von Verwaltungsportalen kann in Zukunft besser gelingen, wenn sie zu einem interoperablen Portalverbund verknüpft werden. Ziel ist es, dass eine Verwaltungsleistung von einem beliebigen Portal aus in Anspruch genommen werden kann. Der Portalverbund nutzt dafür gemeinsame zentrale Komponenten, um die individuellen Komponenten der Verwaltungsportale miteinander zu verbinden. Zu den zentralen Komponenten gehören beispielsweise die Servicekonten als Identifizierungs- und Authentisierungslösung mit Postfachfunktion und das Portalverbund Online-Gateway als Suchdienst für Verwaltungsleistungen. Die individuellen Komponenten der Verwaltungsportale sind insbesondere Onlineantragsdienste für die unterschiedlichen Verwaltungsleistungen.

BUND UND LÄNDER STIMMEN RICHTLINIE AB

Die „IT-Sicherheitsverordnung Portalverbund“[2] formuliert IT-Sicherheitsanforderungen an die Komponenten des Portalverbunds. Neben den Maßnahmen aus dem IT-Grundschutz gibt die Verordnung besonders die Technischen Richtlinien des BSI als Stand der Technik vor, um IT-Sicherheit zu gewährleisten. Derzeit entsteht die Technische Richtlinie BSI TR-03172 Portalverbund[3] in Abstimmung mit Bund und Ländern. Dabei steht der Sicherheitsaspekt individueller Komponenten im Fokus – zugleich wird die Absicherung des gesamten Portalverbunds betrachtet.

Aktuell sind die ersten drei Dokumente (Rahmendokument und Teile 3 und 4) in Arbeitsfassungen veröffentlicht, sie werden hier kurz vorgestellt: Das Rahmendokument der BSI TR-03172 liefert grundlegende Informationen für Personen, die sich mit der Sicherheit eines Portalverbunds befassen. Es beinhaltet eine Einleitung, erläutert den Aufbau eines Portalverbunds und macht das Zusammenspiel der einzelnen Komponenten anhand einer beispielhaften Antragsstellung deutlich. Ein Glossar erläutert die wichtigsten Begriffe.

Teil 3 „Onlinedienst“ der Technischen Richtlinie listet Anforderungen an webbasierte Antragsdienste und -assistenten für Verwaltungsleistungen auf. Dabei werden vorrangig Funktionalitäten behandelt, die für Onlinedienste in diesem Kontext notwendig sind, etwa Authentisierung, Sessionmanagement oder Eingabevalidierung. Zudem sind Vorgaben zur Gestaltung einer sicheren Architektur sowie zum Zwischenspeichern und Absenden von Anträgen enthalten.

Ein Antragsroutingdienst ist erforderlich, wenn mehrere Fachbehörden an einen Onlinedienst angebunden sind und innerhalb dieser das für den jeweiligen Antrag zuständige Fachverfahren ermittelt werden muss. Im Anschluss wird der befüllte Antrag an das ermittelte Verfahren übermittelt. Die Anforderungen für diese Prozesse sind in der Technischen Richtlinie 03172-4 „Antragsrouting“ formuliert.

WEITERE DOKUMENTE ZU WICHTIGEN KOMPONENTEN FOLGEN

Der Portalverbund umfasst darüber hinaus weitere Komponenten, die zukünftig in der TR-03172 abgebildet werden sollen. Dazu gehört beispielsweise das Datenschutzcockpit. Es erlaubt natürlichen Personen gemäß Paragraf 10 OZG, den Austausch ihrer Daten zwischen angeschlossenen Behörden nachzuvollziehen, sofern dieser unter Verwendung der Identifikationsnummer (IDNr) der Person stattgefunden hat. Wenn Protokolle über den Austausch bei den Registern vorliegen, erhält eine Person eine Übersicht darüber, welche Daten aus dem Register von einer anderen Behörde abgefragt worden sind. So kann mehr Transparenz in der Verwendung personenbezogener Daten erreicht werden.

Das Datenschutzcockpit wird unter der Federführung des Landes Bremen entwickelt. Das BSI unterstützt bei den sicherheitstechnischen Aspekten und hat somit die Gelegenheit, die dazugehörige TR-03172-2 praxisnah und parallel zum Entwicklungsprozess zu erarbeiten. Besondere Beachtung findet die Absicherung der schützenswerten Daten, die nur der abrufenden Person angezeigt werden dürfen. Aus diesem Grund ist die zweifelsfreie Bestimmung der Identität der anfragenden Person im Rahmen der Anmeldung essenziell. Weiterhin muss sichergestellt werden, dass keine personenbezogenen Daten im Datenschutzcockpit gespeichert werden oder abfließen können.

Weitere Dokumente zu Komponenten wie dem Portalverbund Online-Gateway oder einem Bezahldienst zum Begleichen von anfallenden Gebühren werden die TR-03172 zukünftig ergänzen.

VIELFALT DER IT-SYSTEME WIRD ZUR HERAUSFORDERUNG

Eine Herausforderung bei der Entwicklung der Technischen Richtlinie ist die vielfältige Landschaft von IT-Systemen, die über den Portalverbund hinausgeht. Parallel zur Digitalisierung der Angebote für die Nutzenden müssen auch die Verwaltungsstrukturen, inklusive Fachverfahren und Register, sicher digital gestaltet werden. Im Rahmen der Registermodernisierung[4] begleitet das BSI diesen Umsetzungsprozess. Das OZG-Änderungsgesetz trägt den Erfahrungen und Erkenntnissen der bisherigen Umsetzung der Digitalisierung von Verwaltungsleistungen Rechnung. So ist eine Stärkung der eID als Standard-Authentisierungsmittel vorgesehen, ebenso wie ein neuer und zentraler Siegeldienst, um qualifizierte elektronische Siegel aufzubringen und zu verifizieren. Die Verwaltungsdigitalisierung wird nunmehr als Daueraufgabe verstanden. Eine vereinfachte, beschleunigte und medienbruchfreie Kommunikation mit der Verwaltung kann nur dann sicher und vertrauenswürdig gelingen, wenn Informationssicherheit dabei von Anfang an mitgedacht wird. ■

Technische Richtlinie:

https://www.bsi.bund.de/dok/tr-03172

1 https://www.gesetze-im-internet.de/ozg/BJNR313800017.html
2 https://www.gesetze-im-internet.de/itsiv-pv/BJNR001800022.html
3 https://www.bsi.bund.de/dok/tr-03172
4 https://www.gesetze-im-internet.de/regmog/BJNR059100021.html

Der europäische Cyber Resilience Act – ein Update

Europa einigt sich auf Regeln für mehr Cybersicherheit

von Anna Thurm, Referat Marktaufsicht über zertifizierte Dienstleister und Produkte

Im Dezember 2023 haben Europäische Kommission, Rat und Parlament nach dreimonatigen Verhandlungen eine Einigung über den Cyber Resilience Act (CRA) erzielt und damit den sogenannten Trilog abgeschlossen. Nach Finalisierung des Textes wurde das Gesetz im März 2024 im Europäischen Parlament verabschiedet und wartet jetzt auf die Zustimmung des Rats

Im September 2022 veröffentlichte die Europäische Kommission den Entwurf zum CRA. Die EU-Verordnung zielt darauf ab, dass erstmalig horizontale – also produktkategorieunabhängige – Cybersicherheitsanforderungen für den Schutz von digitalen Produkten über deren gesamten Lebenszyklus eingeführt werden.

EIN UPGRADE FÜR DIE INFORMATIONSSICHERHEIT

Das neue Regelwerk wird sich auf alle vernetzten oder vernetzbaren Produkte beziehen, für die es nicht bereits weiter gehende Regelungen gibt, wie z. B. für Medizinprodukte, motorisierte Fahrzeuge, zivile Luftfahrt. Es gilt damit auch für Software. Explizit ausgenommen vom Geltungsbereich ist lediglich Open-Source-Software außerhalb einer kommerziellen Tätigkeit.

Die Verordnung definiert Zugangsvoraussetzungen für den EU-Binnenmarkt und erweitert damit den Geltungsbereich des bereits bekannten CE-Kennzeichens. Tritt der CRA in Kraft, steht diese Zusicherung der Sicherheit eines Produktes durch den Hersteller erstmals nicht nur für Safety, also die Betriebssicherheit, sondern auch für Security, also die Informationssicherheit. Um diese zu gewährleisten, ergeben sich für die Hersteller nun neue Pflichten, die nicht nur für den Kaufzeitpunkt gelten, sondern auch für die Laufzeit der üblichen Nutzung eines Produktes.

Der CRA stellt sowohl Anforderungen an Hersteller von Produkten mit digitalen Elementen als auch an die Produkte selbst. Dies umfasst grundlegende Anforderungen an die Produkte wie Security by Design, Security by Default, Gewährleistung von Vertraulichkeit und Integrität der verarbeiteten Daten. Darüber hinaus beinhaltet der CRA Anforderungen an den Hersteller zum Umgang mit Schwachstellen, z. B. die Verpflichtung, Sicherheitsupdates über den gesamten Lebenszyklus des Produkts bereitzustellen, Schwachstellen zu melden und zu beheben sowie eine Software Bill of Materials (SBOM) zu pflegen. Zudem werden eine umfangreiche Dokumentation für Anwenderinnen und Anwender zum Produkt sowie Kontaktmöglichkeiten für Schwachstellenmeldungen verlangt.

Einige Details der Regelung waren noch Gegenstand der Diskussion im Trilog. Gegenüber dem 2022 veröffentlichten Entwurf haben sich in den Verhandlungen beispielsweise folgende Änderungen am Gesetzestext ergeben:

- Angabe zum Ende des Supportzeitraums beim Kauf gut sichtbar auf dem Produkt
- Festlegung des Supportzeitraumes des Produkts durch den Hersteller unter Betrachtung von u. a. angemessenen Nutzererwartungen und üblicher Nutzungsdauer
- Meldewege und -fristen für Schwachstellen
- Zuordnungen von Produktkategorien zu Risikoklassen, Umbenennung der Risikoklassen
- Übergangsfrist bis Geltungsbeginn
- Konkretisierung der Ausnahme für Open Source

Diese Verpflichtungen gelten nicht nur für Hersteller, sondern auch für Importeure oder Vertriebe, also die Akteure, die Produkte mit digitalen Elementen im EU-Binnenmarkt in den Verkehr bringen. In den einzelnen Mitgliedsstaaten werden Marktüberwachungsbehörden eingesetzt, die bei Nichteinhaltung der Anforderungen betroffene Produkte vom Markt nehmen können. Zudem drohen empfindliche finanzielle Strafen.

SUPPORT DURCH DAS BSI, DIE ANFORDERUNGEN DES CRA UMZUSETZEN

Die Übergangsfrist von Inkrafttreten bis Geltungsbeginn der EU-Verordnung wird 36 Monate betragen. Aufgrund seines horizontalen Geltungsbereichs wird der CRA in seiner Anwendung verpflichtend für eine Vielzahl von Produkten mit digitalen Elementen gelten. Für Hersteller ist es ratsam, sich auf die neuen Marktzugangsvoraussetzungen vorzubereiten. Es benötigt Zeit und einige Erfahrungszyklen, um die notwendigen Prozesse zu etablieren. Um die Anforderungen des CRA vorab greifbarer zu machen, erarbeitet das BSI eine Technische Richtlinie, in der die Anforderungen an die Hersteller und Produkte hinsichtlich der Cyberresilienz übersichtlich und konkret beschrieben sind. Bereits im August 2023 wurde ein Teildokument mit Vorgaben zu Umfang, Inhalt und Format einer Software Bill of Materials zur Verfügung gestellt.

Das BSI engagiert sich auch im Rahmen der Standardisierung. Für viele konkretere Vorgaben im Rahmen des CRA, z. B. für besonders schützenswerte Produktkategorien, greift die EU-Kommission auf das Fachwissen der europäischen Standardisierungsgremien zurück. Dort wirken die Experten des BSI für eine sichere Ausgestaltung von Verbraucherprodukten mit. ■

Stärkung der Zusammenarbeit und Cyberresilienz in Europa

Spitzentreffen der europäischen Cybersicherheitsbehörden im Februar in München

von Clarissa Wilkie, Referat Internationale Beziehungen

Auf Einladung des BSI kamen 26 Direktorinnen und Direktoren der für Cybersicherheit zuständigen Behörden aus Europa zusammen, um sich über aktuelle nationale, europäische und internationale Herausforderungen auszutauschen. Der Schwerpunkt des diesjährigen Treffens lag auf den Herausforderungen neuer EU-Rechtsakte zu Cybersicherheit, insbesondere der NIS-2-Richtlinie. Im Sinne einer europaweit kohärenten Vorgehensweise berieten die Teilnehmenden, wie künftig gemeinsam IT-Sicherheitsvorfällen bei multinationalen Unternehmen begegnet werden kann.

Das zentrale Thema des Treffens am 15. Februar waren die europäischen Rechtsvorschriften, die für die Cybersicherheit von Bedeutung sind. Einigkeit bestand darin, dass deren effiziente Umsetzung sowie die Vermeidung einer Fragmentierung zu den großen Herausforderungen zählen, die die zuständigen Behörden nur im engen Schulterschluss bewältigen können. In diesem Sinne wurde auch eine gemeinsame Erklärung erarbeitet, die den Fokus auf die anstehende Umsetzung der NIS-2-Richtlinie legt. Gleichzeitig richtet die Erklärung einen Appell an den EU-Gesetzgeber, den Mitgliedsstaaten ausreichend Zeit für eine effiziente, effektive und harmonisierte Umsetzung der Rechtsakte einzuräumen, bevor neue Legislativvorhaben angestoßen werden.

EUROPÄISCHES ENGAGEMENT DES BSI

Das BSI ist kontinuierlich in einschlägigen EU-Gremien und -Arbeitsgruppen wie der NIS-Kooperationsgruppe engagiert, um dort eigene Erfahrungen etwa aus dem KRITIS-Bereich einzubringen. Die internationale Zusammenarbeit stellt für das BSI einen essenziellen Erfolgsfaktor zur Verbesserung der Cybersicherheit in Deutschland und Europa dar. Das Direktorentreffen, erstmals vom BSI in Zusammenarbeit mit der Munich Cyber Security Conference organisiert, bietet den Teilnehmenden seit 2020 jährlich die Gelegenheit, strategische Handlungsmöglichkeiten im Sinne der europäischen Zusammenarbeit zu diskutieren. An den Treffen nehmen nicht nur Vertreterinnen und Vertreter aus den EU-Mitgliedsstaaten 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).

WICHTIGER BEITRAG ZUR VERNETZUNG DER BEHÖRDEN

Mit der Ausrichtung des Cyber Security Directors' Meeting – so der offizielle Veranstaltungstitel – leistet das BSI einen wichtigen Beitrag zur besseren Vernetzung der Behörden, die jeweils national für Cybersicherheit federführend zuständig sind. Wie groß der Bedarf für einen Austausch auf dieser Ebene ist, zeigt der Beschluss des Direktorentreffens, die Veranstaltung zukünftig mindestens zweimal im Jahr durchzuführen. Ein zweites Treffen wurde bereits im Mai 2024 von der belgischen Partnerbehörde des BSI im Rahmen der EU-Ratspräsidentschaft in Gent ausgerichtet. ■

BSI-Präsidentin Claudia Plattner moderierte als Gastgeberin die Veranstaltung. Im Fokus des Austauschs standen strategische Fragen der Cybersicherheit.

Eine Vielzahl an Direktorinnen und Direktoren folgte der Einladung des BSI nach München.

DAS INTERNATIONALE ENGAGEMENT DES BSI

Die internationale Zusammenarbeit ist für das BSI seit seiner Gründung vor mehr als 30 Jahren ein essenzieller Faktor zur Verbesserung der Cybersicherheit. Ziel des BSI ist, neben seiner nationalen Rolle als Cybersicherheitsbehörde des Bundes, Cybersicherheit auch international mitzugestalten sowie die eigene technologische Beurteilungsfähigkeit zu stärken. Um seiner Verantwortung dafür angemessen nachzukommen, intensiviert und erweitert das BSI kontinuierlich seine Beziehungen zu Behörden, Organisationen, Unternehmen sowie Akteuren der Wissenschaft und Zivilgesellschaft weltweit. Die Arbeit in diversen Fachgremien zu Informations- und Cybersicherheit im EU-, NATO- und internationalen Kontext ist dabei wesentlicher Bestandteil des internationalen Engagements des BSI.

Europäische Perspektive(n) für einen starken Digitalen Verbraucherschutz

Inspirierender Austausch beim ersten Europäischen Symposium „Cybersecurity for Europe: Integrating the Consumer Perspective“ in Dresden

von Kristina Unverricht und Dr. Jörg Hübner, Referat Grundsatzfragen des Digitalen Verbraucherschutzes und Kooperationen

Das BSI organisierte Anfang Februar 2024 erstmals das Europäische Symposium „Cybersecurity for Europe: Integrating the Consumer Perspective“. Vertreterinnen und Vertreter europäischer Cybersicherheitsorganisationen, von Verbraucherschutzorganisationen und der Europäischen Kommission nutzten die Chance, Ideen und Ansätze für die Verbesserung des Digitalen Verbraucherschutzes zu entwickeln.

Zentrales Thema des Symposiums waren die Herausforderungen des Digitalen Verbraucherschutzes und – angesichts grenzüberschreitender Cyberkriminalität – die Bedeutung einer gemeinsamen europäischen Perspektive. Für das BSI sind drei zentrale Punkte für die zukünftige Ausrichtung des Digitalen Verbraucherschutzes in Deutschland von Bedeutung:

- Wir sorgen dafür, dass IT-Geräte und Software sicher auf den Markt kommen: Mit dem IT-Sicherheitskennzeichen hat das BSI bereits heute ein wirksames Werkzeug zur Verbesserung der Produktsicherheit implementiert. Da Security by Design im Digitalen Verbraucherschutz fest verankert ist, sieht sich das BSI deshalb auch in der Verantwortung, die Marktüberwachungsfunktion des Cyber Resilience Acts anzunehmen.

- Das BSI wird zur zentralen deutschen Stelle zum Schutz der Menschen im Netz ausgebaut: Weil unterschiedliche Standards innerhalb Europas langfristig eine Schwächung der IT-Sicherheit von Anwendenden darstellen, bauen wir aktiv die Vernetzung bedeutender Stakeholder auf dem Kontinent aus. So fördern wir die sichere, grenzüberschreitende Digitalisierung.

- Der Digitale Verbraucherschutz sollte nicht bei Informationsangeboten für Verbraucherinnen und Verbraucher enden, sondern diese mit aktiven Schutzmaßnahmen untermauern: Neben der wichtigen Aufklärungsarbeit ist es notwendig, technische Mittel zu identifizieren, um Schäden und Cyberangriffe in ihrer Entstehung zu unterbinden. Dabei wird das Prinzip des menschzentrierten Designs (User-Centred Design) im Zentrum der Maßnahmengestaltung stehen.

SOUVERÄNE VERBRAUCHERINNEN UND VERBRAUCHER

Diskussionsstoff boten die Fragen, wie notwendige Rahmenbedingungen für einen erfolgreichen Schutz im digital vernetzten Alltag aussehen müssen und wie die Verbraucherschutzperspektive in die europäische Cybersicherheitsregulierung integriert werden kann. Argumente hierfür wurden durch praxisorientierte Vorträge rund um die Interessen und Anforderungen der Verbraucherinnen und Verbraucher an ihre Cybersicherheit untersetzt.

Links: Panel-Diskussion zu den gemeinsamen Perspektiven eines europäischen Digitalen Verbraucherschutzes, v.l.n.r.: Lars Bartsch (BSI), Ruben Verstraete (Directorate General for Economic Inspection, Inspector International Coordination, FPS Economy, Brussels), Dr. Karen Renaud (Strathclyde University, Glasgow), Claudio Teixeira (Legal Officer – Digital and Consumer Rights, The European Consumer Organisation BEUC), Kristina Unverricht (BSI)

Die Vortragenden stellten die folgenden Thesen für einen wirksamen Digitalen Verbraucherschutz der Zukunft auf:

- Digitaler Verbraucherschutz schützt vor Cybergefahren im digitalen Raum, ohne die Souveränität von Verbraucherinnen und Verbrauchern einzuschränken. Ein grundlegender Schutz muss durch Mindestsicherheitsanforderungen für alle vernetzten Produkte und Dienste sichergestellt werden.

- Digitaler Verbraucherschutz schließt alle Verbrauchergruppen ein. Dies gilt insbesondere für die Anforderungen vulnerabler (verletzlicher) Verbraucherinnen und Verbraucher. Hierfür bedarf es entsprechender Beteiligungsformate. Die Verantwortung für Cybersicherheit darf nicht den Verbraucherinnen und Verbrauchern auferlegt werden. Entwicklungen in der Digitalisierung und technologische Innovationen dürfen nicht zulasten von Verbraucherinnen und Verbrauchern gehen, sondern müssen grundsätzlich von Beginn an sicher gestaltet werden.

- Digitaler Verbraucherschutz setzt auf vielfachen Ebenen an: insbesondere beim (nutzerzentrierten) Produkt- und Dienstdesign, aber auch auf Marktplätzen für digitale Produkte.
  Für eine wirksame und effiziente Umsetzung benötigt Europa neue Strategien und Werkzeuge.

- Effizienter Digitaler Verbraucherschutz entsteht durch einen kooperativen Ansatz, d. h. durch das Einbringen der jeweiligen Fachexpertise der beteiligten Organisationen und Stakeholder.

Das Symposium diente als Plattform für Vernetzung und Austausch, aber auch der Wissensvermittlung, um gemeinsam weiter an den Herausforderungen für einen starken europäischen Digitalen Verbraucherschutz zu arbeiten. Das erfolgreiche Veranstaltungsformat soll zukünftig regelmäßig Raum für den Austausch bieten. ■

Dr. Karen Renaud von der Strathclyde University (Glasgow) gab Einblicke in „Menschzentrierte Sicherheitsaspekte" zur Verbesserung des Digitalen Verbraucherschutzes.

András Zsigmond, Legal Coordinator of the Consumer Product Safety Unit der Europäischen Kommission, referierte zur neuen EU-Produktsicherheitsverordnung GPSR.

Weitere Informationen zum Digitalen Verbraucherschutz:

www.bsi.bund.de/VerbraucherInnen

Social Engineering: Schutz vor KI-gestützten Cyberangriffen

Künstliche Intelligenz bringt Cyberangriffe auf ein neues Level

von Jan Lammertz, Referat Cybersicherheit für Gesellschaft und Bürger

Maschinell erstellte Videos, Bilder, Texte oder Stimmen sind mittlerweile weitverbreitete Phänomene. Werden Menschen, z. B. mithilfe solcher generierter Imitationen, so getäuscht, dass sie Angreifenden vertrauen und beispielsweise Zugriff auf Daten gewähren, dann spricht man von Social Engineering. Durch den Einsatz von Künstlicher Intelligenz (KI) können Cyberkriminelle diese manipulativen Angriffe mitunter auch effizienter und effektiver gestalten.

Wir werfen einen Blick auf die Dynamiken dieses Phänomens, den Einfluss von KI auf Social Engineering und die Herausforderungen sowie Schutzmöglichkeiten für Nutzerinnen und Nutzer.

Digitale Täuschungen können durch Künstliche Intelligenz ein neues Level erlangen, und genau dies wird beim Social Engineering ausgenutzt: Cyberkriminelle versuchen menschliche Verhaltensweisen zu manipulieren. Durch den Einsatz von KI ist eine neue Dimension erreicht worden. „Social Engineering 2.0“ zeichnet sich durch noch stärker personalisierte und höherentwickeltere Angriffe aus, bei denen KI genutzt wird, um gefälschte Videos, Bilder, Stimmen oder Persönlichkeitsprofile zum Täuschen von Menschen zu erstellen. Ziel ist, Zugang zu Informationen, Systemen oder Netzwerken zu erhalten. KI ermöglicht es Cyberkriminellen nun auf effizientere Weise, überzeugendere Angriffe durchzuführen und ihre Opfer zu unüberlegten Aktionen zu drängen.

Mittels maschinellen Lernens kann KI menschliches Verhalten immer besser imitieren und aufgrund von Datenanalysen personalisierte Angriffe schneller orchestrieren als bislang. Diese Techniken erschweren es, betrügerische Aktivitäten zu erkennen, da die Angriffe auf den individuellen Verhaltensmustern der Zielperson basieren.

Diese Methoden werden ständig weiterentwickelt. Die Angreifer versuchen, den Sicherheitsmaßnahmen voraus zu sein. Deswegen sind Sensibilisierung, Schulungen und regelmäßige Sicherheitsüberprüfungen entscheidend, um sich gegen Social-Engineering-Angriffe zu schützen.

WIR STELLEN EINIGE FORMEN DES SOCIAL ENGINEERINGS KURZ VOR:

Spear Phishing:
Der Angreifende richtet seine Phishing-Angriffe auf eine spezifische Person oder Organisation, indem er personalisierte Informationen nutzt, um Vertrauen zu gewinnen.

Whaling:
Ähnlich ausgelegt wie Spear Phishing, zielt aber auf hochrangige Führungskräfte oder wichtige Persönlichkeiten ab.

Vishing (Voice Phishing):
Der Angreifende verwendet Telefonanrufe, um sich als legitime Person oder Organisation auszugeben und so sensible Informationen zu erhalten.

Social Media Exploitation:
Durch die (automatisierte) Analyse von Social-Media-Profilen sammeln Cyberkriminelle persönliche Informationen, um gezielt Einzelpersonen anzugreifen.

Deepfakes:
Künstliche Intelligenz wird verwendet, um gefälschte Videos oder Audioaufnahmen zu erstellen und Personen zu bestimmten Handlungen zu verleiten oder z. B. Fake News zu verbreiten.

IoT-Exploitation:
Angreifer nutzen Schwachstellen in vernetzten Geräten und dem Internet der Dinge (IoT) aus, um Zugang zu persönlichen oder geschäftlichen Netzwerken zu erhalten.

WAS KÖNNEN PRIVATANWENDENDE GEGEN SOCIAL ENGINEERING TUN?

Für Privatanwendende ergeben sich aus Social Engineering mit KI-gestützten Angriffen besondere Herausforderungen: Die zunehmende Schwierigkeit, zwischen echten und gefälschten Inhalten zu unterscheiden, erfordert eine verbesserte Sicherheitssensibilisierung. Da die Angriffe immer personalisierter und subtiler werden, müssen die Menschen in ihrem digitalen Alltag lernen, aufmerksamer gegenüber ungewöhnlichen Anfragen oder verdächtigen Aktivitäten zu sein.

Um sich gegen diese hoch entwickelten Angriffe zu schützen, sollten Privatanwendende ihre Sicherheitsvorkehrungen verstärken. Beispielsweise der Einsatz von zeitnah installierten Softwareupdates und stets aktuell gehaltenen Antivirenprogrammen sowie Firewalls bietet eine sinnvolle Grundlage für den Schutz vor unautorisierten Zugriffen.

Zusätzlich ist eine gesunde Skepsis gegenüber unerwarteten digitalen Nachrichten und Anfragen sinnvoll. z. B. kann man sich wirkungsvoll vor Angriffen schützen, indem man versucht, die vermeintlichen Absenderinnen und Absender einer Nachricht auf einem anderen Kanal zu erreichen und das Anliegen zu verifizieren. Betroffene eines solchen Angriffs sollten Beweise per Screenshots sammeln und den Fall bei der Polizei anzeigen.

WIE KANN DER EINSATZ VON TECHNIK DIE MENSCHEN SCHÜTZEN?

Cyberkriminelle und Cyberabwehrsysteme befinden sich in einem ständigen Wettlauf, der oft über Erfolg oder Misserfolg eines Cyberangriffs entscheidet. Einerseits haben Cyberkriminelle durch KI die Möglichkeit, effektive Methoden des Social Engineerings zu entwickeln. Andererseits können im Gegenzug Machine Learning Tools, z. B. zur Erkennung von KI-generierten Phishing-Versuchen, eingesetzt werden.

Oberstes Ziel einer solchen KI-gestützten Erkennungssoftware ist es, auf Basis von Trainingsdaten bestimmte Muster von Phishing-Inhalten in Nachrichten oder auf Webseiten zu identifizieren und zu blockieren. Solche Filter können in Webbrowsern, E-Mail-Diensten oder IT-Netzwerken integriert werden, um in Echtzeit nach Anomalien oder verdächtigen Aktivitäten Ausschau zu halten und, wenn nötig, Alarm zu schlagen.

EIN GESTEIGERTES RISIKOBEWUSSTSEIN IST GRUNDVORAUSSETZUNG

Social Engineering, unterstützt durch Künstliche Intelligenz, erfordert also eine fortlaufende Anpassung der Sicherheitspraktiken sowie eine unaufhörliche Wachsamkeit. Privatanwendende müssen sich bewusst sein, dass die Angriffslandschaft aufgrund der Nutzung von KI durch Cyberkriminelle deutlich vielfältiger und unsicherer geworden ist. Durch technische Maßnahmen, ein gesteigertes Risikobewusstsein sowie eine erhöhte Vorsicht im digitalen Alltag lassen sich die eigene digitale Identität und persönliche Daten effektiver schützen. ■

Weitere Informationen:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/Sichere-Verwendung/sichere-verwendung_node.html

BSI-Basis-Tipp

Tipps für den digitalen Familienalltag

Wie Eltern ihre Kinder online begleiten und schützen können

von Larissa Hänzgen, Referat Cybersicherheit für Gesellschaft und Bürger

Zum Familienleben gehören digitale Medien inzwischen selbstverständlich dazu. Computer, Laptop, Spielekonsole, Smart Speaker und vor allem Smartphone und Tablet sind häufig Teil des Alltags. Sie werden bereits von den Jüngsten gerne genutzt – oftmals unbegleitet. Die meisten dieser Geräte bieten einen einfachen und nahezu unbegrenzten Zugang zum Internet. Ohne entsprechende Einstellungen birgt dies Gefahren und Sicherheitsrisiken.

IT-BASISSCHUTZ FÜR KINDER UND JUGENDLICHE

Wer Kinder und Jugendliche begleitet, steht vor der Herausforderung, den bewussten Umgang mit digitalen Medien zu fördern und eine sichere Online-Umgebung zu schaffen. Zum Glück gibt es technische Schutzmaßnahmen, um die jungen Mediennutzenden online vor potenziellen Gefahren zu schützen. In modernen Betriebssystemen sind Basis-Kindersicherungen meist integriert, müssen aber erst aktiviert und an die jeweiligen Bedürfnisse angepasst werden. Mit den folgenden BSI-Basis-Tipps legen Sie den Grundstein für einen sicheren digitalen Familienalltag.

1. RICHTEN SIE EIN EIGENES BENUTZERKONTO FÜR JEDES KIND EIN

Die Einrichtung eines separaten Benutzerkontos ohne Administratorenrechte am PC ist ein erster wichtiger Schritt. In den Einstellungen des Computers können Sie unter Konto einen Benutzer hinzufügen. Durch die Einrichtung eines separaten Kontos beschränken Sie z. B. den Zugriff auf sensible Daten und Einstellungen des Hauptkontos. Dadurch wird beispielsweise verhindert, dass sich Schadsoftware Administratorberechtigungen zunutze macht und Dateien im System infiziert oder beschädigt.

Risiken für Kinder und Jugendliche im Internet

Schutz vor Schadprogrammen

Besonders die jungen Nutzerinnen und Nutzer lassen sich schnell dazu verleiten, Symbole und Links anzuklicken, die spannende Inhalte oder kostenlose Spiele versprechen. So können sie leicht in die Falle von Internetkriminellen tappen. Durch das Öffnen infizierter E-Mails oder anderer elektronischer Nachrichten, aber auch alleine durch den Besuch von Webseiten können Computer mit bösartigen Programmen wie Viren, Würmern oder Trojanern infiziert werden.

Gefahr durch Spam und Phishing

Auch Kinder und Jugendliche werden per Mail, Messenger oder in sozialen Netzwerken mit Spam oder betrügerischen Phishing-Nachrichten konfrontiert. Neben klassischer Werbung enthalten diese Nachrichten mitunter auch Schadsoftware oder Links auf infizierte Webseiten oder zielen darauf ab, persönliche und sensible Daten zu entlocken.

Preisgabe persönlicher Daten

Soziale Medien leben vom Informationsaustausch, von den Fotos der Freunde und Freundinnen oder von Videos aus dem Urlaub. Allerdings birgt diese Masse an Daten auch Risiken. Sensible Daten wie Name, Geburtsdatum, Telefonnummer, Adresse oder auch Account- und Bankdaten sollten auf keinen Fall preisgegeben werden.

Cybermobbing nimmt zu

Nicht nur Cyberkriminelle haben es auf persönliche Daten abgesehen. Inzwischen werden Beleidigungen und Ausgrenzungen vermehrt online ausgetragen. Täterinnen und Täter nutzen soziale Netzwerke oder Messenger, um ihre Opfer bloßzustellen, zu schikanieren oder zu beleidigen. Sie drohen dann etwa, private Bilder zu verbreiten oder zu veröffentlichen.

Ungeeignete Inhalte für Kinder im Netz zugänglich

Neben vielen nützlichen Inhalten sind im Internet insbesondere für Kinder auch ungeeignete Inhalte nur einen Mausklick weit entfernt. Gewaltverherrlichende Onlinespiele und rassistische oder pornografische Äußerungen und Darstellungen sind nur einige Beispiele. Selbst in vermeintlich harmlosen Onlinediensten wie Messengern und sozialen Medien lauern Risiken.

2. NUTZEN SIE EIN VIRENSCHUTZPROGRAMM

Unsichere Downloads, z. B. von Spielen, können schädliche Software auf dem Computer des Kindes installieren. Ein Virenschutzprogramm erkennt und blockiert Malware und Sicherheitsbedrohungen. In die meisten Betriebssysteme ist bereits ein Virenschutzprogramm integriert. Aktivieren Sie die Software in den Sicherheitseinstellungen des Computers und halten Sie diese mit automatischen Updates auf dem neuesten Stand.

3. ÜBERPRÜFEN SIE DIE FIREWALL

Die meisten Betriebssysteme verfügen über eine integrierte Firewall. Überprüfen Sie unbedingt in den Einstellungen des Systems, ob diese aktiviert ist. Falls nicht, aktivieren Sie die Firewall und passen Sie diese auf Ihre individuellen Bedürfnisse an, um das eigene System und das Ihrer Kinder vor unbefugten Zugriffen und potenziellen Gefahren von außen zu schützen. Die Firewall können Sie außerdem so konfigurieren, dass nur bestimmte Programme und Anwendungen auf das Internet zugreifen können. Dadurch wird das Risiko minimiert, dass Kinder und Jugendliche schädliche Anwendungen, Programme oder Spiele herunterladen.

4. NUTZEN SIE EINEN ROUTER MIT KINDERSCHUTZFUNKTIONEN

Mit modernen Routern lässt sich der Internetzugang für alle Geräte, die im Heimnetzwerk angemeldet sind, einzeln regeln. Jedem Gerät wird dafür über den Router ein Zugangsprofil zugewiesen, in dem z. B. die Onlinezeit begrenzt, Netzwerkanwendungen freigegeben bzw. beschränkt oder bestimmte Internetseiten gesperrt werden können. Die Einstellungen können bei allen Geräten der Kinder und Jugendlichen vorgenommen werden, während die Geräte der Eltern den vollen Zugriff behalten. Sichern Sie Ihr drahtloses Netzwerk zudem mit einem starken Passwort, um unbefugten Zugriff zu verhindern und die Kontrolle darüber zu behalten, wer auf das Internet zugreifen kann.

5. VERWENDEN SIE EINE SUCHMASCHINE FÜR KINDER

Um Kinder bei der sicheren Onlinesuche zu unterstützen, gibt es spezielle Kindersuchmaschinen. Diese zeigen nur kindgerechte und sogar redaktionell gefilterte Inhalte. Außerdem unterdrücken die meisten Suchmaschinen für Kinder auch Werbung oder (gefälschte) Pop-ups. Das minimiert das Risiko, dass der Nachwuchs auf gefälschte Webseiten geleitet wird, Malware herunterlädt oder ungeeignete Inhalte sieht. Wenn Sie sich für eine Suchmaschine entschieden haben, legen Sie diese im Browser als Startseite fest. Auch die meisten Browser bieten Kinderschutz durch Browser-Erweiterungen an, mit denen einzelne Webseiten gesperrt werden können.

6. LEGEN SIE ZEITBESCHRÄNKUNGEN FEST

Diese Funktion ist oft in Kindersicherungssoftware, aber auch in Betriebssysteme integriert. Mit Zeitlimits können Sie festlegen, wie lange Ihre Kinder ihre Geräte nutzen und online sein können. Dabei geht es nicht nur darum, für die gesamte Woche die Dauer der Bildschirmzeit zu begrenzen, sondern sie auch auf verschiedene Tageszeiten zu beschränken, um zu verhindern, dass Kinder bis spät in die Nacht oder unbeaufsichtigt online sind. Manche Betriebssysteme und Softwarelösungen bieten auch die Möglichkeit, Limits für bestimmte Spiele und Apps zu vergeben.

7. SENSIBILISIEREN SIE FRÜHZEITIG FÜR GUTEN ACCOUNTSCHUTZ

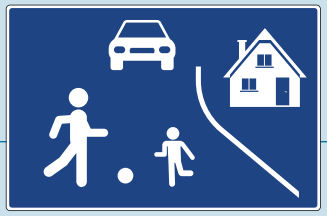
Sobald Kinder und Jugendliche online unterwegs sind, können auch sie Opfer von Phishingangriffen werden. Erklären Sie Kindern die Bedeutung von sicheren Passwörtern und wie man sie erstellt und beispielsweise mit einem Passwortmanager verwaltet. Richten Sie, wann immer möglich, die Zwei-Faktor-Authentisierung ein. Kinder sollten zudem wissen, dass sie Passwörter niemals mit anderen teilen und keine persönlichen Informationen an Unbekannte weitergeben sollen.

8. SPRECHEN SIE ÜBER GEFAHREN UND SCHUTZMASSNAHMEN IM INTERNET

Damit Kinder zu souveränen und selbstbestimmten Onlinenutzerinnen und Onlinenutzern werden, müssen sie in einem kritischen und verantwortungsbewussten Umgang mit digitalen Medien unterstützt und gefördert werden. Genauso wichtig wie technische Schutzmaßnahmen ist eine offene und vertrauensvolle Gesprächsbasis. Sprechen Sie Ihren Nachwuchs auf Augenhöhe an, zeigen Sie Interesse und Verständnis – auch in schwierigen Situationen. Verbote, Strafen oder der Entzug der Geräte können dazu führen, dass sich Ihre Kinder Ihnen nicht mehr anvertrauen.

9. WAHREN SIE DIE PRIVATSPHÄRE VON KINDERN UND JUGENDLICHEN

Kinder und Jugendliche haben nach Artikel 16 der UN-Kinderrechtskonvention ein Recht auf Privatsphäre. Passen Sie die Kinderschutzsoftware an das Alter des Kindes an, informieren Sie es über die hinterlegten Einstellungen und halten Sie ein angemessenes Maß zwischen Privatsphäre und technischen Schutzmaßnahmen.



HINWEIS:

Viele moderne Betriebssysteme bieten bereits integrierte Kindersicherungsfunktionen, die an die jeweiligen Bedürfnisse und dem Alter entsprechend angepasst werden können. Zudem gibt es eine große Auswahl an zusätzlichen Kinderschutzprogrammen von Drittanbietern. Diese Funktionen und Programme ermöglichen es Eltern, den Zugriff auf bestimmte Websites, Apps und Inhalte zu beschränken und auch die Onlineaktivitäten zu kontrollieren.

Weitere Informationen:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Sicher-im-digitalen-Schulalltag/digitaler-schulalltag_node.html

Acht Tipps für den digitalen Familienalltag:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/Wegweiser_kompakt_digitaler_Familienalltag.html

Schritt für Schritt zu Jugendschutzeinstellungen bei Apps, Spielen & Co.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/SfS-Anleitung_Jugendschutzeinstellungen_Apps_Spiele_Co.html

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 Cybersicherheitsthemen, 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 × im Jahr, Print)
☐ Die Lage der IT-Sicherheit in Deutschland (1 × 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 87 53175 Bonn Telefon: +49 (0) 228 999582-0 E-Mail: bsi-magazin@bsi.bund.de Internet: www.bsi.bund.de
Stand:	Juni 2024
Redaktion:	Katrin Alberts, Sonia Golás, Brigitte Hoffmann, Mark Schulz, Bundesamt für Sicherheit in der Informationstechnik; KOMPAKTMEDIEN, Agentur für Kommunikation GmbH, Torstraße 49, 10119 Berlin, www.kompaktmedien.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-Mag24/717-1
Bildnachweise:	Titel: BSI; Seite 3: © BMI/Henning Schacht; Seite 4 – 5 (von links nach rechts): AdobeStock © ipopba; BSI; BSI; AdobeStock © Limitless Visions; AdobeStock © MNStudio; AdobeStock © Summit Art Creation und AdobeStock © Inactive; Seite 6 – 7: © BSI; Seite 9: AdobeStock © ipopba; Seite 10 – 11 (von links nach rechts): AdobeStock © Aon Khanisorn; AdobeStock © phaisarnwong; AdobeStock © New Africa; AdobeStock © visoot; AdobeStock © Donson/peopleimages.com; AdobeStock © standret; AdobeStock © Alessandro Rizzi; AdobeStock © olga_demina; AdobeStock © chokniti; AdobeStock © Климов Максим; AdobeStock © Gorodenkoff; AdobeStock © Syntetic Dreams; AdobeStock © likoper; Seite 12 – 13: © BSI; Seite 14 – 15 (oben): AdobeStock © Sergey Nivens und AdobeStock © DP, (unten): © BSI; Seite 16 – 17: AdobeStock © Sascha; Seite 18: © BSI/bundesfoto Bastian Geza Aschoff; Seite 19: © BSI/bundesfoto Bastian Geza Aschoff; Seite: 21: AdobeStock © Genestro; Seite 22: © BSI/bundesfoto Bernd Lammel; Seite 23 (oben und rechts): © BSI/bundesfoto Bernd Lammel, (unten links un Mitte): © BSI/bundesfoto Bastian Geza Aschoff; Seite 24 – 25: AdobeStock © xyz; Seite 26: © Matthias Rietschel; Seite 27: © BSI und privat; Seite 29: © BSI; Seite 15: © BSI; Seite 32: © Markus J. Feger; Seite 33: AdobeStock © Vikky Mir; © BSI, AdobeStock © The KonG, © BSI, © Fotolia, © BSI, © BSI/bundesfoto Bernd Lammel; Seite 34: privat, privat; Seite 36 – 39: AdobeStock © nongkran_ch, Seite 38: © Markus J.Feger; Seite 40 – 41: AdobeStock © Limitless Visions, © BSI, © BSI; Seite 42: © BSI; Seite 43: © BSI; Seite 45: AdobeStock © vegefox.com; Seite 46 – 47: AdobeStock © nosorogua, AdobeStock © MNStudio; Seite 49: © BSI; Seite 50 – 51: AdobeStock © Natasa Tatarin, © BSI; Seite 52: AdobeStock © David Santos Mendoza; Seite 53: AdobeStock © Summit Art Creations und AdobeStock © Inactive; Seite 54 (oben): AdobeStock © musmellow, (unten): AdobeStock © Mariia Korneeva; Seite 55 – 56 (Verkehrsschilder): AobeStock © Dejan Jovanovic; Seite 57: © BSI

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:


SICHERER
E-MAIL-DIENST?
HAB ICH
GECHECKT!
Bundesamt
für Sicherheit in der
Informationstechnik
Jetzt scannen
und informieren:
IT-Sicherheitskennzeichen
Bundesamt für Sicherheit in der Informationstechnik
Der Hersteller versichert:
Das Produkt entspricht den
Anforderungen des BSI.
Das BSI informiert:
Aktuelles zum Produkt
bsi.bund.de/deutschlandcheckts
E-Mail-Service
IT-Sicherheitskennzeichen
Bundesamt für Sicherheit in der Informationstechnik
Der Hersteller versichert:
Das Produkt entspricht den
Anforderungen des BSI.
Das BSI informiert:
Aktuelles zum Produkt
bsi.bund.de/deutschlandcheckts
Deine Wunsch-E-Mail-Adresse
JETZT REGISTRIEREN >
#Deutschlandcheckts

ICH HAB NICHTS GEMACHT!

Schützen Sie Ihre smarten Geräte vor Schwierigkeiten. Wir helfen Ihnen dabei: einfachabsichern.de

Bundesamt
für Sicherheit in der
Informationstechnik

#einfachaBSIchern