BSI-Magazin 2023/02

Mit Sicherheit

Im Blickpunkt:

Künstliche Intelligenz

IT-Sicherheit in der Praxis

Cybersicherheit für Kommunen: WiBA

Cybersicherheit

CERT-Bund: Bewährte Anlaufstelle und Partner

Das BSI

Neues Labor in Freital: 5G/6G-Sicherheit im Fokus

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Editorial

Liebe Leserin, lieber Leser,

die Bedeutung eines Themas für unsere Gesellschaft können wir daran ablesen, wo es diskutiert wird. Über Künstliche Intelligenz berichten inzwischen neben Branchenblättern auch Tageszeitungen oder gar das Fernsehen. Die Chancen und Risiken der Schlüsseltechnologie sind als Gesprächsthema am Arbeitsplatz, auf Schulhöfen und im Wohnzimmer angekommen, weil Jung und Alt sie nutzt: Sprachassistenzprogramme für Schularbeiten oder Fahrassistenzsysteme für mehr Sicherheit und Bequemlichkeit am Steuer. Wir sorgen jetzt dafür, dass die Cybersicherheit auch ganz nach oben auf die Agenda kommt. Denn: Die Cybersicherheit dieser Schlüsseltechnologie muss Schritt halten und gleichermaßen in unserem Alltag, in Produkten der Wirtschaft ebenso wie in Abläufen von Behörden, verankert sein. Ziel ist es, die Cyberresilienz substanziell zu erhöhen, damit wir Angriffen Stand halten und uns schnell wieder von ihnen erholen können.

Dazu lohnt sich ein Blick in unseren Blickpunkt Künstliche Intelligenz. Wir berichten, wie wir im BSI die Bedrohungsszenarien für Quanten-unterstütztes maschinellen Lernen untersuchen oder in Projekten zu KI-Sicherheit im Auto mit externen Expertinnen und Experten kooperieren. In einem Interview sprechen zwei Expertinnen der Medienaufsicht über das KI-Tool KIVI und wie es dabei hilft, Verstöße gegen Jugendschutz oder Menschenwürde aufzuspüren.

Beim Lesen des BSI-Magazins wird deutlich: Wir agieren keineswegs allein, sondern kooperieren in alle Richtungen, vernetzen uns und verbinden viele Akteure miteinander. Denn wir stehen vor einer gesamtstaatlichen Aufgabe, zu deren Erfüllung Politik, Wirtschaft und Gesellschaft konsequent zusammenarbeiten müssen. Das wird in unserem Fachartikel über die Notwendigkeit globaler Sicherheitsanforderungen für Satelliten ebenso deutlich wie beim Bericht über das Symposium deutschsprachiger Sicherheitsbehörden in Luxemburg zum Thema digitale Verwaltung.

Auch im Spitzengespräch der Vorsitzenden des Verwaltungsrates der European Union Agency for Cybersecurity (ENISA) liegt ein Fokus darauf, dass wir uns über jede Grenze hinweg abstimmen und unterstützen müssen. Dieser Vernetzungsgedanke hat System. Ich bin überzeugt: Nur, wenn Politik, Wirtschaft und Wissenschaft kooperieren, können wir unsere Technologiekompetenzen gezielt einsetzen und einen Cybermarkt Deutschland schaffen. Wenn Bund und Länder zusammenarbeiten, können wir die Digitalisierung voranbringen. Wenn die Staaten der EU an einem Strang ziehen, können wir die Cybersicherheit pragmatisch gestalten.

Deutschland muss sich als Cybernation verstehen. So können wir die nötige Resilienz aufbauen, um der sehr realen Bedrohungslage im Cyberbereich wehrhaft zu begegnen. Das BSI steht als Möglichmacher, Partner und Helfer bereit, die Cybernation Deutschland zu bauen.

In diesem Sinne wünsche ich eine spannende Lektüre.

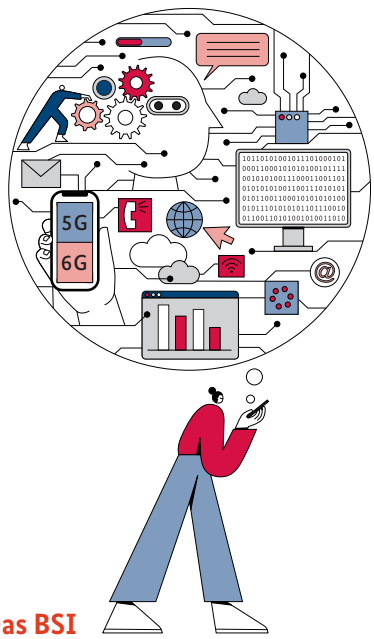
Herzliche Grüße
Ihre

Claudia Plattner
Präsidentin des Bundesamts für Sicherheit
in der Informationstechnik

Inhalt

Cybersicherheit

Im Blickpunkt: Künstliche Intelligenz



Das BSI

IT-Sicherheit in der Praxis

BSI International

Digitale Gesellschaft

Aktuelles

V. l. n. r.: Dirk Wieseler (BSI), Dr. Lydia Hüskens (Ministerin für Infrastruktur und Digitales in Sachsen-Anhalt), Dr. Gerhard Schabhüser (BSI-Vizepräsident), Ariane Steinke (BSI), Axel Gerster (CISO Sachsen-Anhalt)

BSI und das Land Sachsen-Anhalt unterzeichnen Kooperationsvereinbarung

Das BSI und das Land Sachsen-Anhalt, vertreten durch das Ministerium für Infrastruktur und Digitales, haben eine Kooperationsvereinbarung geschlossen. Diese konkretisiert die bisherige Zusammenarbeit in insgesamt neun spezifischen Kooperationsfeldern und legt Schwerpunkte für die kommenden Jahre fest. Im Fokus stehen u. a. gemeinsame Sensibilisierungsmaßnahmen, ein weiterhin enger und vertrauensvoller Austausch von Cybersicherheitsinformationen sowie gegenseitige Hospitationen. BSI-Vizepräsident Dr. Gerhard Schabhüser sagte anlässlich der Unterzeichnung: „Die sichere Gestaltung der Digitalisierung ist mir ein besonderes Anliegen und kann nach meiner Überzeugung nur gemeinsam von Bund und Ländern zum Erfolg geführt werden. Mit dem Land Sachsen-Anhalt verbindet uns eine langjährige Zusammenarbeit, die wir mit diesem Schritt bekräftigen. Gemeinsam setzen wir damit einen verbindlichen Rahmen der bilateralen Kooperation. Wir freuen uns, gemeinsam mit dem Land Sachsen-Anhalt, das Thema Cybersicherheit in Deutschland weiter voranzubringen.“ Das BSI vertieft mit den Kooperationsvereinbarungen kontinuierlich die Zusammenarbeit zwischen dem Bund und den Ländern weiter.

Chefetage im Blick: Publikationsreihe Management Blitzlicht gestartet

Mit der neuen Publikationsreihe Management Blitzlicht informiert das BSI Unternehmensleitungen schnell und kompakt über aktuelle Themen der Cybersicherheit.

Die ersten Ausgaben sind zu den Themen Cyber-Supply Chain Risk Management und Zero-Trust-Architekturen erschienen. Das Management Blitzlicht „Zero Trust: Ein ganzheitlicher Sicherheitsansatz“ beschreibt beispielsweise die Grundlagen des Zero-Trust-Ansatzes und zeigt, welche sieben Schritte zur erfolgreichen Umsetzung von Zero Trust erforderlich sind.

Weitere Informationen:

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

Basiskurs für Digitale Ersthelfer: Qualifikationsangebot für Vorfallbearbeitung im Unternehmen

Das BSI bietet Unternehmen die Möglichkeit, ihre Mitarbeiterinnen und Mitarbeiter in einem Basiskurs zu Digitalen Ersthelfern qualifizieren zu lassen. In dem Kurs lernen die Teilnehmenden Erste-Hilfe-Maßnahmen bei IT-Störungen und kleineren IT-Sicherheitsvorfällen. Sie erhalten zudem Kenntnisse, wie die digitale Rettungskette des Cyber-Sicherheitsnetzwerks (CSN) aufgebaut ist, sodass sie im Falle eines IT-Sicherheitsvorfalls als Schnittstelle mit den Helfenden des CSN kommunizieren können. Der Basiskurs steht als Onlinekurs zum Selbststudium kostenfrei auf der CSN-Webseite zur Verfügung.

Weitere Informationen:

https://www.bsi.bund.de/dok/947558

Cyberstudiengang DACS: Erster Jahrgang diplomiert

Die ersten Absolventinnen und Absolventen des dreijährigen Studiums „Digital Administration and Cyber Security“ (DACS) haben erfolgreich ihre Abschlussprüfungen absolviert. Vier Semester Theorie an der Hochschule des Bundes und zwei Praxissemester in unterschiedlichen Bereichen beim BSI haben die jungen Fachkräfte fit für einen Job in der Cybersicherheit gemacht. BSI-Präsidentin Claudia Plattner freut sich über die neuen Kolleginnen und Kollegen: „Cybersicherheit in Deutschland braucht digitale Talente und das BSI hat wahnsinnig spannende Jobs. Der DACS-Studiengang bietet damit eine absolute Win-win-Situation für alle Beteiligten. Ich freue mich, dass wir nun die ersten Absolventinnen und Absolventen im BSI begrüßen dürfen, die mit einem engagierten Team das Cybersicherheitsniveau in Deutschland weiter erhöhen werden.“

Cyber-Supply Chain Security – Bedeutung, Inhalte und Risiken im Überblick

Die zunehmende Digitalisierung der Lieferketten birgt Chancen und Risiken zugleich

von Salsabil Hamadache und Raphael Miether, Referat Kooperation mit Herstellern und Dienstleistern

Führungskräfte sind besorgt über Schwachstellen in ihrer Lieferkette – zu Recht: Laut dem Global Cybersecurity Outlook 2022 des World Economic Forums gaben fast 40 Prozent der Befragten an, dass sie von einem Cybersicherheitsvorfall im Zusammenhang mit Drittanbietern beziehungsweise liefernden Firmen negativ betroffen waren. 58 Prozent der befragten CEOs hielten ihre Geschäftspartner und Zulieferbetriebe für weniger widerstandsfähig als ihre eigene Organisation.

Heutige Lieferketten sind weit verzweigte, global vernetzte Systeme, in denen Institutionen sowohl aus dem öffentlichen als auch aus dem privaten Sektor eng zusammenarbeiten. Dazu gehören Einkäufer, Lieferanten, Entwickler, Systemintegratoren, Dienstleister und weitere Fachleute aus verschiedensten Bereichen, die gemeinsam Produkte und Dienstleistungen erforschen, entwickeln, herstellen, beschaffen, liefern, integrieren und in vielfältiger Weise nutzen oder verwalten. Dabei spielt die Cybersicherheit eine zentrale Rolle, da diese Interaktionen von einer breiten Palette von Technologien, gesetzlichen Rahmenbedingungen und strategischen Ansätzen geprägt und beeinflusst werden, um die Integrität und Sicherheit dieser globalen Lieferketten zu gewährleisten. Die Absicherung solch komplexer Systeme stellt eine enorme Herausforderung dar und kann nur über ganzheitliche Sicherheitskonzepte realisiert werden.

SCHMERZHAFTE ERFAHRUNGEN

Einer der bis heute prominentesten Lieferkettenangriffe ist der Angriff auf das Netzwerk-Monitoring-Tool Orion der Firma Solarwinds. Angreifern war es gelungen, Zugriff auf das Build-System des Unternehmens zu erlangen und über einen längeren Zeitraum einen Schadcode einzuschleusen, der dann in Form von Updates an die Kundschaft von Solarwinds verteilt wurde. Der Angriff diente hauptsächlich der Spionage und blieb damit weit unter dem eigentlichen Schadenspotenzial, dennoch sind die Komplexität und die Auswirkungen des Angriffs beträchtlich. Das modifizierte Update wurde an 18.000 Nutzerinnen und Nutzer ausgeliefert, darunter US-Behörden wie das Finanzministerium oder die Nationale Verwaltung für Nukleare Sicherheit (NNSA). Der Angriff gilt bis heute als Textbuchversion eines Supply-Chain-Angriffs (Advanced Persistent Threat).

Ein weiteres bekanntes Beispiel für eine Sicherheitslücke in der Lieferkette ist „log4shell“. Dabei handelte es sich um eine Sicherheitslücke in dem beliebten Java-Logging-Framework log4j. Die Schwachstelle erlaubte es Angreifern, einen beliebigen Code auf den betroffenen Systemen auszuführen. Besonders problematisch war die weite Verbreitung des Open-Source-Frameworks, das Bestandteil vieler Produkte namhafter Hersteller war. Auch dieser Vorfall zeigt, dass gerade die Intransparenz in Softwarelieferketten zu schweren Sicherheitsvorfällen führen kann.

REGULATORISCHE VORGABEN

Die Politik reagiert auf die Lage und adressiert das Thema Lieferkettensicherheit in zwei kommenden Regulierungsvorhaben. So werden unter Artikel 21 der NIS-2-Direktive bzw. Paragraf 30 des Umsetzungsgesetzes wesentliche und wichtige Einrichtungen aufgefordert, geeignete und verhältnismäßige technische, betriebliche und organisatorische Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit nach dem „All-Hazards-Approach“ zu ergreifen. Konkret werden Unternehmen, die in den Geltungsbereich fallen, verpflichtet, ein Cyber-Supply Chain Risk Management (C-SCRM) zu etablieren. Um ein funktionierendes C-SCRM aufsetzen zu können, bedarf es wiederum einer Vielzahl von Prozessen,

Hier finden Sie die Broschüre:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Management_Blitzlicht_C-SCRM.html

die u. a. die nötige Transparenz in die Lieferkette bringen, wie etwa durch die Einrichtung eines Lieferantenregisters und den Betrieb eines IT-Asset-Managements. Weiterhin müssen Faktoren wie die Cybersicherheitspraktiken der zuliefernden Unternehmen für eine entsprechende Risikobewertung herangezogen werden. Die Prüfung und Erweiterung bestehender Verträge ist hier eine logische Konsequenz, um den Anforderungen der NIS-2-Direktive gerecht zu werden.

Ein weiteres Regulierungsvorhaben der EU ist der Cyber Resilience Act (CRA). Mit diesem soll zukünftig ein einheitlicher Rechtsrahmen für den gesamten Binnenmarkt der EU geschaffen werden. Dieser wird Voraussetzungen im Bereich der IT-Sicherheit für das Inverkehrbringen von Produkten mit digitalen Elementen festlegen, darunter Mindestanforderungen an das IT-Sicherheitsniveau. Diese müssen von fast allen Produkten mit digitalen Elementen eingehalten werden – angefangen bei Smart-Home-Geräten bis hin zu gesamten Betriebssystemen. Die Anforderungen werden die Sicherheit über den gesamten Produktzyklus (Planung, Konzeption, Entwicklung, Herstellung, Lieferung, Wartung) inklusive der Verwendung von Komponenten Dritter berücksichtigen.

Neben den geplanten Gesetzesvorhaben gelten für bestimmte Sektoren bereits heute Vorgaben im Bereich Lieferkettensicherheit. So ist etwa der Finanzsektor durch den Digital Operations Resilience Act (DORA) reguliert, der unter Kapitel V Anforderungen an das Management von IKT-Drittparteienrisiken stellt. Die Radio Equipment Directive (RED), welche hier in Deutschland durch das Funkanlagengesetz umgesetzt wird, regelt die Lieferketten von auf dem europäischen Markt bereitgestellten Funkanlagen.

ÖKONOMISCHE ASPEKTE

Mit Beginn der Corona-Pandemie zeigte sich die Relevanz ökonomischer Aspekte wie Produktverfügbarkeit und verlängerte Lieferzeiten. Insbesondere die Halbleiterindustrie hatte mit starken Lieferengpässen zu kämpfen. Der russische Angriffskrieg gegen die Ukraine verschärfte die Situation zudem, da Lieferwege von für die Halbleiterherstellung benötigten Edelgasen abgeschnitten wurden. Diese Situation ist als indirektes Risiko für die Cybersicherheit zu bewerten, da Lieferantenwechsel notwendig werden – unter Umständen zu weniger vertrauenswürdigen Lieferanten, die neue Angriffsvektoren öffnen, etwa durch Counterfeiting. Um dieses Risiko zu minimieren und gleichzeitig die digitale Souveränität Europas zu stärken, möchte die Europäische Kommission mithilfe des European Chip Act den europäischen Marktanteil im Halbleiterbereich bis 2030 auf 20 Prozent verdoppeln. Da die Abhängigkeiten aber nicht erst bei den fertigen Halbleitern beginnen, sondern schon beim Rohmaterial, soll mithilfe des Critical Raw Materials Act gleichzeitig die Versorgung mit seltenen Erden und anderen wichtigen Rohmaterialien sichergestellt werden.

Counterfeiting, vor allem im Bereich der Halbleiter bekannt, bezeichnet die illegale Herstellung und Verbreitung gefälschter Komponenten, die als echte Produkte verkauft werden, aber minderwertig oder sogar schädlich sein können.

NEUE ANSÄTZE EBNEN DEN WEG ZU ERHÖHTER LIEFERKETTENSICHERHEIT

Lieferkettensicherheit ist komplex und erfordert eine ganzheitliche Betrachtung. Grundsätzlich mangelt es nicht an technischen Lösungen. Doch für die Absicherung der Lieferkette reichen diese allein nicht aus. Sie sind viel mehr als Werkzeuge zu betrachten: Im Bereich der Softwarelieferketten erhöht eine Software Bill of Material (s. auch Artikel auf S. 12) die Transparenz. Auch verkürzt die Nutzung maschinenles-

barer Security-Advisories – wie im Common Security Advisory Framework (CSAF) beschrieben – die Reaktionszeit auf eine bekannt gewordene Sicherheitslücke deutlich. Lieferkettensicherheit kann jedoch nur mithilfe ganzheitlicher Sicherheitskonzepte gewährleistet werden.

Zu erprobten Maßnahmen zählen etwa das IT-Asset-Management, das Cyber-Supply Chain Risk Management (C-SCRM) und die entsprechende Beachtung der Thematik in Awareness-Maßnahmen. Diese Maßnahmen werden für viele Unternehmen durch die kommenden Regulierungsvorhaben verpflichtend.

Das BSI unterstützt mit zahlreichen Angeboten wie etwa dem CyberRisikoCheck, der kleinen und mittleren Unternehmen (KMU) eine Positionsbestimmung des eigenen IT-Sicherheitsniveaus ermöglicht. Er zeigt auch auf, welche konkreten Maßnahmen umgesetzt werden sollten. Da KMU einen großen Teil der Lieferketten ausmachen, aber gleichzeitig eher kleinere Budgets für Cybersicherheit zu Verfügung haben, ist diese niederschwellige Hilfe essenziell.

Ein weiteres wichtiges Element ist die Technische Richtlinie TR-03183-2, die Anforderungen an eine Software Bill of Materials beschreibt. Nicht nur sind SBOMs eine Anforderung des CRA, vielmehr sind sie der einzige Weg, Informationen über Abhängigkeiten in Softwarekomponenten interoperabel über Unternehmensgrenzen hinweg zu teilen.

Lieferkettensicherheit muss Chefsache sein. Deshalb schildert das „Management Blitzlicht“, ein neues Publikationsformat des BSI für die Chefetage, in seiner ersten Ausgabe, wie der Aufbau eines effektiven C-SCRM gelingt. Mehr Details bietet das Handbuch „Management von Cyber-Risiken“ der Allianz für Cyber-Sicherheit. Da die Lieferkettensicherheit fast alle Bereiche eines Unternehmens betrifft, sind die nötige Aufmerksamkeit des Managements sowie die Bereitstellung der benötigten Ressourcen eine unverzichtbare Grundvoraussetzung. ■

Lieferkettenrisiken bedrohen...

...Ihre Handlungsfähigkeit.

...Ihre Firmengeheimnisse.

...Ihre Vertrauenswürdigkeit.

...Ihre Reputation.

Weitere Informationen:

https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

https://www.spektrum.de/news/solarwinds-ein-hackerangriff-der-um-die-welt-geht/1819187

Mehr Sicherheit in der Lieferkette dank SBOM

Eine Software Bill of Materials (SBOM) dokumentiert Bestandteile von Softwareprodukten und hilft so, Schwachstellen aufzudecken

von Anna Thurm, Referat Marktaufsicht über zertifizierte Dienstleister und Produkte

In einer SBOM werden sowohl kommerzielle als auch freie Softwarebestandteile von Produkten festgehalten. So macht die Softwarestückliste Abhängigkeiten von Komponenten Dritter transparent und hilft damit Herstellern, Sicherheitsforschenden sowie professionellen Anwenderinnen und Anwendern beim Monitoring von Schwachstellen.

WAS IST EINE SBOM?

Eine Software Bill of Materials ist eine Liste der Bestandteile einer Software. Sie gibt an, welche eigenen oder fremden Komponenten (z. B. Bibliotheken) in der Software verwendet werden. Da fast immer viele unterschiedliche Quellen und Komponenten im Softwareentwicklungsprozess eingesetzt werden, sind SBOMs ein wichtiges Instrument zur transparenten Darstellung der Softwarelieferkette. Eine SBOM ist damit vergleichbar mit einer Zutatenliste bei Lebensmitteln. Sie wird automatisiert erstellt und liegt im Ergebnis als maschinenlesbare Datei vor.

NUTZEN VON SBOMS

Werden Informationen zu einer Schwachstelle in einer Software oder Softwarebibliothek bekannt, stehen Hersteller, Betreiber und Administratoren vor der schwierigen Aufgabe herauszufinden, ob die von ihnen hergestellte oder betriebene Software von dieser Schwachstelle betroffen ist. Mit einer SBOM haben sie eine Liste der verwendeten Komponenten zur Verfügung und können so leichter prüfen, ob in ihrem Fall Handlungsbedarf besteht. Dazu wird die Komponentenliste des Produktes mit Informationen zu Schwachstellen von Komponenten aus Schwachstellendatenbanken abgeglichen.

VERSCHIEDENE FORMEN EINER SBOM

Besonders aussagekräftig ist eine SBOM, wenn die aufgeführten Komponenten der beschriebenen Software jeweils wiederum in ihre Bestandteile zerlegt werden. So werden auch indirekte Abhängigkeiten über mehrere Ebenen transparent gemacht. SBOMs können also einen unterschiedlichen Detaillierungsgrad aufweisen und danach charakterisiert werden. Zudem werden sie danach klassifiziert, in welchem Stadium der Softwareerstellung sie erzeugt wurden, z. B. auf Basis des verwendeten Quelltexts (Source SBOM) oder als Teil des Build-Prozesses (Build SBOM).

GESCHICHTE DER SBOM

Ursprünglich wurden SBOMs genutzt, um einen Überblick über die verschiedenen Lizenzen der eingebundenen Softwarekomponenten zu erhalten. Mit dem hinzugekommenen Nutzen für die Sicherheit in der Softwarelieferkette haben SBOMs auch Eingang in gesetzliche Anforderungen gefunden. Mit der Executive Order 14028 von 2021 wird für Software, die von der US-Regierung erworben wird, eine SBOM gefordert. Eine solche SBOM muss den Anforderungen der National Telecommunications and Information Administration (NTIA) genügen, die unter dem Titel „The Minimum Elements For a Software Bill of Materials (SBOM)“ veröffentlicht wurden.

ZUKUNFT VON SBOM

SBOMs gehören zu den zentralen Forderungen des europäischen Cyber Resilience Act (CRA). Dieser liegt seit September 2022 als Entwurf der EU-Kommission vor und befindet sich derzeit im Gesetzgebungsverfahren. Hersteller von Produkten mit digitalen Elementen sollen darin verpflichtet werden, zum Schwachstellenmanagement eine SBOM zu pflegen. Eine Veröffentlichung der SBOM wird aber nicht verlangt. Sie muss lediglich auf Verlangen der Marktüberwachungsbehörde vorgelegt werden.

WELCHE FORMATE GIBT ES FÜR SBOM?

Zur Darstellung und Übertragung einer SBOM existieren unterschiedliche Formate. Am weitesten verbreitet sind SPDX und CycloneDX. Wesentliche Informationen, z. B. die von der NTIA oder in der Technischen Richtlinie des BSI geforderten Datenfelder, können in beiden Formaten dargestellt werden. Nutzt man den vollen Umfang der möglichen Inhalte des jeweiligen Formats, sind sie aber nicht komplett verlustfrei ineinander überführbar.

SCHWACHSTELLENINFORMATIONEN UND SBOMS

Eine SBOM selbst enthält keine Aussage zu Schwachstellen oder deren Ausnutzbarkeit. Ob und in welchem Maße durch eine Schwachstelle einer Softwarekomponente ein Risiko für das Produkt besteht, das durch die SBOM beschrieben wird, geht aus der Liste nicht hervor. Hierzu sind weitere Informationen über die konkrete Schwachstelle erforderlich, beispielsweise mittels Schwachstelleninformationen (sogenannter Security-Advisories) in den Formaten Common Security Advisory Framework (CSAF) oder Vulnerability Exploitability eXchange (VEX).

Empfehlungen des BSI für SBOMs

Das BSI hat im August 2023 die Technische Richtlinie TR-03183-2 mit formellen und fachlichen Vorgaben zu SBOM als Handreichung veröffentlicht. In der TR-03183-2 werden z. B. notwendige Datenfelder, der notwendige Umfang und die möglichen Formate definiert. Diese Anforderungen haben bisher nur empfehlenden Charakter und sollen Orientierung bieten sowie auf mögliche Vorgaben von der EU-Kommission vorbereiten.

Weitere Informationen:

https://www.bsi.bund.de/dok/TR-03183

Prävention und Reaktion

CERT-Bund: Bewährte Anlaufstelle und Partner

Stefan Ritter, Fachbereichsleiter CERT-Bund, über die Arbeit des Computer Emergency Response Teams (CERT) der Bundesverwaltung im Spannungsfeld dynamischer Bedrohungslagen, über die Vernetzung von CERT-Bund und seine Erwartungen an ein besonderes CERT-Bund-Jahr 2024

Herr Ritter, was macht eigentlich das Team von CERT-Bund?
Stefan Ritter: CERT-Bund informiert und warnt die Bundes- und auch Landesverwaltungen, seine nationalen und internationalen Partner, die Betreiber kritischer Infrastrukturen sowie Wirtschaft und Gesellschaft vor besonders relevanten und neuen Schwachstellen und Angriffen.

Das Arbeitsfeld aller CERTs ist seit der Gründung des CERT im BSI 1994 stark gewachsen. Für die vielfältigen Aufgaben sind wir intern wie extern gut aufgestellt, denn wir bewegen uns intensiv innerhalb nationaler und internationaler CERT-Communitys. Je nach Vorfall wägen wir vertrauensvoll und verantwortungsbewusst „need to share“ gegen „need to know“ ab, d. h., auf welcher Ebene und in welchem Kreis jeweils ein übergreifender Austausch erforderlich ist. Konkret findet dieser Austausch im deutschen CERT-Verbund und dem VerwaltungsCERT-Verbund mit den BundesländerCERTs statt. Internationale CERT-Communitys sind beispielsweise das EU-CSIRT-Netzwerk oder die NATO. Hinzu kommen zahlreiche vertrauensvolle informelle Kreise und bilaterale Kontakte. Übungen wie die EU Cyber Europe oder die NATO Cyber Coalition stärken die Vernetzung und den Austausch über kollaborative Plattformen mit Funktionalitäten für Chats und Indikatorenaustausch (MISPs) weiter.

Im Bereich der Reaktion stellt CERT-Bund eine große Bandbreite an Hilfen und Unterstützungsmöglichkeiten bereit. Das Angebot reicht von konkreten Hilfeanleitungen, Beratungsgesprächen mit Expertinnen und Experten, punktueller Entlastung und Unterstützung durch ausgewählte technische Analyse relevanter Systeme bis hin zur kompletten Vorfallunterstützung mit Vorfallbearbeitung in einem Mobile Incident Response Team (MIRT) vor Ort und im Backoffice.

Was macht Ihre tägliche Arbeit heute aus, mit welchen Cyberbedrohungen ist CERT-Bund konfrontiert?
Ritter: Ich möchte zwei Beispiele aus unserer Arbeit nennen. Nachdem wir im vergangenen Jahr die BSI Coordinated Vulnerability Disclosure (CVD) Policy veröffentlicht haben, ist das Aufkommen an Meldungen an das BSI zu bislang unbekannten Schwachstellen in Produkten innerhalb und außerhalb der Verwaltung signifikant gestiegen. Dank dieser Meldungen können wir mit dem Warn- und Informationsdienst (WID) meist vor der tatsächlichen Ausnutzung der Schwachstellen durch Angreifer die Bedrohung abwenden.

Seit Jahresanfang unterstützen unsere Incident-Handler und -Analysten Betroffene bei Angriffen auf die Supply-Chain – auch auf IT-Dienstleister des Bundes – bei der Analyse und Bewältigung der Vorfälle. Dabei kümmert sich CERT-Bund um die besonders schweren Vorfälle wie staatliche APT-Angriffe und – im Rahmen verfügbarer Ressourcen – um neuartige Ransomware-Angriffe, die neue, aufwendige und technisch besonders herausfordernde Lösungen erfordern. APT-Angriffe und Ransomware sehen wir weiter als die größten Gefahren im Cyberraum. Und zukünftig wird die sogenannte Zeitenwende infolge des russischen Angriffskriegs gegen die Ukraine und die dedizierte Haltung gegenüber China diese Herausforderungen weiter intensivieren und neue Formen von Vorfällen hervorbringen.

Eine besondere Herausforderung bei den Angriffen stellt die Reaktion und Betreuung der indirekt Betroffenen dar, also der Kunden und Geschäftspartner der Betroffenen, die indirekt vom Vorfall berührt sind. Bei ihnen kann es kurzfristig zu längeren Nichtverfügbarkeitszeiten der eingekauften Dienstleistung kommen oder zur Sorge um die eigenen Netze (mögliches Lateral Movement) und Angst vor Informations- und Datenverlust. Hier müssen die Krisenkommunikation der Betroffenen, aber auch die Eigensicherungsmaßnahmen der Partner funktionieren.

Wie funktioniert die internationale Kooperation der CERTs?
Ritter: Angriffe auf IT und im Cyberraum können jederzeit und von überall stattfinden. Die Bedrohungslage ist tatsächlich ebenen- und grenzenlos! Genau deshalb sind Netzwerke nationaler wie internationaler Art so wertvoll für CERT-Bund und alle anderen Notfallteams. Der vertrauensvolle und regel-

„Angriffe auf IT und im Cyberraum können jederzeit und von überall stattfinden. Die Bedrohungslage ist tatsächlich ebenen- und grenzenlos!“

mäßige Austausch darin ist so vielfältig wie hilfreich. Egal, ob Sie kurzfristig einen Ansprechpartner für eine vertrauliche Frage oder einen Hinweis zu einem neuen Angriffsvektor benötigen, oder ob Sie erfahren oder checken möchten, welcher Lösungsansatz zur Behebung eines neuartigen Angriffs funktioniert. Im Austausch mit internationalen Partnern können die CERT-Profis Wissen teilen und voneinander profitieren. Hierfür sind Vernetzung und Austausch unverzichtbar!

Wie kann CERT-Bund mit der fortschreitenden Bedrohungslage und der dynamischen Entwicklung in der Digitalisierung Schritt halten?

Ritter: Einen zentralen Anteil daran haben die Kolleginnen und Kollegen im Team CERT-Bund. Sie befassen sich jeden Tag intensiv mit den Vorfällen und den eingesetzten Angriffstools. Durch ihr tägliches Doing und die breit aufgestellte Expertise im Team wissen die Kolleginnen und Kollegen immer, was zu tun ist, wenn es „brennt“. Zu dieser täglichen Praxis kommen natürlich ausgewählte Lehrgänge und die Teilnahme an Fachkonferenzen sowie der schon erwähnte Austausch in der CERT-Community hinzu. Und bislang hat unser Amt uns als CERT hier die Flexibilität und Freiheit gegeben, diese Kreativität und Professionalität zur Bewältigung von Lagen einzusetzen und die Betroffenen davon profitieren zu lassen. Natürlich hilft auch der Rechtsrahmen mit unseren Befugnissen, die uns Handlungssicherheit geben.

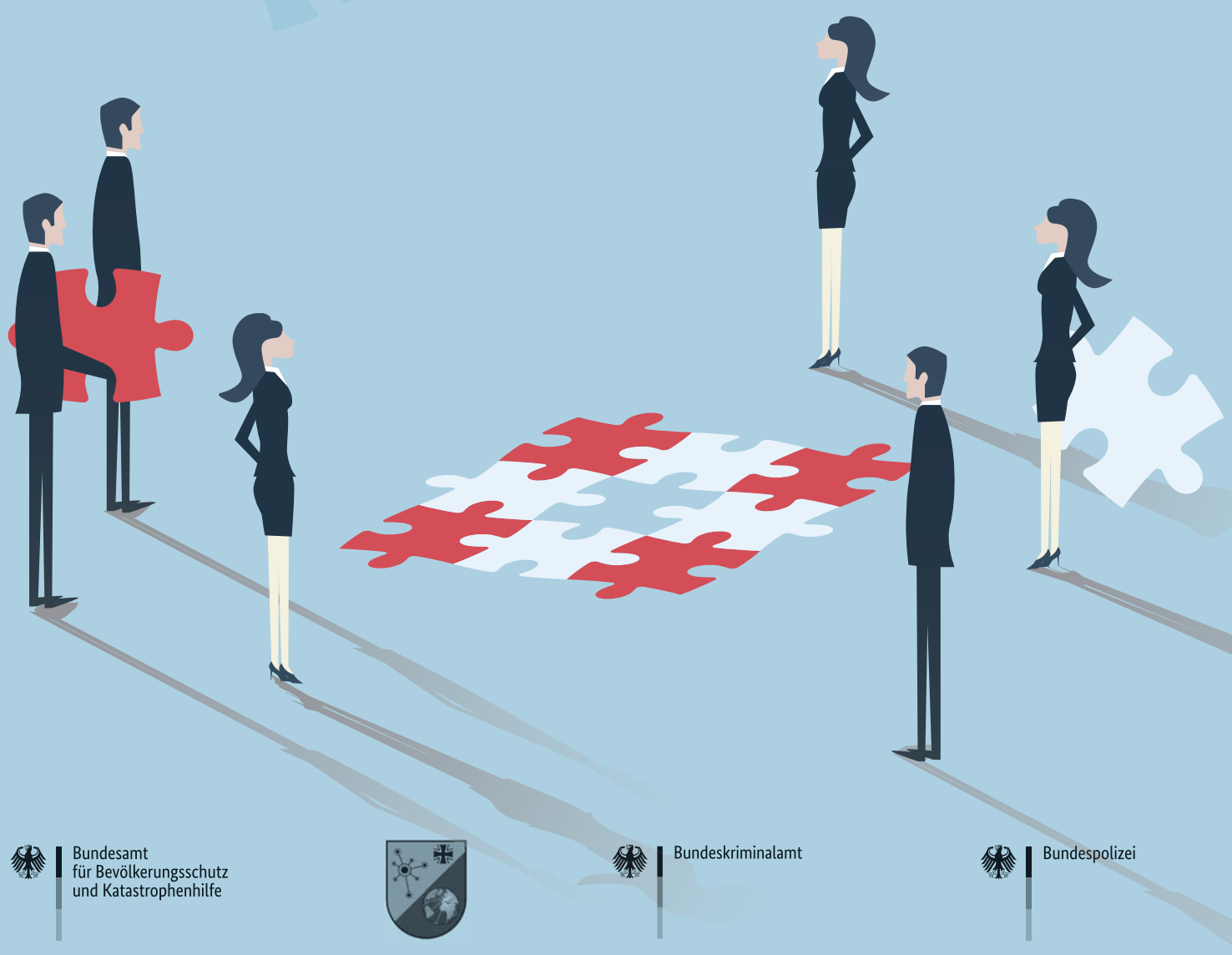
Im kommenden Jahr wird CERT-Bund im BSI 30 Jahre alt: Was bedeutet dieses besondere Jubiläum?

Ritter: 30 Jahre sind schon eine besondere Zahl! Die Bedingungen, unter denen wir damals gestartet sind, sind mit den heutigen nicht mehr vergleichbar. CERT-Bund hat in der Zeit viel geleistet und ist heute die etablierte fachliche Anlaufstelle für seine Zielgruppen beim Warn- und Informationsdienst und vor allem bei Notfällen. Wir freuen uns darauf, die vergangenen Jahre Revue passieren zu lassen und 2024 das Jubiläum mit aktuellen und früheren Wegbegleiterinnen und Wegbegleitern von CERT-Bund in unterschiedlichen Formaten zu feiern. ■

It’s always the single parts that make the big picture!

NATIONALES CYBER-ABWEHRZENTRUM

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



Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Bundeskriminalamt

Bundespolizei

NATIONALE SICHERHEITSSTRATEGIE: Die Bundesregierung veranlasst, dass alle maßgeblichen Akteure zu einem ganzheitlichen Cyberlagebild beitragen. Die darin enthaltenen Informationen werden analysiert und aus gesamtstaatlicher Sicht bewertet. Die Bundesregierung wird hierzu insbesondere die Aufklärungs-und Frühwarnfähigkeiten der betroffenen Behörden und Einrichtungen, vor allem der Nachrichtendienste, verbessern. Die für das Lagebild erforderliche Koordinierungsfunktion wird zunächst im Nationalen Cyber-Abwehrzentrum eingerichtet.

„Der große Wert des Nationalen Cyber-Abwehrzentrums als Kommunikations-, Koordinierungs- und Informationsplattform ergibt sich aus dem schnellen und flexiblen Austausch und der Abstimmung von Maßnahmen bei der Bewältigung von Cybervorfällen."

Erik Schäfer
Polizeidirektor, zuständiger Referent für Cybersicherheit und -abwehr in der Bundespolizei (BPolP)

„Die Mitarbeit im Nationalen Cyber-Abwehrzentrum hat für uns einen großen Wert, da hier IT-Sicherheit und physischer Schutz, z. B. für kritische Infrastrukturen, sehr gut verknüpft werden und der behördenübergreifende Austausch auf dieser Plattform den bei diesem Thema nötigen ganzheitlichen Ansatz erfolgreich zu etablieren hilft."

Dr. Wolfram Geier
Abteilungsleiter Risikomanagement und Internationale Angelegenheiten im Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

„Das Nationale Cyber-Abwehrzentrum ist ein zentraler Baustein in der Cybersicherheitsarchitektur Deutschlands. Wir tauschen uns täglich über die Bedrohungslage aus. Das Nationale Cyber-Abwehrzentrum hat sich bereits mehrfach als wichtiges Instrument der gemeinsamen Lagebewertung und Koordination unserer operativen Maßnahmen bewährt, und das an sieben Tagen in der Woche, rund um die Uhr. Denn in einer vielseitig angespannten Sicherheitslage stellen Cyberbedrohungen eine der wesentlichen Herausforderungen für die deutschen Sicherheitsbehörden dar."

Henrike Stein
Leitende Regierungsdirektorin im Bundesverfassungsschutz (BfV)

„Das Nationale Cyber-Abwehrzentrum ist eine erfolgreiche gemeinsame Plattform, die in Zukunft noch an Bedeutung gewinnen wird. Denn so wie Cyberrisiken sich schnell entwickeln und keine Grenzen kennen, können die zuständigen Behörden in diesem Format bei der Aufklärung und Abwehr dynamisch und niedrigschwellig zusammenwirken."

Dr. Bruno Kahl
Präsident im Bundesnachrichtendienst (BND)

„Das BSI fördert und fordert die Kooperation der Behörden im Nationalen Cyber-Abwehrzentrum. Nur gemeinsam können wir erfolgreich sein."

Claudia Plattner
Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

„Das Nationale Cyber-Abwehrzentrum ist ein wichtiger Bestandteil der gesamtstaatlichen Cyberabwehr. Unsere Beteiligung als Organisationsbereich Cyber- und Informationsraum am Nationalen Cyber-Abwehrzentrum liefert uns wichtige Erkenntnisse für die Erfüllung unserer Aufgabe, nämlich den Schutz der Streitkräfte im Cyberraum."

Dr. Thomas Daum
Vizeadmiral, Inspekteur Cyber- und Informationsraum (KdoCIR)

Bundesamt für den Militärischen Abschirmdienst

Bundesnachrichtendienst

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Verfassungsschutz

Künstliche Intelligenz

Chancen und Risiken großer KI-Sprachmodelle

Die Technologie hat sich rasant entwickelt – die Sicherheitsvorkehrungen müssen nun Schritt halten

von Tobias Alt und Anna Wilhelm, Referat Sicherheit in der Künstlichen Intelligenz

Große KI-Sprachmodelle verfügen über bemerkenswerte Fähigkeiten und bieten Chancen für verschiedene Anwendungsszenarien. Gleichzeitig bergen sie neuartige Risiken, die einerseits in der Natur der Technologie selbst und andererseits in der gezielten Ausnutzung durch Angreifer begründet sind. Eine Publikation des BSI klärt über Möglichkeiten und Herausforderungen auf, das Wichtigste hier in Kürze.

NEURONALES NETZ IM HINTERGRUND

Ein großes KI-Sprachmodell, abgekürzt LLM (englisch: Large Language Model), ist ein statistisches Modell und gehört der Familie der generativen KI an. Letztere ist darauf ausgerichtet, Muster aus vorhandenen Daten zu erlernen und neue Daten und Inhalte zu erstellen, die ebenfalls diesen Mustern folgen. Ein LLM erzeugt zu einer bestimmten Texteingabe (sogenanntem Prompt) eine Textausgabe, die gemäß dem Modell als wahrscheinlich erscheint und eine möglichst passende Fortsetzung der Eingabe darstellt. Dabei liegt dem Modell meist ein neuronales Netz mit Milliarden oder gar Billionen von Parametern (daher auch der Begriff großes KI-Sprachmodell) zugrunde, das die Wahrscheinlichkeitsverteilung während des Trainingsprozesses anhand umfangreicher Textkorpora erlernt.

CHANCEN VON LLMS

Grundsätzlich können LLMs überall dort eingesetzt werden, wo Text (teil-)automatisiert verarbeitet werden kann. Die Anwendungsmöglichkeiten reichen von der klassischen Bearbeitung (z. B. Korrektur von Rechtschreibung) über die Verarbeitung (z. B. Klassifikation, Erstellung von Zusammenfassungen) bis hin zur Generierung (z. B. Verfassen von Texten eines bestimmten Stils). LLMs können dabei unterstützen, Fragen in Chatbots zu beantworten, unerwünschte Inhalte wie Hatespeech in sozialen Netzwerken aufzuspüren oder Programmcodes zu generieren und optimieren (u. a. zur Effizienzsteigerung, Fehlerkorrektur, Schließung von Sicherheitslücken).

RISIKEN VON LLMS

Eine erste Gruppe von Risiken entsteht aufgrund des probabilistischen Charakters von LLMs, da sie Text auf Basis stochastischer Zusammenhänge generieren. Dadurch ist nicht garantiert, dass der Text faktisch korrekt ist; ein Erfinden von Inhalten, die nicht Teil der Eingabe oder des Trainingsdatensatzes waren, wird als Halluzinieren bezeichnet. Zugleich wirken die generierten Texte aufgrund der hohen sprachlichen Qualität überzeugend, weshalb die ungeprüfte Nutzung kritisch ist. Hinzu kommen fehlende Reproduzierbarkeit und Aktualität der Ausgaben und ihres Inhalts, mögliche Sicherheitslücken im generierten Programmcode sowie fehlerhafte Reaktionen auf Prompts, die stark von den Trainingsdaten abweichen.

Die zweite Gruppe von Risiken basiert auf einer missbräuchlichen Nutzung. Aufgrund ihrer Fähigkeit, Ausgaben in verschiedenen Sprachen zu erzeugen und Schreibstile von Personen oder Organisationen zu imitieren, können LLMs für die Erstellung von Social-Engineering-Inhalten oder Falschinformationen verwendet werden. Greift ein LLM auf soziale Netzwerke zu, werden diese Inhalte unter Umständen mit persönlichen bzw. unternehmensspezifischen Informationen angereichert.

Eine dritte Gruppe von Risiken entsteht durch Angriffe, z. B. in Form von sogenannten Prompt Injections. Mittels spezieller Texteingaben wird das Verhalten des Modells beeinflusst, sodass Beschränkungen und Filtermechanismen bei der Verarbeitung und Generierung von Textausgaben umgangen werden. Greifen LLMs auf externe Inhalte wie Webseiten zu, können Angreifende dort Anweisungen platzieren, die ausgeführt werden, sobald die Webseite ausgewertet werden soll. In diesem Fall spricht man von „Indirect Prompt Injection“.

RISIKOANALYSE UND -BEHANDLUNG

In vielen LLMs bzw. LLM-basierten Anwendungen sind Maßnahmen implementiert, die schadhafte Ein- und Ausgaben herausfiltern. Diese schützen meist nur teilweise vor Missbrauchs- und Angriffsszenarien und bieten z. B. keinen Schutz vor Halluzinationen der LLMs. Nutzende müssen sich daher der Risiken bewusst sein und Ausgaben gewissenhaft prüfen und ggf. nachbearbeiten. Beim Einsatz eines LLM im Behörden- oder Unternehmensumfeld sollte eine Risikoanalyse für den konkreten Anwendungsfall durchgeführt werden, um anwendungsbezogene Risiken zu detektieren, zu bewerten, geeignete Maßnahmen zu ergreifen und über die Voraussetzungen eines späteren Einsatzes fundiert entscheiden zu können.

ENTWICKLUNGSDYNAMIK MIT POTENZIAL

In den vergangenen Jahren haben sich LLMs rasant weiterentwickelt und können immer komplexere Aufgaben in einer hohen Qualität lösen. Dadurch steigert sich das Potenzial der Modelle – ebenso wie die Risiken der Nutzung. Es ist davon auszugehen, dass die Entwicklung weiterhin zügig voranschreitet und LLMs immer häufiger in Systeme verschiedener Anwendungsbereiche integriert werden. Diese technologische Dynamik erfordert daher auch in Zukunft eine ebenso dynamische Bewertung der IT-Sicherheit beim Einsatz großer KI-Sprachmodelle. ■

Publikation „Große KI Sprachmodelle – Chancen und Risiken für Industrie und Behörden“:

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

Schwachstellenmeldung zu Indirect Prompt Injections:

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2023/2023-249034-1032.pdf?__blob=publicationFile&v=3

Crashtests für KI in Fahrzeugen

Ohne KI kein automatisiertes Fahren – neue Herausforderungen verlangen neue Lösungsansätze

von Rainer Plaga und Britta Sennewald, Referat Bewertungsverfahren für eID-Technologien in der Digitalisierung, und Dr. Arndt von Twickel, Referat Cyber-Sicherheit für intelligente Transportsysteme und Industrie 4.0

Die Schlüsseltechnologie Künstliche Intelligenz (KI) ermöglicht eine Vielzahl von Digitalisierungsanwendungen, wie etwa automatisiertes Fahren. Sie bringt jedoch auch neue Herausforderungen, wie etwa eine neue Qualität und Quantität von IT-Sicherheitsrisiken. Dieser Beitrag befasst sich anhand der Domäne Automotive mit dem aktuellen Stand der Entwicklung von Anforderungen, Prüfmethoden und Prüfwerkzeugen für KI-basierte Systeme. In Kombination mit technischen Richtlinien des BSI und nationalen sowie internationalen Standardisierungs- und Regulierungsaktivitäten sollen sie perspektivisch zu einer sicheren und vertrauensvollen Anwendung von KI führen.

Die Digitalisierung von Fahrzeugen macht große Fortschritte. Die Automatisierung steigert nicht nur den Komfort, etwa dank der Sprachsteuerung, sie ist auch relevant für die Sicherheit, wie das Beispiel der Spurhalteassistenten zeigt. Viele dieser Funktionen sind hochkomplex, da sie von sehr variablen Sensorinformationen abhängen, wie sie z. B. auf einer belebten Straßenkreuzung zu unterschiedlichen Tages- und Jahreszeiten auftreten. Aufgrund dieser Komplexität scheitert meist die direkte Programmierung. Als Alternative werden Systeme der KI eingesetzt, die anhand von großen Datenmengen trainiert werden. Diese Systeme sind „Black-Box"-Systeme, deren Güte u. a von der Qualität der Trainingsdaten abhängt. Zudem sind sie nicht mehr direkt interpretierbar und können nicht formal verifiziert werden. Daher können sie auch nur experimentell getestet werden. Nicht zuletzt zeigen sich KI-Systeme verwundbar, u. a. durch adversariale und Backdooring-Angriffe.

Damit KI-Systeme trotz ihrer Vulnerabilität akzeptiert und eingesetzt werden, ist Vertrauen notwendig. Weltweit gibt es hierzu Regulierungsbemühungen, u. a. den AI Act der EU. Die praktische Umsetzung dieses Regelwerks für KI wird aktuell noch erforscht. Insbesondere müssen geeignete und allgemein anerkannte Anforderungen, Prüfmethoden und Prüfwerkzeuge entwickelt und praxistauglich implementiert werden. So soll die Vertrauenswürdigkeit der Systeme nachgewiesen werden.

Je nach Anwendung werden unterschiedliche Aspekte geprüft: Geht es um Mobilität, hat die funktionale Sicherheit höchste Priorität, also der Schutz von Gesundheit und Umwelt. Die Cybersicherheit von KI-Systemen in Fahrzeugen ist hierbei eine wesentliche Grundlage für die Verkehrssicherheit.

MODULARE UND NUTZERORIENTIERTE LÖSUNGSANSÄTZE

Aufgrund der Komplexität der Aufgabe ist ein generalistischer Lösungsansatz initial nicht zielführend. Es geht nicht um die Entwicklung von geeigneten Methoden, Kriterien und Werkzeugen für eine Prüfung aller KI-Systeme. Stattdessen verfolgt das BSI einen modularen Use-Case-zentrierten Ansatz. Über die Bearbeitung unterschiedlicher Use-Cases werden in den verschiedenen Digitalisierungsdomänen iterativ ein modularer „Prüfwerkzeugkasten" sowie Best-Practice-Empfehlungen aufgebaut. Ziel ist, dass sich mit fortschreitender Verfeinerung

der Aufwand der Anpassung an neue Use-Cases reduziert. Für die Bearbeitung der einzelnen Use-Cases wird neben KI- und Cybersicherheitsexpertinnen und -experten auch Expertise aus der jeweiligen Digitalisierungsdomäne benötigt, etwa aus der Fahrzeugsicherheit und -IT in der Mobilitätsdomäne.

Mit dem Projekt AIMobilityAudit verfolgt das BSI daher das Ziel, einen modularen Prüfwerkzeugkasten für die Mobilitätsdomäne anhand von zwei Use-Cases zu den Themen Verkehrsschildklassifikation und Fußgängererkennung zu entwickeln. Die 50 im Vorprojekt AIMobilityAuditPrep erarbeiteten Prüfanforderungen sollen dabei evaluiert und verfeinert werden. Hierzu bringt das Projekt KI-, Cybersecurity- und Automotive-Fachwissen vom BSI, der Technologiefirma ZF und TÜVIT zusammen. Aufgrund der Komplexität der Anwendungen und der Notwendigkeit von empirischen Tests wird eine Kombination von Tests in Simulationen, in Hardware-in-the-Loop-Systemen und auf realen Teststrecken durchgeführt. Um diese Tests möglichst praxisnah und offen kommunizierbar zu gestalten, werden parallel Open-Source-Systeme und proprietäre Industrielösungen erprobt. Sie laufen aktuell im Labor und vor Ort in Koblenz und Friedrichshafen. Unter anderem werden speziell präparierte Verkehrsschilder und Kleidungsstücke daraufhin getestet, ob – und falls ja, in welchen Situationen – sie die Klassifikations- und Detektionssysteme zu Fehlentscheidungen verleiten können.

BSI SCHAFFT SOLIDE GRUNDLAGE FÜR DIE UMSETZUNG DES AI ACTS

Im weiteren Verlauf des Projekts sollen neben der Verwundbarkeit der aktuellen Systeme auch konkrete Mitigationsstrategien untersucht werden. Aufbauend auf den Ergebnissen ist im Laufe des Jahres 2024 die Erstellung einer modularen technischen Richtlinie zur Prüfung von KI-Systemen im Automotivebereich vorgesehen. Diese soll dann einerseits als Vorlage für weitere Digitalisierungsdomänen dienen (beispielsweise in BSI-Projekten zu den Domänen Medizin, Landwirtschaft und Finanzen) und andererseits als Grundlage für die nationale und internationale Gremienarbeit im KI- und Fahrzeugbereich genutzt werden. Das BSI trägt somit zu einer soliden Grundlage für die Operationalisierung des europäischen AI Acts bei. ■

AI-Security als Voraussetzung für Vertrauen in automatisiertes Fahren: Ein Fachgespräch

Welche Rolle spielt Cybersicherheit von KI-Systemen in Fahrzeugen für den Erfolg von automatisiertem Fahren? Mit dieser Frage befasst sich Dr. Arndt von Twickel, BSI-Referatsleiter Cybersicherheit für intelligente Transportsysteme und Industrie 4.0, im Gespräch mit Dr. Georg Schneider, Leiter ZF AI-Lab Saarbrücken, und Vasilios Danos, Berater für Cybersicherheit bei TÜV Informationstechnik, über das gemeinsame KI-Projekt AIMobilityAudit.

Dr. Arndt von Twickel: Herr Schneider, Sie leiten ein Labor für Künstliche Intelligenz (KI) beim Technologiekonzern ZF, der Systeme für die Mobilität von Pkw, Nutzfahrzeugen und Industrietechnik liefert. Was sind wichtige KI-Entwicklungsprojekte in Ihrem Zuständigkeitsbereich, und welche Art KI-Technologie setzen Sie ein?

Georg Schneider: Wir beschäftigen uns mit der Erforschung und Anwendung von KI in den Bereichen automatisiertes Fahren und Fahrerassistenz (AD/ADAS) sowie bei Prozess- und Produktionsanwendungen. Ein dritter Bereich ist das Thema der vertrauenswürdigen KI (Trusted AI), zu dem auch das Projekt AIMobilityAudit (s. Artikel auf S. 20) gehört, an dem wir gemeinsam mit dem BSI und TÜV Informationstechnik (TÜVIT) arbeiten.

Hinsichtlich der eingesetzten KI-Technologien sind wir sehr breit aufgestellt: Wir nutzen sowohl klassische Verfahren wie Entscheidungsbäume als auch die neuesten Technologien des Deep Learnings.

Twickel: Setzen Sie die KI-Technologie ein, weil sie kostengünstiger ist oder weil sie besser funktioniert als klassische Software?

Schneider: Aufgrund der Komplexität vieler Aufgaben wie z. B. beim automatisierten Fahren ist der Einsatz von KI vielerorts alternativlos. Bei der Verarbeitung komplexer Sensorinformationen kommen klassische Algorithmen sehr schnell an ihre Grenzen.

Twickel: Herr Danos, welche Berührungspunkte haben Sie bei der TÜVIT, die auf den technischen Check von Hard- und Software spezialisiert ist, mit dem Thema KI? Wo sehen Sie die Rolle von KI bei der Mobilität?

Vasilios Danos: Wir nutzen KI einerseits als Werkzeug zur Erkennung komplexer Datenmuster bei Sicherheitsanalysen von z. B. Smartcards. Andererseits erarbeiten wir für KI-Systeme Prüf- und Zertifizierungsverfahren. Unsere Kunden kommen aus unterschiedlichen Anwendungsdomänen wie Biometrie und Mobilität. Im Mobilitätsbereich sehen wir enormes Potenzial von KI: von der Sensorik und Fahrassistenzsystemen bis hin zu autonomen Fahrfunktionen.

Twickel: Aus Sicht des BSI ist Cybersicherheit Voraussetzung für Vertrauen in die Digitalisierung und damit für ihren Erfolg. Welche Rolle spielt die Cybersicherheit von KI in Ihrer Arbeit, Herr Danos?

Danos: Cybersicherheit ist aus unserer Sicht untrennbar mit KI verbunden und stellt eine Grundvoraussetzung für einen sicheren und vertrauensvollen Betrieb dar. Neben zahlreichen Vorteilen enthalten KI-Systeme auch eine Reihe von Schwachstellen, die von Angreifern ausgenutzt werden könnten. Als Prüfdienstleister sehen wir uns daher in der Verantwortung, die Sicherheit der Anwendung zu überprüfen.

Twickel: Herr Schneider, welche Rolle spielt Cybersicherheit im Kontext KI beim ZF AI-Lab Saarbrücken?

Schneider: Im ZF-Konzern gibt es unterschiedliche Abteilungen, die sich ausschließlich mit der Cybersicherheit von ZF und allen ZF-Produkten beschäftigen. Wir wollen neben der „klassischen“ Cybersecurity auch dann Sicherheit gewährleisten, wenn neuartige KI-Angriffsvektoren eingesetzt werden. Dafür ist eine tiefe Einsicht in die neueste KI-Technologie im Kontext der Anwendung notwendig – dies wird aktuell im gemeinsamen Projekt AIMobilityAudit untersucht.

Vasilios Danos, Berater für Cybersicherheit, TÜV Informationstechnik

Dr. Arndt von Twickel, Referatsleiter Cybersicherheit für intelligente Transportsysteme beim BSI

Dr. Georg Schneider, Leiter ZF AI-Lab Saarbrücken

Twickel: Welche neuen Aspekte sehen Sie beide hier im Vergleich zu klassischer IT? Ist aus Ihrer Sicht ein neuer Begriff wie AI-Security zielführend?

Schneider: Ich halte diesen neuen Begriff sogar für notwendig, denn das Thema wird bisher weder in einer verabschiedeten Norm für Cybersicherheit noch in einer anderen Norm ausreichend behandelt. Die neuen Eigenschaften von KI sind zu berücksichtigen: Das sind z. B. der „Blackbox-Charakter" vieler KI-Modelle und die riesigen Eingabe- und Parameterräume, die sogenannte adversariale Angriffe oder Hintertürangriffe möglich machen.

Danos: Dem stimme ich zu. Ein eigener Begriff könnte die Besonderheit von Cybersecurity in Verbindung mit KI hervorheben und somit viele Eigenarten der heutigen KI-basierten Anwendungen bündeln. Im Gegensatz zu klassischer Cybersecurity lassen sich KI-spezifische Schwachstellen nicht nur auf eine fehlerhafte Implementierung oder fehlerhaften Betrieb zurückführen, sondern basieren auch auf darunterliegenden maschinellen Lernverfahren, die eine Schwachstellenanalyse und Ursachenforschung im Problemfall erschweren.

Twickel: Wie sollte Ihrer Meinung nach die AI-Security in der Mobilität geprüft werden?

Schneider: Im Projekt verfolgen wir einen Use-Case-zentrierten Ansatz, d. h., wir schauen uns konkrete Anwendungsbeispiele an und entwickeln und evaluieren Prüfanforderungen, -prozesse und -werkzeuge. Ziel ist es hierbei, die Anforderungen so generisch wie nötig und so konkret wie möglich zu formulieren. Gleichzeitig ist uns wichtig, dass alle Methoden und Tests praxistauglich gestaltet sind.

Danos: Jede Anwendung bringt ihre eigenen Sicherheitsanforderungen mit sich. Prüfungen müssen daher risikobasiert und auf den jeweiligen Anwendungsfall zugeschnitten erfolgen. Mit der wachsenden Erfahrung aus der Entwicklung von Prüfprozessen für verschiedene Anwendungen können dann gemeinsame Prüfbausteine und -strategien identifiziert, generalisiert und ggf. automatisiert werden, sodass der Entwicklungs- und Prüfaufwand für neue Anwendungen minimiert wird. Zudem können wir auf etablierten Prüfprozessen, im Mobilitätsbereich insbesondere auf Safety- und Securitystandards, aufbauen und diese durch eine sogenannte Gap-Analyse hinsichtlich AI-Security sinnvoll ergänzen.

Twickel: Final ausgereifte Prüfprozesse lassen wohl noch einige Zeit auf sich warten. Inwieweit berücksichtigen Sie bereits heute AI-Security bei Ihrer Arbeit?

Schneider: Durch einen permanenten Austausch mit unseren Fachabteilungen und unseren Cybersecurity-Abteilungen stellen wir sicher, dass ZF die neuesten Erkenntnisse zur AI-Security direkt bei der Entwicklung mit einfließen lässt.

Danos: Die Sicherheit von KI-basierten Anwendungen ist schon heute ein wesentlicher Aspekt bei modernen Fahrzeugen. Neue Fahrzeuge und deren (KI-)Komponenten müssen homologiert werden und entsprechende (Prüf-)Anforderungen gemäß gültiger Standards (beispielsweise ISO 26262) einhalten.

Twickel: Welche Herausforderungen sehen Sie hier aktuell und zukünftig?

Danos: Eine große Aufgabe ist die Einbettung von KI-spezifischen Prüfungen in bestehende Prozesse – hierfür werden zeitnah neue Standards benötigt. Diese erfordern eine gemeinsame interdisziplinäre Anstrengung von Industrie, Forschung und Behörden. Herausfordernd bleibt auch die Festlegung von Prüfparametern und die Interpretation der Ergebnisse. Wir müssen entscheiden, welches Maß an Toleranz oder welches Restrisiko wir bereit sind zu akzeptieren.

Schneider: Ich schließe mich an und bin optimistisch, dass uns gemeinsam diese Aufgabe gelingt: AI-Security wird eine wichtige Rolle auf dem Weg zum automatisierten Fahren spielen.

Twickel: Herzlichen Dank für diesen spannenden Austausch!

Neue Risiken durch KI im Auto

BSI goes Museum: Das BSI hat am neuen Erlebnisraum zu Robotik und Mobilität im Deutschen Museum Bonn mitgewirkt

von Matthias Neu und Britta Sennewald, Referat Bewertungsverfahren für eID-Technologien in der Digitalisierung, und Dr. Arndt von Twickel, Referat Cyber-Sicherheit für intelligente Transportsysteme und Industrie 4.0

Mit Künstlicher Intelligenz (KI) beschäftigten sich das BSI und das Deutsche Museum Bonn schon länger. Im Mai 2023 hat das Deutsche Museum einen neuen Erlebnisraum zum Thema „KI in Robotik und Mobilität" eröffnet. Eines der Exponate ist in Kooperation mit dem BSI im Rahmen einer studentischen Abschlussarbeit entstanden. Das Ausstellungsstück demonstriert interaktiv, wie angreifbar ein KI-basiertes Fahrassistenzsystem ist, das Verkehrsschilder automatisch klassifizieren soll.

Fahrassistenzsysteme werden seit einigen Jahren vermehrt in PKWs genutzt, um die Sicherheit auf den Straßen zu erhöhen. Seit Anfang 2020 ist der Einbau bestimmter Fahrassistenzsysteme in Neuwagen sogar durch eine EU-Verordnung vorgeschrieben. Dazu zählen auch intelligente Geschwindigkeitsassistenten. Damit sie reibungslos funktionieren, müssen solche Assistenten die aktuell auf der Strecke zugelassene Höchstgeschwindigkeit erfassen. Dies geschieht zumeist über visuelle Sensoren, deren erfasste Daten von KI-Systemen verarbeitet werden, um Verkehrsschilder zu erkennen. Damit dieser Prozess reibungslos funktioniert, müssen die beteiligten KI-Systeme absolut zuverlässig und genau arbeiten. Die KI-Systeme müssen Verkehrsschilder bei jeder Witterung und in verschiedensten Situationen korrekt bestimmen können und robust gegenüber Angriffen sein.

ANGRIFFE AUF NEURONALE NETZE

Auch bei KI-Verfahren spielen die klassischen Schutzziele der IT-Sicherheit – Integrität, Vertraulichkeit und Verfügbarkeit – eine wichtige Rolle. KI-Verfahren können auf verschiedenste Arten angegriffen werden. Typische Angriffe auf neuronale Netze sind:

Adversariale Angriffe: Ein Angreifer manipuliert die Eingabedaten, um das Klassifikationsergebnis eines KI-Systems während des Betriebs zu verändern. Dabei ist die Manipulation für Menschen kaum als solche erkennbar.

Poisoning-Angriffe: Diese Angriffskategorie wird in der Trainingsphase eines KI-Systems durchgeführt. Der Angreifer manipuliert dabei die Trainingsdaten mit dem Ziel, den Lernprozess des Systems zu beeinflussen.

Privacy-Angriffe: Im Gegensatz zu den vorherigen Angriffsarten liegt bei den Privacy-Angriffen der Fokus nicht auf der Manipulation des Ergebnisses. Das Ziel ist es, Informationen über das Modell, über die Beschaffenheit der Trainingsdaten oder über die Existenz von bestimmten Daten im Trainingsset zu erhalten.

INTENSIVE ZUSAMMENARBEIT MIT STUDIERENDEN

Das BSI untersucht in praktischen Untersuchungen die Auswirkung von adversarialen Angriffen auf verschiedene Verkehrsschilderkennungssysteme. Dabei arbeitet das BSI intensiv mit Studierenden zusammen und betreut Abschlussarbeiten und Praktika. Im Fokus der Bachelorarbeit

Bild oben: *Bachelorstudent Steffen Jendrny (rechts) und sein Betreuer, Referatsleiter Dr. Arndt von Twickel (DI 23), bei der Eröffnung der KI-Ausstellung im Deutschen Museum Bonn.* ***Bild unten:*** *Die Visualisierung der Ergebnisse des KI-Systems bei der Erkennung eines Stoppschildes.*

von Steffen Jendrny von der Fernuniversität Hagen stand der Einsatz von Hardware-in-the-loop(HIL)-Systemen zur Evaluation der IT-Sicherheit von visuellen Fahrassistenzsystemen. Mit HIL-Systemen können viele verschiedene Fälle aus realen Fahrsituationen nachgestellt und evaluiert werden, indem Fahrzeugkomponenten in eine Simulation integriert werden. Ziel der Arbeit war es, daraus reale Angriffsvektoren zu extrahieren, um über diese Rückschlüsse auf die Angreifbarkeit der Systeme zu ziehen. Dies stellt eine wichtige Grundlage für die Erstellung einer Methodik zur Evaluation von Fahrerassistenzsystemen dar.

EIN SICHERHEITSRISIKO ALS INTERAKTIVES EXPONAT

Das Exponat im Deutschen Museum wurde im Kontext der Abschlussarbeit entwickelt und demonstriert interaktiv, wie ein KI-System zur Verkehrsschilderkennung angegriffen werden kann. Die Besucherinnen und Besucher können in die Rolle eines Angreifers schlüpfen, indem sie ein Verkehrsschild mit Aufklebern partiell verdecken. Aufkleber auf Verkehrsschildern sind insbesondere in bewohnten Gebieten häufig zu finden. Im Museum zeigt ein Monitor, welche Auswirkungen das Bekleben des Schildes auf das Klassifizierungsergebnis des KI-Systems hat. So lässt sich ein Stoppschild z. B mit einem „Eating-Animals"-Aufkleber in Sekundenschnelle in ein Vorfahrtsschild umwandeln.

Die Besuchenden im Museum erfahren somit, wie KI-Systeme bereits durch leichte Veränderungen zu einer Fehlfunktion verleitet werden können – was für den realen Straßenverkehr ein großes Sicherheitsrisiko darstellt. „Die Besucherinnen und Besucher nehmen das Exponat sehr gut an", sagt Ralph Burmester, Kurator des Deutschen Museums. Fahrassistenzsysteme sind inzwischen sehr verbreitet, und viele Besucherinnen und Besucher interessiere es, ob Fahrzeuge Verkehrsschilder richtig erkennen und ggf. korrekt reagieren – denn das habe hohen Einfluss auf die Sicherheit der Menschen im Fahrzeug.

Die Ausstellung im Deutschen Museum Bonn ist von Dienstag bis Freitag sowie sonntags von 10:00 bis 17:00 Uhr und samstags von 12:00 bis 17:00 Uhr geöffnet. ■

Quantum-Machine-Learning bringt neue Sicherheitsaspekte mit sich

Das BSI untersucht Bedrohungsszenarien für maschinelles Lernen auf Quantencomputern

von Fabian Petsch, Referat Grundsatz, Strategie und Nachweise in der Künstlichen Intelligenz

Der Begriff des Quantum-Machine-Learnings (QML) bezeichnet ein dynamisches Forschungsfeld, das Methoden des maschinellen Lernens mit den Potenzialen der Quanteninformationsverarbeitung kombiniert. Von praktischem Interesse ist dabei vor allem, inwiefern bestimmte Subroutinen oder auch die Modellbildung selbst nutzbringend auf einen Quantencomputer ausgelagert werden können. Als Kompetenzzentrum für Künstliche Intelligenz (KI) im Zusammenhang mit IT-Sicherheit begleitet das BSI die Entwicklungen des QML, um auf eine sichere Ausgestaltung der neuen Technologie hinzuwirken.

Als vielversprechende Methoden des QML treten derzeit vor allem die sogenannten variationellen Quantenschaltkreise, kurz VQCs (Variational Quantum Circuits), in Erscheinung. Kennzeichnend hierbei ist ein Wechselspiel zwischen klassischer IT und dem Quantencomputer: Der entsprechende Quantenschaltkreis verfügt hierbei typischerweise über Parameter, die iterativ mithilfe eines klassischen Optimierers angepasst werden. Für VQCs existiert mittlerweile eine beträchtliche Zahl unterschiedlicher Ansätze und Architekturen, u. a. in Form sogenannter Quantum Neural Networks. VQCs sind aufgrund ihrer vergleichsweise niedrigen Anforderungen an die benötigten Quantencomputing-Ressourcen bereits prinzipiell auf der aktuell verfügbaren, d. h. noch nicht hinreichend fehlerkorrigierten und intermediären, Quanten-Hardware realisierbar.

PARALLELEN ZWISCHEN QML UND KLASSISCHEN KI-VERFAHREN

In der Analyse der Bedrohungsszenarien für QML-Systeme und -Methoden ist festzustellen, dass sich der Lebenszyklus in gewisser Abstraktion (Datensammlung und -präparation, Modellselektion und Training/Testing, laufender Betrieb) nicht grundsätzlich von demjenigen klassischer KI-Verfahren unterscheidet, auch wenn die genutzten Quantenkomponenten neue Spezifika in die Sicherheitsbetrachtung einbringen. In erster Überlegung ergibt sich damit, dass die für klassische KI-Systeme bekannten Angriffskategorien, d. h. Evasion-Attacks, Data-Poisoning, Model-Stealing und Privacy-Attacks, zumindest prinzipiell auf QML übertragbar sind. Die Vorgehensweisen und Implementierungen der jeweiligen Angriffe, z. B. zum Auffinden von Adversarial Examples oder dem Eintrainieren einer Hintertür, sind in vielen Fällen zunächst modellagnostisch. Auch wenn speziell für Evasion-Attacks und deren Mitigation mittels Adversarial Training bereits erste Arbeiten und Ergebnisse existieren, so sind die weiteren Angriffskategorien bisher nahezu unerforscht. Ob die Anwendung der genannten Angriffe auf QML mit einer abweichenden, womöglich sogar reduzierten Wirksamkeit verbunden ist, ist derzeit noch nicht umfassend bestimmt.

NEUE BEDROHUNGSSZENARIEN MÖGLICH

Neben diesen aus der Sicherheit klassischer KI-Systeme motivierten Bedrohungsszenarien gibt es für das QML auch neuartige, Quantencomputer-spezifische Angriffsflächen. So bietet der Vorgang des Transpilierens, bei dem ein theoretisch beschriebener Quantenschaltkreis für die Ausführung auf der jeweiligen Quanten-Hardware vorbereitet und an deren Gegebenheiten angepasst wird, unterschiedliche Möglichkeiten der Manipulation. Ein Angreifer kann hier beispielsweise Qubits mit besonders hohen Fehlerraten sowie fehlender Konnektivität untereinander zuweisen oder gar den Quantenschaltkreis an sich verändern. Ein zweiter Angriffsvektor ergibt sich aus dem Ansatz, zur effektiven Ausnutzung der vorhandenen Ressourcen mehrere Quantenschaltkreise parallelisiert auf einem einzelnen Quantenchip auszuführen. Unbeabsichtigte, aber physikalisch bedingte Kopplungen zwischen den Qubits (sogenannter Cross-Talk) können in diesem Zusammenhang ausgenutzt werden, um die Funktionalität des Quantenschaltkreises zu beeinflussen. Auch wenn die Durchführbarkeit derartiger Angriffe bereits gezeigt ist, muss noch bewertet werden, wie realistisch diese Bedrohungsszenarien zukünftig in der Praxis sind.

Aus wissenschaftlicher Perspektive sind viele fundamentale Zusammenhänge zur Sicherheit von QML-Methoden und -Systemen, die sich einerseits aus den generellen Gegebenheiten der Quanten-Hardware und andererseits aus den Spezifika der QML-Methoden ergeben, derzeit nicht abschließend ergründet. So ist bisher nur in Ansätzen untersucht, inwiefern die für herkömmliche KI-Systeme bekannten Angriffe und Verteidigungen durch die diversen auf dem Quantencomputer vorhandenen Noise-Arten beeinflusst werden. Daneben besteht beispielsweise noch Unklarheit darüber, wie unterschiedliche Techniken zum Überführen der Daten in Quantenzustände auf die Widerstandsfähigkeit von QML-Methoden wirken.

BSI BETREIBT GRUNDLAGENFORSCHUNG

Aus Sicht des BSI ist eine tiefergehende Beschäftigung mit den Sicherheitsaspekten des QML auch bereits zum jetzigen Zeitpunkt nachdrücklich angezeigt. Mit Blick auf die rasanten Fortschritte und hohen Investitionen im Bereich des Quantencomputings insgesamt ist ein Einzug von Quantencomputern im Anwendungskontext des maschinellen Lernens vorausschauend zu diskutieren. Das BSI engagiert sich deshalb in Form eigener Projektaktivitäten maßgeblich in der Grundlagenforschung bezüglich der hier skizzierten Angriffspfade, Mitigationsmaßnahmen und weiteren Sicherheitseigenschaften von QML-Methoden und -Systemen. ■

Wie KI die Medienaufsicht vereinfacht – Best Practice für Behörden

Neben den Projekten, die das BSI im Bereich KI selbst durchführt oder begleitet, blicken die Kolleginnen und Kollegen auch regelmäßig über den fachlichen Tellerrand und sind dabei auf ein weiteres spannendes Projekt aufmerksam geworden. Das KI-Tool KIVI erleichtert den Landesmedienanstalten die Arbeit: Gewaltdarstellung, Volksverhetzung und andere Verstöße können damit leichter aufgespürt werden. Ein Interview mit Ruth Meyer, Direktorin der Landesmedienanstalt Saarland, und Ina Goedert, Abteilungsleiterin Medienaufsicht und Medienforschung der Landesmedienanstalt Saarland, über Vorteile von KI in der Arbeit der Medienaufsicht. Die Erkenntnisse aus der Arbeit mit dem Tool können in zukünftige KI-Projekte bei Behörden einfließen.

Ruth Meyer, Direktorin der Landesmedienanstalt Saarland

Ina Goedert, Abteilungsleiterin Medienaufsicht und Medienforschung der Landesmedienanstalt Saarland

Welche grundlegenden Funktionen stellt das Tool KIVI bereit?

Ruth Meyer: KIVI beschleunigt, vereinfacht und verbessert die Arbeit der Medienaufsicht, indem es das Netz durchsucht und Mitarbeitende der Medienanstalten auf mögliche Rechtsverstöße hinweist. Dabei ist die Funktionsweise Grundlage der Namensgebung. So ist der Name KIVI die Verschmelzung der Begriffe KI und vigilare (lat. für wachsam sein). Der Fokus liegt bislang auf dem Schutz der Menschenwürde und dem Jugendschutz. Zu den konkreten Verstoßkategorien zählen beispielsweise Gewaltdarstellungen, Volksverhetzung, die Verwendung verfassungsfeindlicher Kennzeichen oder frei zugängliche Pornografie. Aber auch Erweiterungen im Bereich der Aufsichtsfelder, die im Zuständigkeitsbereich der Medienanstalten liegen, sind vorstellbar und bereits angedacht.

Was gab den Anstoß zur bundesweiten Etablierung des Tools?

Ina Goedert: Ausgangspunkt waren die Fragen, ob man zeitgemäß und effektiv auf Rechtsverstöße in einem digitalen Umfeld reagieren kann, das täglich wächst, und ob wir eine Lösung finden können, die im föderalen System der Medienanstalten über Ländergrenzen hinweg Rechtsdurchsetzung im Netz ermöglicht. Die Antwort auf unsere Fragen lautet: Ja, wir finden Lösungen mithilfe modernster Technologie, digitaler Hilfsmittel und vor allem Künstlicher Intelligenz. Eine effektive und moderne Medienaufsicht im Internet ist nur möglich, wenn wir die Möglichkeiten der Digitalisierung bei der Wahrnehmung unserer Pflichten berücksichtigen und zu unserem Nutzen einsetzen.

Unsere Schwesternanstalt – die Landesanstalt für Medien NRW (LFM NRW) – hat hierzu 2019 eine Machbarkeitsanalyse durchgeführt und sich anschließend entschlossen, ein Werkzeug basierend auf Künstlicher Intelligenz zu entwickeln. Umgesetzt hat die Entwicklung als technischer Dienstleister die Condat AG aus Berlin. 2020 hat die LFM NRW dann begonnen, das Tool zu entwickeln und zu testen, sodass ab April 2022 die anderen Medienanstalten „ongeboardet" werden konnten.

Welche Besonderheiten gibt es beim Training und der Arbeit mit KI?

Meyer: Die KI lernt durch Bild- und Textbeispiele, die wir aktiv einspeisen. Es handelt sich um Beispiele, die als Verstoß bewertet wurden. Wir geben täglich Rückmeldung, ob sich ein Verdacht bestätigt hat oder nicht. Daher gilt: Je länger wir mit dem Tool arbeiten, desto effizienter kann die KI lernen und umso qualitativ bessere Ergebnisse liefert sie.

Dennoch ist wichtig zu betonen: Das KI-Tool ist ein Hilfsmittel. Jeder Verdacht, den das Tool ausweist, wird zunächst geprüft. Die zuständigen Häuser entscheiden mindestens im Vieraugenprinzip, ob ein formelles Verfahren eingeleitet wird. Die KI entscheidet nicht selbst! Sollte die KI einen Verdacht ausweisen, der sich nicht bestätigt, wird auch diese Information an das Tool zurückgegeben.

Wie wird der Effekt des Tools von den Mitarbeitenden wahrgenommen? Und welche Auswirkungen sind hier generell zu erwarten?

Goedert: Von X (vormals Twitter) und YouTube bis zu Plattformen wie Telegram und VK kann das Tool täglich mehr als 10.000 Seiten automatisch durchsuchen. Ohne diese technische Hilfe konnten wir nur einen Bruchteil davon schaffen. Die deutliche Steigerung unserer Präsenz im Netz ist ein erster großer Erfolg des Tools. Dadurch finden wir mehr Rechtsverstöße, ohne unsere Ressourcen für die Suche zu verwenden. Zudem erhalten wir einen Überblick über die Gefahrenlage im Internet und können den Rechtsverstößen priorisiert nachgehen. Außerdem können wir so – häuserübergreifend und gemeinsam – den großen Berg an Verstößen bearbeiten, bei denen uns die Herkunft eines Hasspostings oder Gewaltvideos nicht bekannt ist. Ohne doppelte Arbeit, aber mit 14-facher Stärke.

Das Ergebnis sind nicht nur eine flächendeckend bessere Erkennbarkeit von potenziellen Verstößen und die Erzielung von mehr Ergebnissen, sondern auch ein deutlich erhöhter Schutz für die Mitarbeiterinnen und Mitarbeiter: Bevor sie einen Inhalt öffnen, wissen sie schon, zu welcher Kategorie er wahrscheinlich gehört. Sie sind also bereits vorgewarnt und stoßen nicht ganz unvermittelt auf Darstellungen von Gewalt, wie etwa ein Enthauptungsvideo oder ein Missbrauchsfoto. Sie können außerdem festlegen, welche möglicherweise verstörenden Inhalte zunächst unscharf dargestellt werden sollen – was gerade bei Gewaltdarstellungen die psychische Belastung mindern kann. Oder sie entscheiden sich, gewisse Kategorien an diesem Arbeitstag nicht mehr zu sichten. Das Tool ermöglicht es, selbstbestimmter in der Monitoringarbeit zu sein.

Wie können sich Interessierte über das Thema informieren oder sogar helfen?

Goedert: Wir gehen sehr transparent mit dem Einsatz von KI um und sind dankbar für jeden Hinweis zur Verbesserung unserer Methoden und KI-Systeme. Unter anderem setzen wir auf eine stichwort- und linkbasierte Suche nach Inhalten im freien Internet und auf sozialen Plattformen wie Scraping oder Link-Extraction. Die Analyse von Bildern und Texten mit KI-Methoden erfolgt mittels neuronaler Netzwerke und vortrainierter Modelle und Services (Convolutional Neural Network, TransferLearning, Amazon Recognition Unsafe Content) und klassischen statistischen Machine-Learning-Methoden (Naive-Bayes-Verfahren). Hinweise zur Verbesserung und zu möglichen Datenlücken sind daher bei allen Medienanstalten willkommen. ■

Gemeinsam die Cybernation Deutschland bauen

Nur mit harter Arbeit können wir die Cyberresilienz substanziell erhöhen

Ein Interview mit Claudia Plattner, BSI-Präsidentin

Liebe Claudia, wie hast Du Dich eingelebt in Deine neue Rolle als oberste Cybersicherheitschefin in Deutschland? Wie war Dein Eindruck?
Schöne Jobbezeichnung, aber als so jemand sehe ich mich nicht. Mir ging es in der ersten Zeit vor allem darum, einen umfassenden Überblick zu bekommen. Und dabei haben mir die ganzen Cybersicherheitsexpertinnen und -experten – all meine Kolleginnen und Kollegen im BSI – ganz wunderbar geholfen. Denn sie sind der Garant dafür, dass bei uns „der Laden läuft".
Ich habe nach vielen Kennenlernterminen und intensivem Austausch eine steile Lernkurve hinter mir, bin aber auch noch lange nicht fertig mit Lernen. Ich habe mich sehr herzlich aufgenommen gefühlt und fand die Einblicke spannend und die Diskussionen gewinnbringend. Das finde ich immer noch.

Mein Eindruck nach den ersten knapp 100 Tagen: Wir befinden uns in einem enormen Spannungsfeld. Verschiedenste Faktoren wirken in einer Gemengelage auf uns ein, die von geopolitischen Spannungen über einer zunehmenden Bedrohungslage im Cyberraum bis hin zu einer allgemein angespannten Stimmung in der Gesellschaft reicht, bei der Leute befürchten, Deutschland verliere bei der Digitalisierung den Anschluss. In dieser Situation das Steuer zu übernehmen, ist eine große Aufgabe, der ich mich gerne stelle. Denn wenn wir uns gut aufstellen, uns gut vorbereiten und vor allem gut zusammenarbeiten, können wir das schaffen.

Stichwort Bedrohungslage: Wie schätzt Du die Lage der IT-Sicherheit in Deutschland ein?
Der Bericht zur Lage der IT-Sicherheit in Deutschland, den wir Anfang November 2023 in der Bundespressekonferenz vorgestellt haben, zeichnet ein besorgniserregendes Bild. Wir haben ein echtes Problem: Eine Viertelmillion neue Schadsoftwarevarianten und 21.000 infizierte System tagtäglich, dazu mehr als 2.000 Schwachstellen in Softwareprodukten pro Monat. Der Schaden durch Angriffe auf deutsche Unternehmen beläuft sich auf über 200 Milliarden Euro laut Digitalverband bitkom. Das sind 43 Prozent des gesamten Bundeshaushalts, um die Zahl in eine Verhältnis zu setzen.

Der Bericht zur Lage der IT-Sicherheit in Deutschland zeichnet ein besorgniserregendes Bild.

Was sind für Dich die schwerwiegendsten Gründe für diese Situation?
Es gibt viele Bedrohungsszenarien. Fünf Punkte, die ineinandergreifen, möchte ich gerne herausstellen:

Cyberangriffe mit Ransomware sind immer noch das dringlichste Problem. Neben den damit verbundenen hohen Kosten und den nachhaltig gestörten Wertschöpfungsketten sehe ich das schwindende Vertrauen in Staat, Verwaltung und schlussendlich in die Digitalisierung als kritisch. Durchschnittlich zwei Kommunen und kommunale Unternehmen sind pro Monat betroffen.

Oft werden die Daten aber nicht nur verschlüsselt, sondern gestohlen und es wird mit Veröffentlichung gedroht, was wir Double Extortion nennen. Dieser Datendiebstahl birgt ein weiteres Problem: Spionage. Geschäftsgeheimnisse oder vertrauliche Informationen preiszugeben, kann zu wettbewerblichen Nachteilen führen. Und handelt es sich nicht nur um wirtschaftliche Details, so sprechen wir von politischer Motivation, was uns unter Betrachtung der geopolitischen Lage und der hybriden Bedrohungen zur Sabotage führt.


BSI

Im schlimmsten Fall legen Angreifer kritische Infrastrukturen lahm. Was wir bereits jetzt tagtäglich sehen – und deren Intensität und Gefährlichkeit nimmt zu –, sind DDoS-Attacken, die auch staatliche Organisationen in ihren Aktivitäten stören.

Auch, wenn diese Angriffe vornehmlich zu Propagandazwecken eingesetzt werden, leitet dieser Punkt zum nächsten Szenario über: Politische Einflussnahme durch Desinformation. Deepfakes auf Social-Media-Plattformen werden eingesetzt, um Meinungen zu beeinflussen, Wahlen zu manipulieren oder gar Gesellschaften zu destabilisieren.

Besonders beunruhigend bei allen diesen Bedrohungsszenarien sind die steigende Professionalität, mit der hier vorgegangen wird, der Einsatz von modernster Technologie wie KI und die Arbeitsteilung vor allem bei Ransomware-Attacken. „Cybercrime-as-a-Service“ nimmt immer weiter zu.

Wie können wir dieser Situation Herr (oder Frau) werden?
Bereits einfache Maßnahmen können die Informationssicherheit signifikant erhöhen: regelmäßig Updates einspielen, sichere Passwörter, Passwortmanager und Zwei-Faktor-Authentisierung nutzen, Makros deaktivieren, regelmäßige Datensicherungen (Back-ups) so anlegen, dass eine Schadsoftware sie nicht mitverschlüsselt und sich regelmäßig auf den Ernstfall vorbereiten. Das raten wir vor allem kleinen und mittleren Unternehmen immer wieder. Städten und Kommunen bieten wir mit unserem Projekt „Weg in die Basis-Absicherung (WiBA)“ außerdem einen niedrigschwelligen Einstieg in den IT-Grundschutz des BSI an. Anhand von Checklisten mit einfachen Prüffragen und zugehörigen Hilfsmitteln können Kommunen die dringlichsten Maßnahmen selbst identifizieren und umsetzen. So kann ein erster, aber wesentlicher Schritt in Richtung systematischer Informationssicherheit erfolgen.

Das IT-Sicherheitskennzeichen ist ein weiteres Beispiel: Es schafft Transparenz für Verbraucherinnen und Verbraucher in Bereichen wie Smart Home-Multimedia. Produkte mit unserem Kennzeichnen erfüllen grundlegende Sicherheitsstandards, das gibt Orientierung für informierte Kaufentscheidungen und fördert den Schutz vor Cyberkriminalität. Wir geben damit Anreize in den Verbrauchermarkt, dass Informationssicherheit ein wichtiges Argument für die Kauf- und Nutzungsentscheidung bei IT-Produkten ist.

Aber reicht das Deiner Meinung nach aus?
Nein, das reicht bei Weitem nicht. Das Thema Cybersicherheit gehört groß gedacht. Deutschland muss sich als Cybernation verstehen. Wir – also wir alle als Gemeinschaft – müssen diesem Selbstverständnis Ausdruck verleihen und Taten folgen lassen. Als die Cybersicherheitsbehörde des Bundes verfolgen wir die Vision, gemeinsam diese Cybernation Deutschland zu bauen. Dafür sind unter anderem folgende sechs Punkte wichtig:

Wir müssen Cybersicherheit auf die Agenda heben. Erst, wenn das Thema von Entscheiderinnen und Entscheidern auf höchster Ebene als wichtig anerkannt wird, kann sich grundlegend etwas verbessern.

Wir müssen die Cyberresilienz substanziell erhöhen. Dabei kommt jede Menge harte Arbeit auf uns zu.

Wir müssen die Digitalisierung nachhaltig voranbringen. Denn: Moderne Technologien sind besser schützbar. Wenn alle Systeme auf dem Stand der Technik sind, können wir die sicherheitsrelevanten Vorzüge nutzen. Dafür müssen wir Schlüsseltechnologien entwickeln und erforschen. Damit meine ich etwa KI-, Quanten-, eID- oder Cloudlösungen.

Wen brauchst Du als Partner, um diese Vision umzusetzen?
Alle. Jede und jeden! Die Cybernation Deutschland zu bauen ist eine Gemeinschaftsaufgabe. Wir brauchen die Akteure aus Politik, Wirtschaft, Wissenschaft und Gesellschaft – und zwar national wie international.

Wie willst Du, wie will das BSI, die Ziele dieser Vision erreichen?
Wir haben einen ganzen Blumenstrauß an konkreten Maßnahmen definiert, die auf diese Ziele einzahlen. Auf einen Punkt möchte ich gerne genauer eingehen:

Wir brauchen vor allen Dingen EIN Lagebild. Dafür ist das Thema Zentralstelle wichtig. Für unsere Cyberresilienzsteigerung ist grundlegend, dass wir transparent

Das Thema Cybersicherheit gehört groß gedacht.
Deutschland muss sich als Cybernation verstehen. Wir – also wir alle als Gemeinschaft – müssen diesem Selbstverständnis Ausdruck verleihen und Taten folgen lassen.
Als die Cybersicherheitsbehörde des Bundes verfolgen wir die Vision, gemeinsam diese Cybernation Deutschland zu bauen.

Wir müssen unsere Technologiekompetenz bündeln. Um das gesamte technologische Potenzial der Cybersicherheit zu heben, brauchen wir eine koordinierte Zusammenarbeit aller Akteure und über alle Grenzen hinweg.

Wir müssen die Cybersicherheit aktiv gestalten. Schnelle Klarheit über Sicherheitseigenschaften der Produkte von morgen schafft Handlungssicherheit. Unsere Vorgaben und Anforderungen bei der Zertifizierung und Standardisierung setzen da bereits an. Unseren Standards im IT-Grundschutz oder unsere Technischen Richtlinien stehen als Vorgaben und Arbeitswerkzeuge bereit, die als Hilfe zur Selbsthilfe für Behörden, Unternehmen und Institutionen dienen.

Wir müssen einen Cybermarkt schaffen. In einem florierenden Cyberökosystem aus dem Dreieck Politik, Wissenschaft und Wirtschaft können sichere digitale Produkte erforscht und entwickelt werden, die dann auch tatsächlich genutzt werden, um die Cybersicherheit zu steigern.

und kooperativ Informationen austauschen, eng zusammenarbeiten und uns gegenseitig unterstützen. Es reicht außerdem nicht aus, nur einen eingeschränkten Bereich im Blick zu haben. Angreifer scannen täglich das gesamte Internet. Diese Transparenznachteile müssen wir ausgleichen. Wir brauchen den gesamten Blick. Nur so können wir als ganzes Land aussage-, handlungs- und entscheidungsfähig sein.

Was meinst Du, wenn Du von Cyberresilienz steigern sprichst?
Wir müssen uns vorsorglich besser vor Cyberangriffen schützen und den Notfall üben. Denn es ist längst nicht mehr die Frage ob, sondern wann wir betroffen sind. Wir müssen in der Lage sein, uns gegenseitig zu helfen und den Regelbetrieb schnell wiederherzustellen.

Am Ende ist das das ultimative Ziel, denn hundertprozentige Sicherheit gibt es nicht. Daran arbeiten wir als Möglichmacher, Partner und Helfer jeden Tag. Lasst es uns gemeinsam anpacken! ■

5G/6G-Security-Lab: Neues Testlabor für 5G-Netze am BSI-Standort Freital

Im August wurde in Anwesenheit von BSI-Präsidentin Claudia Plattner die erste Aufbaustufe des Sicherheitslabors in Betrieb genommen – zukünftig sollen auch 6G-Netze erprobt werden

von Dr. Matthias Weber, Referat Sicherheit der Infrastruktur für Telekommunikationsnetze, 5G/6G

Das BSI hat das Sicherheitslabor „Test Environment for Mobile Infrastructure Security“ (TEMIS) eingerichtet, um zur stetigen Verbesserung der Mobilfunksicherheit in Deutschland beizutragen. TEMIS stellt neben 5G-Netzen (und später auch 6G-Netzen) verschiedener Hersteller auch entsprechende Mess- und Prüfmittel mit Fokus auf sicherheitsrelevante Tests bereit.

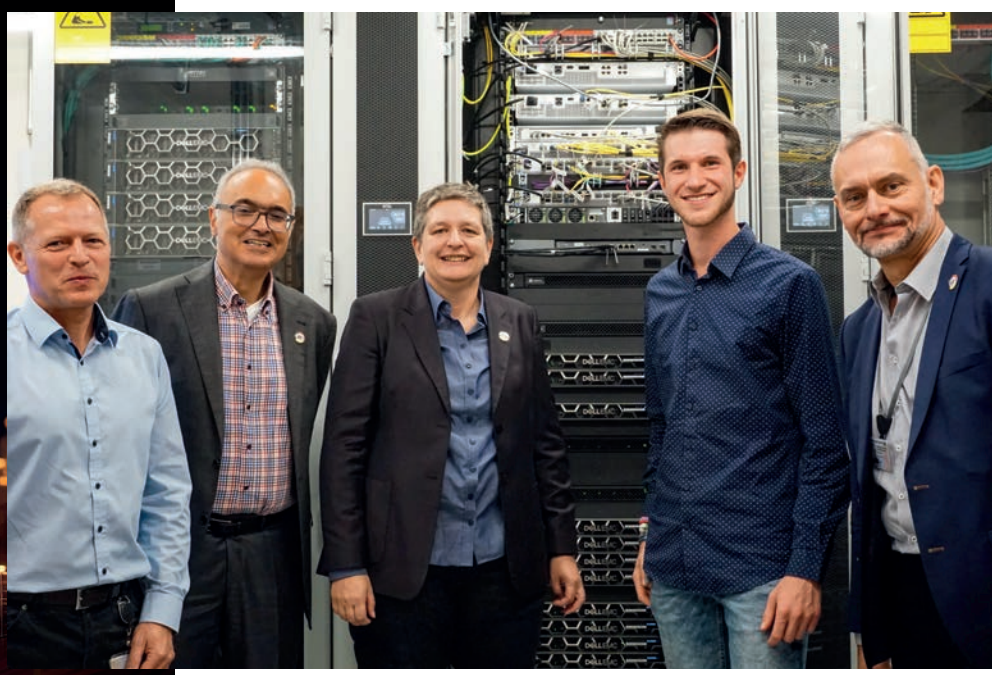
Die Sicherheit von 5G-Netzen ist von großer Bedeutung, da sie die Grundlage für viele Anwendungen und Dienste bilden, die unser tägliches Leben beeinflussen. Die hohe Komplexität des 5G-Standards führt dabei zu Systemen, die nur aufwendig und unter Berücksichtigung vieler Spezialfälle zu testen sind.

Das BSI hat den Anspruch, auch in diesem Gebiet relevante Beiträge mit Bezug zur IT-Sicherheit zu leisten. Dazu sind Arbeiten im Rahmen eines eigenen 5G/6G-Security-Labs unerlässlich – deshalb wurde TEMIS geplant und aufgebaut. Das Sicherheitslabor beinhaltet sowohl kommerzielle 5G-Netzwerktechnik, wie sie von den Mobilfunkbetreibern eingesetzt wird, als auch Open-Source-basierte Bausteine für Tests und Simulationen. Zudem enthält TEMIS eine Testumgebung mit mehreren Funkzellen im eigenen Campusnetz. Das Basissystem umfasst Komponenten für ein Cloud-natives 5G-Kernnetz (Core) sowie Funktechnik (RAN), die sowohl 5G- als auch 4G-Funktionen abdecken. An Erweiterungen des Labors inklusive Open-RAN-Technologie sowie temporärer Teststellungen wird derzeit gearbeitet.

BSI-Präsidentin Claudia Plattner betonte beim Besuch in Freital die Bedeutung des Projekts: „Ein zentrales Thema für das BSI ist die Cybersicherheit in mobilen Infrastrukturen. Mit der ersten Aufbaustufe des 5G/6G-Security-Labs im BSI in Freital haben wir einen wichtigen Meilenstein erreicht.“ Das BSI verfolgt das Ziel, das Sicherheitsniveau und die Resilienz von nationalen und privaten 5G-Netzen kontinuierlich zu erhöhen. Mithilfe des 5G/6G-Security-Labs werden beispielsweise die Vorgaben und Richtlinien für die Netzbetreiber im Einvernehmen mit der Bundesnetzagentur praxisorientiert fortgeschrieben. Weitere inhaltliche Schwerpunkte betreffen Zertifizierung, Standardisierung und Sicherheitsuntersuchungen.

TESTENTWICKLUNG UND -VALIDIERUNG FÜR DIE ZERTIFIZIERUNG

Mit dem IT-Sicherheitsgesetz 2.0 wurde die Zertifizierung für kritische 5G-Netzwerkkomponenten in Deutschland gesetzlich vorgeschrieben. Für 5G wird vom BSI vorrangig das Schema NESAS CCS-GI entwickelt (Network Equipment Security Assurance Scheme Cybersecurity Certification Scheme – German Implementation). NESAS verwendet als Testvorschriften die von der 3GPP – dem Standardisierungsgremium für 5G – definierten Security Assurance Specifications (SCAS). Das BSI hat die Aufgabe, die Prüfgrundlagen für die Prüfstellen zu beschreiben. Dazu müssen die SCAS-Tests validiert, präzisiert und ggf. erweitert werden. Diese Ergänzungen werden in TEMIS evaluiert, Anwendungshinweise und



Im August eröffnete BSI-Präsidentin Claudia Plattner gemeinsam mit Abteilungsleiter Sandro Amendola und Fach- und Führungskräften aus dem in Freital angesiedelten Fachbereich Cyber-Sicherheit in mobilen Infrastrukturen und Chiptechnologie das neue Labor (v.l.n.r. Heiner Grottendieck, Sandro Amendola, Claudia Plattner, Elias Ullrich und Uwe Hoppenz).

Interpretationen technisch abgesichert und anschließend im „Dokument Anwendungshinweise und Interpretationen zum Schema“ (AIS-N2) veröffentlicht. TEMIS dient auch dazu, von den Prüfstellen gemeldete Probleme mit Testfällen nachzustellen und zu bewerten. Für die Reproduzierbarkeit und Automatisierung von Testfällen entwickelt das TEMIS-Team des BSI eine eigene Simulations- und Steuerungsumgebung: das SCAS-Test-Framework.

MITGESTALTUNG SICHERER STANDARDS

Das Prinzip „Security by Design“ muss bereits bei der Entwicklung von Standards und Testspezifikationen für den 5G-Mobilfunk berücksichtigt werden. Die von der 3GPP definierten SCAS-Tests werden daher vom BSI aktiv mitgestaltet, verbessert und, falls nötig, neu initiiert. Das dazu nötige Wissen entsteht vorrangig durch die konkrete Arbeit an der Technik und den Umgang mit repräsentativen Produkten. TEMIS erlaubt die technische Implementierung eigener Entwürfe von Testfällen und die Validierung der bestehenden oder von Dritten vorgeschlagenen Tests. Die daraus resultierenden Beiträge des BSI in den Standardisierungsgremien stärken die IT-Sicherheit. Gleichzeitig bringt das BSI die in Deutschland gewonnenen Erfahrungen in die Arbeit bei den EU-Gremien für ein europäisches 5G-Zertifizierungsschema ein.

ZUSAMMENARBEIT MIT FORSCHUNG UND ENTWICKLUNG

Das BSI hat in der 5G/6G-Sicherheit mit einer Förderrichtlinie zahlreichen Projekten zum Start verholfen. Die Spannbreite reicht dabei von 5G-Prüfstellen über größere Forschungskonsortien bis hin zu Start-ups. Diese Projekte sowie auch Sicherheitsforschende können ihre Ergebnisse mithilfe des 5G/6G-Security-Labs validieren. Erste Analysen mit Wissenschaftlerinnen und Wissenschaftlern konnten bereits erfolgreich durchgeführt werden.

Das Team des BSI freut sich nach der Vorbereitungsphase nun auf die intensive Nutzung der neuen Möglichkeiten für die IT-Sicherheit. ■

Weitere Informationen des BSI zu 5G:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/5-G/5-g_node.html

Weitere Informationen zur Förderrichtlinie des BSI (KoPa45):

https://www.bsi.bund.de/dok/KoPa45

Ransomware, Schwachstellen und Resilienz

Die Lage der IT-Sicherheit in Deutschland 2023

Einmal im Jahr berichtet das Bundesamt für Sicherheit in der Informationstechnik über die Lage der IT-Sicherheit in Deutschland. In seinem diesjährigen Bericht kommt das BSI zu dem Schluss: Die Bedrohung ist so hoch wie nie zuvor. Die Professionalisierung der Angreifer im Cyberraum schreitet ungemindert voran. Staat, Wirtschaft und Gesellschaft brauchen eine entsprechende Abwehr.

RANSOMWARE BLEIBT DIE GRÖSSTE BEDROHUNG

Bei Cyberangriffen mit Ransomware beobachtet das BSI eine Verlagerung der Attacken: Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Mittelpunkt, sondern zunehmend auch kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen. Insbesondere von erfolgreichen Cyberangriffen auf Kommunalverwaltungen und kommunale Betriebe sind die Bürgerinnen und Bürger unseres Landes oft auch unmittelbar betroffen: So kann es dazu kommen, dass bürgernahe Dienstleistungen eine Zeit lang nicht zur Verfügung stehen oder persönliche Daten in die Hände Krimineller gelangen.

AUF DEM VORMARSCH: CYBERCRIME-AS-A-SERVICE

Wie die Realwirtschaft setzen auch Cyberkriminelle zunehmend auf Arbeitsteilung, ein wachsendes Dienstleistungsangebot und eine enge Vernetzung über Länder- und Branchengrenzen hinweg. Mit dem Konzept des „Cybercrime-as-a-Service“ agieren Cyberkriminelle immer professioneller, denn die Spezialisierung auf bestimmte Dienstleistungen ermöglicht es ihnen, ihre „Services“ gezielt zu entwickeln und einzusetzen.

SCHWACHSTELLEN BEI SOFTWARE AUF BESORGNISERREGENDEM NIVEAU

Das BSI registriert immer mehr Schwachstellen bei Software. Diese Schwachstellen sind oft das Einfallstor für Cyberkriminelle auf ihrem Weg zu einer Kompromittierung von Systemen und IT-Netzen. Das BSI hat mit durchschnittlich knapp 70 neuen Schwachstellen in Softwareprodukten pro Tag nicht nur rund ein Viertel mehr registriert als im Berichtszeitraum davor. Mit der Anzahl stieg auch ihre potenzielle Schadwirkung: Immer mehr Lücken (etwa jede sechste) werden als kritisch eingestuft.

GENERATIVE KI SORGT FÜR NEUE RISIKEN, ABER AUCH FÜR NEUE CHANCEN

Mit ChatGPT, Bard und LlaMa sowie einer Vielzahl weiterer Tools ist Künstliche Intelligenz in einer breiten, auch wenig technikaffinen Öffentlichkeit angekommen. Diese Tools sind einfach zu bedienen und liefern eine hohe Qualität. Dabei können sie auch für kriminelle Zwecke missbraucht werden. So können sie dafür sorgen, dass sogenannte Deepfakes – manipulierte Bilder, Videos und Stimmen – immer authentischer werden und dadurch immer schwerer zu entlarven sind. Auch kann KI Phishing-Mails glaubwürdiger machen, im Social Web zu Desinformationskampagnen beitragen oder selbst Schadcode generieren - und das wesentlich schneller und zum Teil wesentlich besser als menschliche Cyberkriminelle. KI kann auch selbst zur Schwachstelle werden. Sie kann gehackt und missbräuchlich eingesetzt werden. Das stellt das Schwachstellenmanagement in Unternehmen und Behörden vor noch nie da gewesene Herausforderungen.

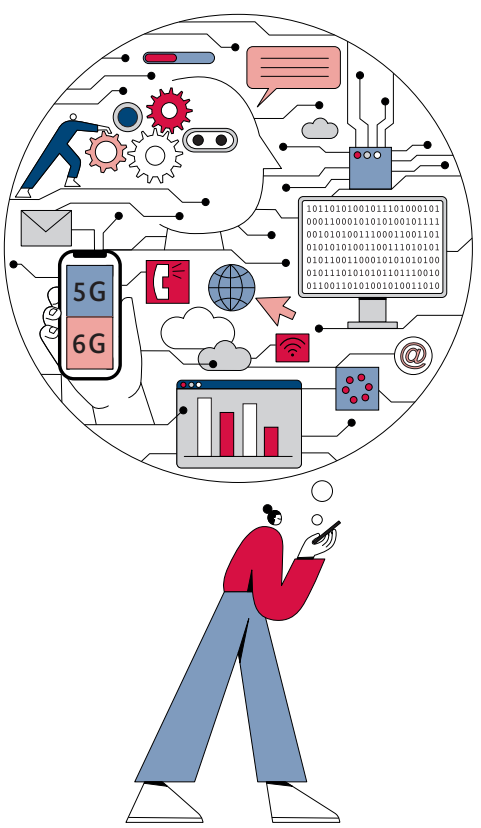
AUSWIRKUNGEN DES UKRAINE-KRIEGS AUF DIE IT-SICHERHEITSLAGE IN DEUTSCHLAND

Der russische Angriffskrieg gegen die Ukraine nahm im Berichtszeitraum weiterhin einen zentralen Platz in der öffentlichen Wahrnehmung ein. Vom BSI registrierte DDoS-Angriffe prorussischer Aktivistinnen und Aktivisten haben in Deutschland bisher aber nur wenig bis keinen bleibenden Schaden anrichten können. Das BSI ordnet die bisherigen Angriffe eher dem Bereich Propaganda zu. Sie sollen Verunsicherung stiften und das Vertrauen in den Staat untergraben. Allerdings kann sich diese Strategie auch ändern, die Vergangenheit hat das gezeigt.

WACHSENDE RESILIENZ GEGEN ZUNEHMENDE BEDROHUNGEN

Eine hundertprozentige Sicherheit gegen Angriffe auf IT-Infrastrukturen und softwaregesteuerte Geräte kann es in einer umfassend vernetzten Gesellschaft nicht geben. Den besten Schutz vor solchen Angriffen bietet aber eine ausgeprägte Cyberresilienz. Dabei geht es darum, die Widerstandsfähigkeit von IT zu erhöhen und Angriffen besser begegnen zu können.

Es werden mehr qualifizierte Sicherheitsexpertinnen und -experten benötigt, um IT-Systeme resilienter zu machen, Angriffe abzuwehren und, im Falle eines erfolgreichen Angriffs, die negativen Folgen zu mindern. Hier hilft eine Professionalisierung auf Abwehrseite – u. a. durch Standardisierung, Zentralisierung und Automatisierung. Staat und Zivilgesellschaft stehen den vielfältigen Bedrohungen im Cyberspace nicht wehrlos gegenüber, sondern können ihnen durchaus erfolgreich begegnen. Dabei steht ihnen das BSI als Cybersicherheitsbehörde des Bundes zur Seite. ■



Alexander Härtel, Nationales IT-Lagezentrum, Analysen und Prognosen

EINBLICK IN DEN MASCHINENRAUM DER CYBERSICHERHEIT – WENN AUS EINEM VORFALL EIN TREND WIRD

Trends in der Bedrohungslage erfasst das BSI mit seinem Threat-Intelligence-Team. Dieses Team beobachtet Angreifer und ihre Vorgehensweisen über einen längeren Zeitraum. Dies erlaubt dem BSI, Meldungen und Vorfälle in einen größeren Kontext einzuordnen und Trends zu erkennen. Daneben werden auch technische Indikatoren gewonnen, die zum aktiven Schutz von Computersystemen, z. B. innerhalb der Bundesverwaltung, eingesetzt werden.

Jeder Trend, der im BSI-Lagebericht 2023 beschrieben wird, fing einmal klein an. Eine einzelne Angreifergruppe entwickelt z. B. eine neue Methode wie das Erpressen mit einer Leak-Seite im Darknet. Diese neue Vorgehensweise kann dem BSI auf unterschiedlichen Wegen bekannt werden. Eine Betroffene oder ein Betroffener kann sich beim Nationalen IT-Lagezentrum im BSI melden. National wie international steht das BSI im ständigen Austausch mit IT-Sicherheitsanalystinnen und -analysten, Partnerbehörden und CERTs. Zusätzlich kauft das BSI auch Threat-Intelligence bei kommerziellen Anbietern ein, um Bedrohungsentwicklungen außerhalb Deutschlands zu verfolgen, da Angreifer nur selten an Landesgrenzen stoppen. Und das ist nur die Spitze des Eisbergs.

Sobald eine neue Methode bekannt wird, stellen sich verschiedene Fragen. Bei finanziell motivierten Angreifern ist es entscheidend abzuwägen, ob diese Methode für die Angreifer einen finanziellen Gewinn bringt. Wenn Angriffe leichter werden oder sich die Erfolgschance für einen Angriff erhöht, besteht ein Risiko, dass sich die Methode ausbreitet und schnell zu einem neuen Trend wird.

Da heute nahezu jeder Bestandteil eines Angriffs als Service angeboten wird, steht eine neue Methode schnell vielen Angreifern zur Verfügung. Hierbei kann auch eine Dynamik zwischen Cyberkriminellen beobachtet werden, die diese Services anbieten. Methoden werden übernommen, weiterentwickelt und noch mehr Angreifern zur Verfügung gestellt. So wurde aus der Erpressung mit Ransomware innerhalb weniger Monate Double Extortion - das Erpressen mit Verschlüsselung von Daten beim Betroffenen und gleichzeitiger Androhung der Veröffentlichung gestohlener Daten.

Ein neuer Trend kann nur selten gestoppt werden. In einer potenziell kritischen Situation wie der akuten Ausnutzung einer Schwachstelle warnt das BSI gezielt die betroffenen Sektoren der Wirtschaft oder auch die Öffentlichkeit. Bei länger anhaltenden Trends werden die Maßnahmenempfehlungen des BSI entsprechend angepasst.

Es ist entscheidend, dass sich Betroffene beim BSI melden. Je nach Vorfall kann das BSI Erkenntnisse über den vermuteten Angreifer teilen oder auch direkt unterstützen. Die Informationen über die Vorgehensweise eines Angreifers kann einer/einem Betroffenen beispielsweise Aufschluss darüber geben, auf welchem Weg ein Angriff stattfand und welche Systeme in einem IT-Netz kompromittiert sein könnten. In Absprache mit der/dem Betroffenen können gewonnene Erkenntnisse wie technische Indikatoren anonym national wie international mit vertrauenswürdigen Partnern geteilt werden.

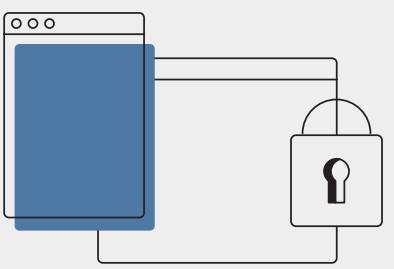
Die Arbeit im Threat-Intelligence-Team ist also die Suche nach der nächsten großen Welle, bevor sie das Land erreicht. Diese zu erkennen, zu verstehen und zu kommunizieren ist herausfordernd, aber auch sehr spannend. ■

Die Lage der IT-Sicherheit in Deutschland 2023 im Überblick

Ransomware

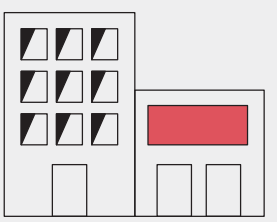
ist weiterhin die größte Bedrohung.

2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

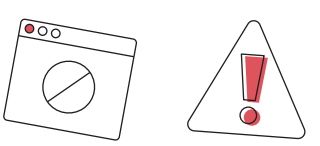
15 davon richteten sich gegen **IT-Dienstleister**.



Mehr als **2.000** **Schwachstellen** in Softwareprodukten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

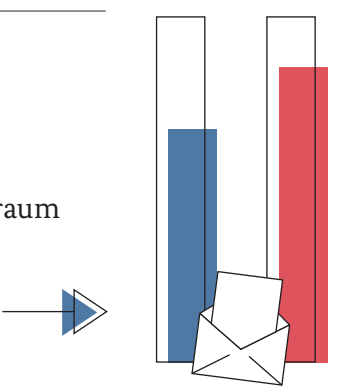
Eine Viertelmillion

neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



66%

aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
34 % Erpressungsmails,
32 % Betrugsmails

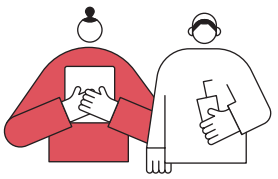


84%

aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

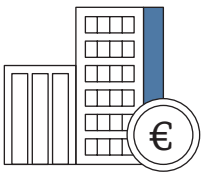
Top-3-Bedrohungen je Zielgruppe:

Gesellschaft



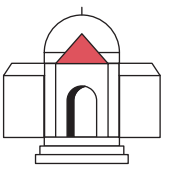
Identitätsdiebstahl
Sextortion,
Phishing

Wirtschaft

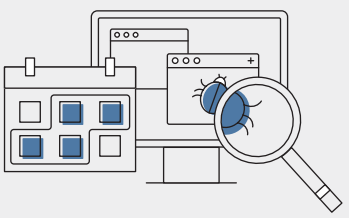


Ransomware
Abhängigkeit innerhalb der IT-Supply-Chain,
Schwachstellen, offene
oder falsch konfigurierte Onlineserver

Staat und Verwaltung

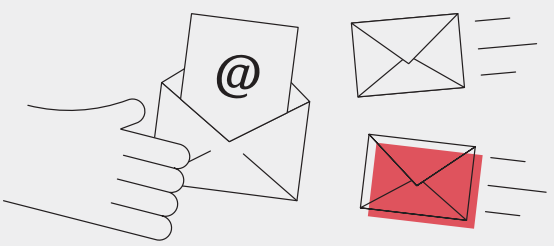


Ransomware
APT,
Schwachstellen, offene oder
falsch konfigurierte Onlineserver

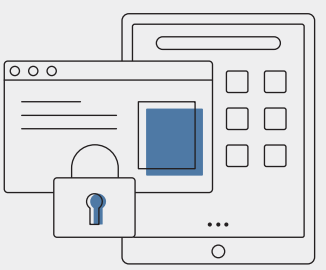


Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.



370 **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.



6.220
2022

5.100
2021

7.120
Teilnehmer hatte die **Allianz für Cyber-Sicherheit** im Jahr 2023.

Deutschland
Digital•Sicher•BSI•

Cybersicherheit auf der Agenda: Das BSI bei der it-sa Expo&Congress

Bei der diesjährigen it-sa Expo&Congress, die vom 10. bis 12. Oktober 2023 in Nürnberg stattgefunden hat, standen zum Aufbau der Cybernation Deutschland diverse Themen auf der Messe-Agenda des BSI. Zahlreiche BSI-Mitarbeitende präsentierten ihre Lösungen, Produkte oder Projektergebnisse am stark frequentierten Stand des BSI und tauschten sich auf fachlicher Ebene mit den Besucherinnen und Besuchern aus. Drei Kolleginnen und Kollegen liefern einen Einblick in ihre Messetage.

MICHAEL KRAUSS, REFERAT CYBER-SICHERHEIT FÜR KLEINE UND MITTLERE UNTERNEHMEN

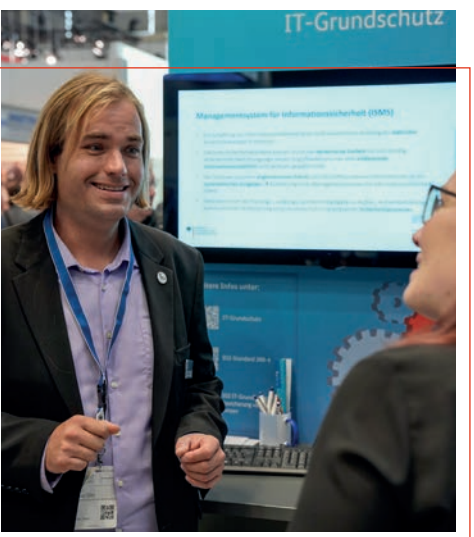
„Der Schutz kleiner und mittlerer Unternehmen liegt meinen Team-Kolleginnen und -Kollegen und mir sehr am Herzen. An unserem Präsentationsstand konnten wir, unterstützt durch unsere Informationsmaterialien, die interessierten Standbesuchenden in einer Vielzahl von Gesprächen über Maßnahmen zur Erhöhung ihrer Cybersicherheit informieren. IT-Dienstleister haben wir darauf hingewiesen, wie sie kleine und Kleinstunternehmen anhand der von uns mitentwickelten DIN Spec 27076 „IT-Sicherheitsberatung für Klein- und Kleinstunternehmen“ sicher in die digitale Zukunft begleiten können. In der Speakers Corner hat mein Referatsleiter Manuel Bach über die Gefahren der Nutzung der Informationstechnik informiert und Hinweise gegeben, wie sich Unternehmen besser aufstellen können. Dabei ist es gar nicht so schwierig sich zu schützen. Das BSI bietet hier eine Reihe von Angeboten.

Die Messe war wieder eine runde Sache und aus meiner persönlichen Sicht ein voller Erfolg. Wir freuen uns auf das nächste Mal. it-sa 2024 in Nürnberg: Wir kommen!“

MARION DEMAND, REFERAT VIRTUALISIERUNG UND CLOUD-SICHERHEIT

„Mein Kollege Heiko Großkopf und ich waren gemeinsam für das Cloud-Team auf der it-sa. Die Standbesuchenden stellten grundlegende Fragen zur sicheren Cloud-Nutzung, zu Cloud-Migration und zum C5. Wir hatten zudem spannende Gespräche zu Spezialthemen wie Edge Computing oder zur Digitalen Souveränität. Dabei war es uns wichtig, auf eine durchdachte Nutzung sowie auf die geteilte Verantwortung in der Absicherung von Cloud-Diensten hinzuweisen. Neben dem Standdienst habe ich Aspekte der sicheren Cloud-Nutzung auch bei einem Vortrag in der Speakers Corner vorgestellt.

Die it-sa-Teilnahme war sehr bereichernd, besonders die speziellen Anwendungsfälle und Sichtweisen aus der Praxis kennenzulernen. Aber auch der Austausch mit Kollegen am Stand war sehr inspirierend. Mein Fazit: Der Standdienst war zwar auch anstrengend, das Positive überwog aber. Ich freue mich schon auf meinen nächsten Einsatz auf der it-sa."



DANIEL GILLES, REFERAT BSI-STANDARDS UND IT-GRUNDSCHUTZ

„Für mich stellt die it-sa immer eine hervorragende Gelegenheit dar, mit unseren Anwenderinnen und Anwendern in den direkten Kontakt zu kommen. So kann ich für unser Team aktuelle Trends aufgreifen und in persönlichen Gesprächen auf die aktuellen Entwicklungen des IT-Grundschutzes eingehen. Wesentliches Thema hierbei waren dieses Jahr unterschiedliche Stellschrauben zur Optimierung des IT-Grundschutzes wie die Reduktion von Dokumentationsaufwänden oder die Integration und Synergie mit weiteren Themen wie BCM, Mindeststandards usw.

Mein persönliches Anliegen ist, dass wir unsere unterschiedlichen Zielgruppen in diese Themen frühzeitig mitnehmen und wir uns der offenen Diskussion dazu stellen. Die it-sa ist hierzu die Gelegenheit."

Deutschlands IT-Sicherheit laufend verbessern

Dafür agiert das BSI vielfältig, mit Normsetzung, Informationshandeln und operativer Cyberabwehr: Teil 2 des Überblicks über die Befugnisse des Bundesamtes

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

Das BSI arbeitet daran, Angriffe, aber auch Lücken in der IT-Sicherheit der Bundesverwaltung zu erkennen und zu beheben. Die Befugnisse und Abläufe in der Zusammenarbeit zwischen dem Bundesamt und anderen Einrichtungen sind dabei ganz genau geregelt. Das BSI agiert dabei sowohl im Hintergrund und präventiv als auch operativ sogar vor Ort in herausgehobenen Fällen.

Das BSI betreibt für die Bundesverwaltung mehrere Systeme zur Erkennung und Abwehr von Schadprogrammen. Hierzu gehören z. B. ein Schadprogramm-Erkennungssystem, ein Schadprogramm-Präventionssystem und der Bundescloud-Dienst Detection-as-a-Service. Mit diesen Programmen darf das BSI gemäß §§ 5 und 5a BSIG zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes Protokolldaten, Protokollierungsdaten und sogenannte Schnittstellendaten automatisiert sowie manuell untersuchen.

Eine manuelle Verarbeitung der analysierten Daten erfolgt nur, wenn die automatisierte Analyse einen begründeten Verdacht geliefert hat und ein Bediensteter mit einer Befähigung zum Richteramt diese anordnet. In der manuellen Verarbeitung kann dann abschließend geklärt werden, ob sich der Verdacht erhärtet hat und welche Art von Angriff vorliegt. Die Befugnisnorm unterscheidet zwischen Protokollierungs-, Protokoll- und Schnittstellendaten, wobei letztere auch Inhaltsdaten enthalten können, und stellt dafür unterschiedliche Anforderungen vor allem mit Blick auf die zulässige Speicherdauer auf.

Anfallende Kommunikationsdaten und personenbezogene Daten werden gemäß den Vorgaben des BSIG gelöscht. Hierzu gibt es ein sorgfältig erarbeitetes und mit dem Bundesdatenschutzbeauftragten abgestimmtes Datenerhebungs- und Verwendungskonzept.

SCANBEFUGNIS – MIT EINSCHRÄNKUNGEN

„Das BSI wird zur Hackerbehörde!“ An diese plakative Schlagzeile können sich sicherlich die meisten Kolleginnen und Kollegen noch erinnern. Grund für diese Berichterstattung in den Medien war die sogenannte Scanbefugnis, die in § 7b BSIG enthalten ist. Diese Befugnis ermöglicht die Detektion von Sicherheitslücken und anderen Sicherheitsrisiken an den Schnittstellen zwischen TK-Netz und der Bundesverwaltung sowie KRITIS, UBIs und digitalen Diensten gem. § 2 Abs. 11 BSIG.

Die Scans dürfen ausschließlich anhand der „weißen Liste“ durchgeführt werden, welche die IP-Adressen von den vorstehend genannten Stellen und Einrichtungen enthält. Ein tatsächlicher Scan darf dann allerdings nur bei ungeschützten Systemen durchgeführt werden. Ein System ist ungeschützt, wenn öffentlich bekannte Sicherheitslücken oder sonstige offensichtlich unzureichende Sicherheitsvorkehrungen vorliegen.

Erkennt das BSI mittels Scan eine Sicherheitslücke oder eine unzureichende Sicherheitsvorkehrung, muss es die Betroffenen unverzüglich informieren. Nach Möglichkeit sind konkrete Hinweise zur Abhilfe mitzuteilen. Der BfDI wird vom BSI jährlich über die nach § 7b BSIG durchgeführten Scan-Maßnahmen informiert.

Überblick über die Befugnisse des BSI gegenüber der Bundesverwaltung

- Sicherheitsvorgaben und -überprüfungen (siehe BSI-Magazin 01/2023)
  - Mindeststandards
  - Freigaben und Zulassungen nach Verschlusssachenanweisung
  - Informationshandeln im Rahmen der zentralen Meldestelle
- Operative Befugnisse
  - Schadprogramm-Erkennungssystem u. a.
  - Scanbefugnis
  - Mobile Incident Response Teams (MIRTs)

EINSATZ EINES MOBILE INCIDENT RESPONSE TEAMS

§ 5b BSIG ermöglicht eine sehr konkrete Variante der Unterstützung: Die Entsendung eines Mobile Incident Response Teams (MIRT) auf Ersuchen einer Stelle des Bundes. Das BSI kann und darf allerdings nicht in jedem Fall Unterstützung nach § 5b BSIG leisten, sondern nur in den sogenannten herausgehobenen Fällen nach § 5b Abs. 2 BSIG. Ein solcher Fall liegt zum einen dann vor, wenn der Angriff auf ein informationstechnisches System eine besondere technische Qualität aufweist. Hiermit sind z. B. APT-Angriffe gemeint, bei denen meistens neuartige Angriffsvektoren eingesetzt werden. Zum anderen liegt ein herausgehobener Fall dann vor, wenn die Wiederherstellung der betroffenen Systeme im besonderen öffentlichen Interesse liegt.

Gemeinsam mit den betroffenen Stellen wird ein Vorfall bewertet und die zur Wiederherstellung der Sicherheit und/oder Funktionsfähigkeit der betroffenen Systeme erforderlichen Maßnahmen beschlossen.

FAZIT

Der Überblick über die Befugnisse des BSI gegenüber der Bundesverwaltung zeigt, dass das BSI eine Vielzahl von Aufgaben aus ganz unterschiedlichen Bereichen wahrnimmt. Ziel ist aber bei allen Handlungen und Empfehlungen die Steigerung der IT-Sicherheit Deutschlands.

Um dies zu erreichen, sind alle drei Tätigkeitsbereiche des BSI (Sicherheitsvorgaben und -überprüfungen, Informationshandeln und operative Tätigkeit) gleichbedeutend. Auch wenn operative Einsätze vor allem nach außen stärker wirken: Wenn etwa ein Bundesserver angegriffen wurde und ein MIRT eingesetzt wird, das die Funktionen wiederherstellen kann, ist das natürlich besonders greifbar. Doch auch das Sammeln und Auswerten von Informationen sowie die Wirkmächtigkeit der Normsetzungsbefugnisse sind ebenso wichtige Werkzeuge bei der täglichen Arbeit des BSI gegen Cyberbedrohungen und für mehr IT-Sicherheit. ■

#TeamBSI ist startklar für die Zukunft

Personalentwicklung beim BSI fördert fachliche Kompetenzen ebenso wie Führungsfähigkeiten und Teamgeist

von Anna Eichhorst, Anke Gaul, René Karle und Mareike Mumm, Referat Personalentwicklung #TeamBSI

Die Zukunft ist ungewiss, aber nicht vorherbestimmt. Wer zum #TeamBSI gehört, kann die Zukunft mitgestalten, das macht die Arbeit so spannend. Neben hoher Fachkompetenz braucht es dafür auch ein wachstums- und entwicklungsorientiertes Mindset, das entscheidend dafür ist, wie mit Problemen, Herausforderungen und Aufgaben umgegangen wird. An beidem richtet die Personalentwicklung im BSI ihre Maßnahmen konsequent aus – in der individuellen Weiterqualifizierung, in der Führungskräfteentwicklung und mit Blick auf die Optimierung von Zusammenarbeit und Kooperation.

Die Zukunft im Blick zu haben heißt im dynamischen Cyberumfeld, vor der Lage zu sein. Das gilt nicht nur für den technologischen Fortschritt, der neben neuen Anwendungen auch neue Angriffsszenarien bringt, sondern auch für die Menschen im #TeamBSI, die diesen Herausforderungen begegnen.

Das Wissen im IT-Bereich unterliegt einer extrem geringen Halbwertszeit und kontinuierlicher Veränderung. Die Anforderungen an die Spezialistinnen und Spezialisten aus dem #TeamBSI, die mit ihrem Know-how das BSI und damit die IT-Sicherheit als einen Grundpfeiler der Gesellschaft schützen, sind daher hoch.

Gleichzeitig gilt: Die besten Ergebnisse erzielen wir im Team. Mit Blick in die Zukunft investiert das BSI daher bereits seit Jahren massiv in eine moderne Personalentwicklung. Ein Umfeld des dauerhaften Lernens ist kein Nice-to-have, sondern ein wesentlicher Bestandteil der Alltagsgestaltung aller Mitarbeitenden – vom Top-Management bis zur Basis.

Die Entwicklung der Mitarbeitenden ist erfolgskritisch, um die Rolle des BSI als wirkungsvoller Partner in der Cybersicherheit dauerhaft zu manifestieren. Zudem sehen wir unsere Investition in das Potenzial eigener Fach- und Führungskräfte als Chance, uns auf dem Arbeitsmarkt als attraktiver Arbeitgeber zu positionieren.

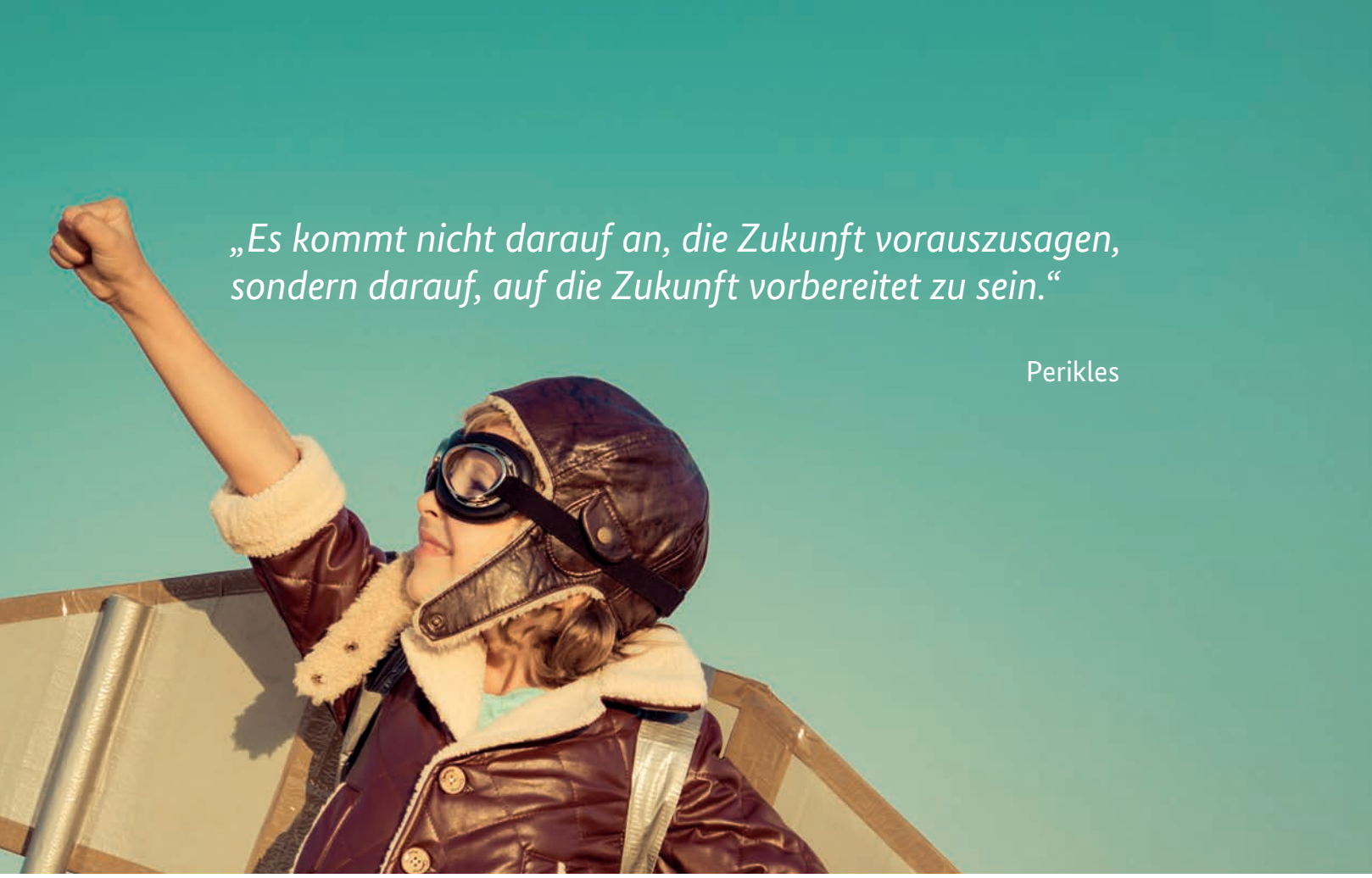
„Indem wir Fähigkeiten erweitern und Wachstum fördern, legen wir den Grundstein für den langfristigen Erfolg unseres Teams und unserer Organisation."

BSI-Präsidentin Claudia Plattner

UNTERSTÜTZUNG FÜR FÜHRUNGSKRÄFTE

Ein zentraler Stellhebel für die Zukunftsfähigkeit jeder Organisation ist gute Führung. Denn sie kann enorme Potenziale freisetzen, die wir in einem modernen öffentlichen Dienst dem Fachkräftemangel, volatilen Märkten & Co entgegensetzen möchten und müssen.

Die Anforderungen an Führung sind dabei auch im #TeamBSI in den vergangenen Jahren vielschichtiger geworden. Gründe dafür sind: ein starker Aufwuchs, mehrere Generationen mit unterschiedlichen Bedürfnissen und Werten am Arbeitsmarkt, wechselnde Teamkonstellationen, digitale und hybride Arbeitsformen und -mittel, sich ändernde und immer komplexer werdende Rahmenbedingungen.



Damit Führung erfolgreich ist, also einen positiven Effekt auf die Gesamtleistung der Organisation hat, braucht es die Akzeptanz der eigenen Rolle als Führungskraft, für die wesentlich mehr Kompetenzen entscheidend sind als „nur“ die fachliche Bewertungsfähigkeit eines Themas.

Um diese Anforderungen transparenter und greifbarer zu machen, hat das BSI im Kompetenzmodell für Führungskräfte im BSI die zentralen Fähigkeiten und Fertigkeiten beschrieben, die Personen in Führungsfunktion haben und auch konstant weiterentwickeln sollen. Das Modell wird kontinuierlich angepasst und dient als wertvolle Grundlage und effektives Hilfsmittel sowohl für eine zielgerichtete Personalentwicklung unserer Führungs- und Nachwuchsführungskräfte als auch im Recruiting auf diesen Ebenen.

Ein weiteres strategisches Steuerungselement ist der 2019 initiierte Prozess Führung@BSI_2025: Innovative Führungsinstrumente kennenlernen, aktuelle Leadership-Impulse in Kurzworkshops und -vorträgen aufnehmen, Austausch in neuen Formaten intensivieren, aber auch den Führungsnachwuchs aus den eigenen Reihen entwickeln sind beispielhafte Maßnahmen, die das klassische Angebot an Qualifizierung und Begleitung, etwa durch Coachings, ergänzen.

ZUKUNFTSKOMPETENZEN IM FOKUS

Aber nicht nur die Anforderungen an Führungskräfte verändern sich. Die Arbeitswelt verlangt von allen Mitarbeitenden ein hohes Tempo bei der Anpassung, etwa an lebenslanges Lernen, die Digitalisierung der Arbeitsmittel und der Zusammenarbeit und an eine neue Komplexität der Informationen. Gleichzeitig können die Mitarbeitenden im #TeamBSI die Zukunft mitgestalten. Dafür haben wir das Kompetenzmodell um sogenannte Zukunftskompetenzen ergänzt, die gemeinsam in der Personalentwicklung mit Stakeholdern und Zukunftsgestaltern erarbeitet und verabschiedet wurden. Neben spezifischen Kompetenzen ist eine generelle wachstums- und entwicklungsorientierte Grundhaltung entscheidend.

„Die gute Beziehung, die unsere Führungskräfte zu ihren jeweiligen Teams aufbauen, ist ein großes Pfund für die Kultur im #TeamBSI!“

Mareike Mumm, Führungskräfte-Entwicklung

Ein intensives und zugleich niedrigschwelliges „Aufschlauen“ ermöglicht das „Kompaktprogramm Zukunftskompetenz“. In Lernwerkstätten bearbeiten die Teilnehmenden u. a. die Themen „Arbeitswelt der Zukunft“, „Digitale Transformation“ und „Agiles Arbeiten“. Dabei geht es neben der Wissensver-

Berufswunsch: Digitalisierung und Cybersicherheit?

Übernehmt spannende Aufgaben und leistet einen wertvollen Beitrag für die sichere Digitalisierung in Deutschland.

Für den Einstieg ins #TeamBSI gibt es verschiedenste Möglichkeiten.

PRAKTIKUM

Ihr sucht einen Platz für ein Pflichtpraktikum oder plant ein freiwilliges Praktikum (Dauer mind. 10 Wochen) und habt Lust auf spannende Aufgaben im Bereich Cyber-Security?

ABSCHLUSSARBEIT

Noch kein Thema für die Bachelor- oder Masterarbeit und Interesse an Themen wie Cloud-Security, KI, digitalem Verbraucherschutz oder Automotive?

DIREKTEINSTIEG

Schaut gerne auf unserer Karriereseite vorbei – dort findet ihr zahlreiche spannende Stellenangebote zu verschiedensten Themen aus der Cybersicherheit. Und falls nichts Passendes dabei ist, gibt es die Möglichkeit, sich „initiativ“ über unsere Ausschreibung „digitale Talente“ bei uns zu bewerben.
Werdet auch ihr Teil des #TeamBSI.

Weitere Infos auf
www.team-bsi.de

mittlung um den Transfer in den beruflichen Alltag bzw. dessen zeitnahe Reflexion in Peer-Gruppen. Außerdem fördern wir im Zuge des Programms die Vernetzung der Teilnehmenden untereinander sowie mit wichtigen Playern inner- und außerhalb des BSI. So entsteht eine stabile, standortübergreifende Community, welche die Zukunft des BSI aktiv mitgestalten wird. Ein entsprechendes Pilotprojekt mit einer ersten Gruppe von 16 Multiplikatoren aus allen Bereichen des BSI ist gerade gestartet.

Das Inhouse-Schulungsprogramm bietet auch einzeln buchbare – vielfach virtuelle – Trainings an, die bereits heute allen Mitarbeitenden zur Verfügung stehen. Neu aufgelegt wurde auch die BSI-eigene Projektleitungsqualifizierung. In Modulen werden die Teilnehmenden optimal vorbereitet, Cybersicherheitsprojekte mit teils sehr hohen finanziellen Volumina zu leiten.

KULTUR DER ZUSAMMENARBEIT

Neben der richtigen Qualifikation braucht es Zeit und Raum „on the Job", um Neues gemeinsam auszuprobieren. Dafür gibt es im BSI vielfältige freiwillige Formate: Einmal im Quartal wird BSI-weit der „Open Friday" geblockt, um diesen Tag für Neues, Kreatives oder auch lange Aufgeschobenes zu nutzen. Bei den „Open Friday Impulsen" können Mitarbeitende ein Thema ihrer Wahl in 45-minütigen Sessions teilen und dabei auch Kolleginnen und Kollegen von anderen Standorten kennen lernen.

Der „New Normal Boxenstopp" lädt die Referate zum Innehalten ein. Mithilfe eines kurzen Leitfadens kann im Team gecheckt werden, ob die Arbeitsbedingungen, die Zusammenarbeit sowie die Kompetenzen den aktuellen Herausforderungen gewachsen sind oder ob im Sinne von Effektivität der Zusammenarbeit nachjustiert werden könnte.

Die regelmäßigen Pulsbefragungen erfassen ein aktuelles Stimmungsbild zu ausgewählten Themen wie z. B. „Belonging" oder „Psychische Gesundheit in der digitalen Zusammenarbeit". Mit den Ergebnissen können Mitarbeitende wie Führungskräfte aktiv Verbesserungen im Team und darüber hinaus anstoßen. Unter dem Motto „Vielfalt ist Mehrwert" sensibilisieren Aktionen wie der „Gender Diversity Impulse" oder der „Vielfaltsmonat" im Mai 2023 die Belegschaft für Chancengerechtigkeit und Inklusion.

„Risiken zu bewältigen und dabei mit einem Team gleichzeitig auf innovative Lösungen im Sinne des Kundennutzens hinzuarbeiten erfordert von Projektleitungen neben einer Methodenkompetenz ein hohes Maß an Flexibilität und Kommunikationsstärke."

Anja Zimmermann, Leiterin Vergabe und Projektbegleitung

MITARBEITENDE UND TEAMS STEHEN IM MITTELPUNKT

Zusammenfassend lässt sich sagen, dass das #TeamBSI bei der Personalentwicklung individuelles Wachstum und organisationale Weiterentwicklung verknüpft. Die Mitarbeitenden stehen im Mittelpunkt: Ihre Fähigkeiten und Potenziale gilt es zu fördern. Die Integration und Anwendung von Technologie, die eine Kultur der Zusammenarbeit fördert und die kontinuierliche Lernprozesse, Diversität und Inklusion berücksichtigt, wird erfolgsentscheidend sein und legt damit den Grundstein für eine sichere digitale Welt, die den Anforderungen von morgen gewachsen ist. Es ist definitiv ein ambitionierter Weg, aber das #TeamBSI ist startklar für die Zukunft. ■

Weitere Informationen:

https://www.team-bsi.de

Das Projekt WiBA: Leichter Einstieg in die Cybersicherheit für Kommunen

So gelingt der „Weg in die Basis-Absicherung“ mit einfachen Mitteln

von Carmen Gros und Florian Hillebrand, Projektgruppe WiBA

Insbesondere für kleine Kommunen bietet der neue „Weg in die Basis-Absicherung“ (WiBA) einen niedrigschwelligen Einstieg in den IT-Grundschutz – und das kostenlos. Anhand von Checklisten mit einfachen Prüffragen und zugehörigen Hilfsmitteln können Kommunen jetzt die dringlichsten Maßnahmen selbst identifizieren und umsetzen. Damit gelingt ihnen ein erster, aber wesentlicher Schritt in Richtung systematischer Informationssicherheit.

In den vergangenen Jahren hat es mehrfach erfolgreiche Cyberangriffe auf Kommunen gegeben – mit teils gravierenden Folgen und einem großen Medienecho. Kommunale Behörden sind für Cyberkriminelle ein attraktives Ziel mit großem Schadenspotenzial. Erleichtert werden solche Angriffe durch eine oft nur rudimentäre Absicherung – was häufig daran liegt, dass für die Informationssicherheit nur geringe Ressourcen zur Verfügung stehen.

Standardisierte Vorgehensweisen zum Aufbau eines Managementsystems für Informationssicherheit (ISMS), die eine systematische Umsetzung von Schutzmaßnahmen ermöglichen, sind häufig sehr komplex. Zwar bietet etwa der IT-Grundschutz des BSI mit der sogenannten Basis-Absicherung eine vereinfachte Einstiegsmethodik an, doch auch diese wird häufig im kommunalen Bereich noch als zu aufwendig empfunden.

Im Herbst 2022 hat das BSI daher das Projekt „Weg in die Basis-Absicherung“ (WiBA) initiiert, um vor allem für Kommunen den Einstieg in die Informationssicherheit zu vereinfachen und praxisnah zu gestalten.

Durch themenspezifische Checklisten und in enger Abstimmung mit kommunalen Akteuren wurde eine Möglichkeit geschaffen, auch ohne tiefere Kenntnis einer formalen Methodik zunächst Sachstände zur Informationssicherheit zu erheben und essenzielle Maßnahmen zur Verbesserung zu identifizieren.

Die Checklisten decken fundamentale Sicherheitsanforderungen für knapp 20 relevante Bereiche der Informationssicherheit ab. Dazu gehören Checklisten zu technischen Themenfeldern wie Serversystemen oder Backups, aber auch Listen zu organisatorischen Bereichen, etwa zur Vorbereitung für IT-Sicherheitsvorfälle.

Mit dem neuen Einstiegslevel können Kommunen ein Schutzniveau aufbauen, das sie im Anschluss nahtlos auf das Niveau des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“ anheben können.

DAS CHECKLISTEN-KONZEPT

Ausgehend vom IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“, das durch die „Arbeitsgruppe kommunale Basis-Absicherung“ der kommunalen Spitzenverbände (AG KoBa) erstellt und gepflegt wird, wurden im Projekt WiBA die wesentlichen Themenfelder und essenziellen Anforderungen zur Informationssicherheit identifiziert, die im kommunalen Behördenumfeld relevant sind.

Die Anforderungen wurden anschließend in Checkfragen überführt, die den Verantwortlichen in den Kommunen in Form von einfachen Ja/Nein-Fragen eine Erhebung des aktuellen Status der Informationssicherheit ermöglichen. Viele der Checkfragen enthalten zudem Hilfsmittel, die bei der Umsetzung offener Maßnahmen unterstützen. Hilfsmittel können aus konkreten Erläuterungen bestehen, aber auch Verweise auf weiterführende Informationen enthalten, die beispielsweise vom BSI bereitgestellt werden.

ERFOLGREICHE ERPROBUNG IN MODELLKOMMUNEN

Um die Checklisten möglichst praxisnah zu gestalten, wurde frühzeitig eine Pilotphase in Modellkommunen geplant. Auf einen entsprechenden Aufruf im Februar 2023 erhielt das BSI über 130 Bewerbungen von interessierten Kommunen. Aus diesen wurden auf Basis verschiedener Kriterien wie Größe, regionaler Lage und bisheriger Erfahrungen im Bereich Informationssicherheit sechs Modellkommunen ausgewählt. In diesen Kommunen fand im Mai und Juni 2023 jeweils ein mehrtägiger Workshop statt, um Praxiserfahrungen und Rückmeldungen zu sammeln. Das Feedback zu WiBA fiel hier sehr positiv aus und konnte bereits in die Checklisten einfließen, die im August als Community Draft veröffentlicht wurden.

VERÖFFENTLICHUNG UND NÄCHSTE SCHRITTE

Auch der Community Draft erhielt umfassendes und sehr positives Feedback, was zeigt, wie wichtig eine einfache Einstiegsvariante in die Informationssicherheit ist und dass ein großer Bedarf dafür besteht.

Die auf dieser Grundlage nochmals überarbeiteten Checklisten wurden rechtzeitig zur IT-Sicherheits-Messe it-sa 2023 im Oktober in Nürnberg veröffentlicht.

WiBA ist jedoch ein „lebendes“ Projekt: Nicht nur die Hilfsmittel sollen fortlaufend erweitert werden, um die Checklisten noch hilfreicher und praxisnäher zu gestalten. WiBA muss auch angepasst werden, sobald das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“, das den Checklisten zugrunde liegt, auf einen neuen Stand gebracht wird. ■

Diese Themen behandeln die WiBA-Checklisten:

- Arbeit außerhalb der Institution
- Arbeit innerhalb der Institution / Haustechnik
- Backup
- Client
- Drucker / Multifunktionsgeräte
- IT-Administration
- Mobile Endgeräte
- Netze
- Organisation und Personal
- Outsourcing
- Bürosoftware
- Rollen und Rechte / Authentisierung
- Serverraum und Datenträgerarchiv
- Serversysteme
- Sicherheitsmechanismen
- Telefonie und Fax
- Umgang mit Informationen
- Vorbereitung für Sicherheitsvorfälle
- Webserver und Webanwendungen

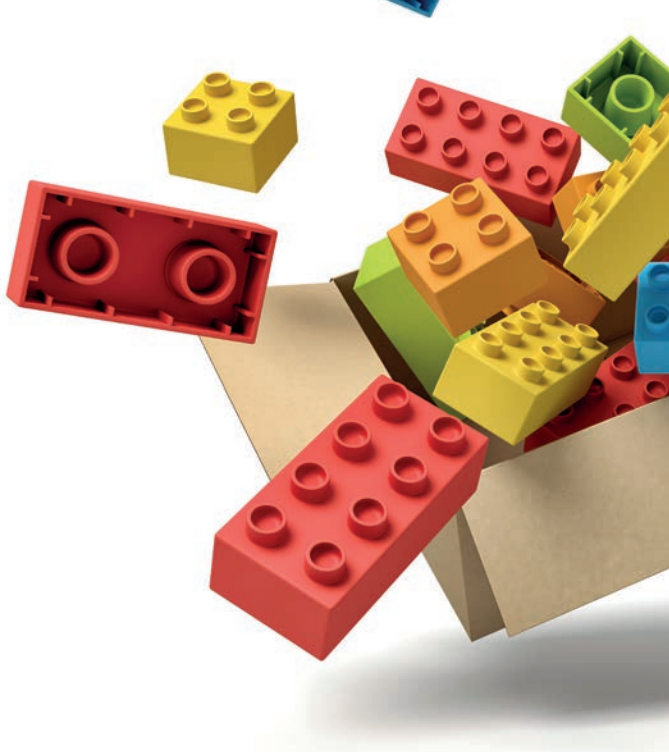
Beispiel: Typische Checkfrage zum Thema IT-Administration

Zu prüfende Anforderung	Aufwand	Erfüllt		
		Ja	Nein	Nicht relevant
Erfordern Aktionen mit administrativen Rechten eine vorherige sichere Authentisierung?	1	✗		
Es sollte mindestens ein sicheres Passwort genutzt werden. Falls möglich, sollte hierfür eine Mehr-Faktor-Authentisierung genutzt werden.				
Notizen Alle Administrationskonten nutzen 2FA mittels USB-Token und Passwort gemäß Richtlinie.				

Weitere Informationen:

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

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html



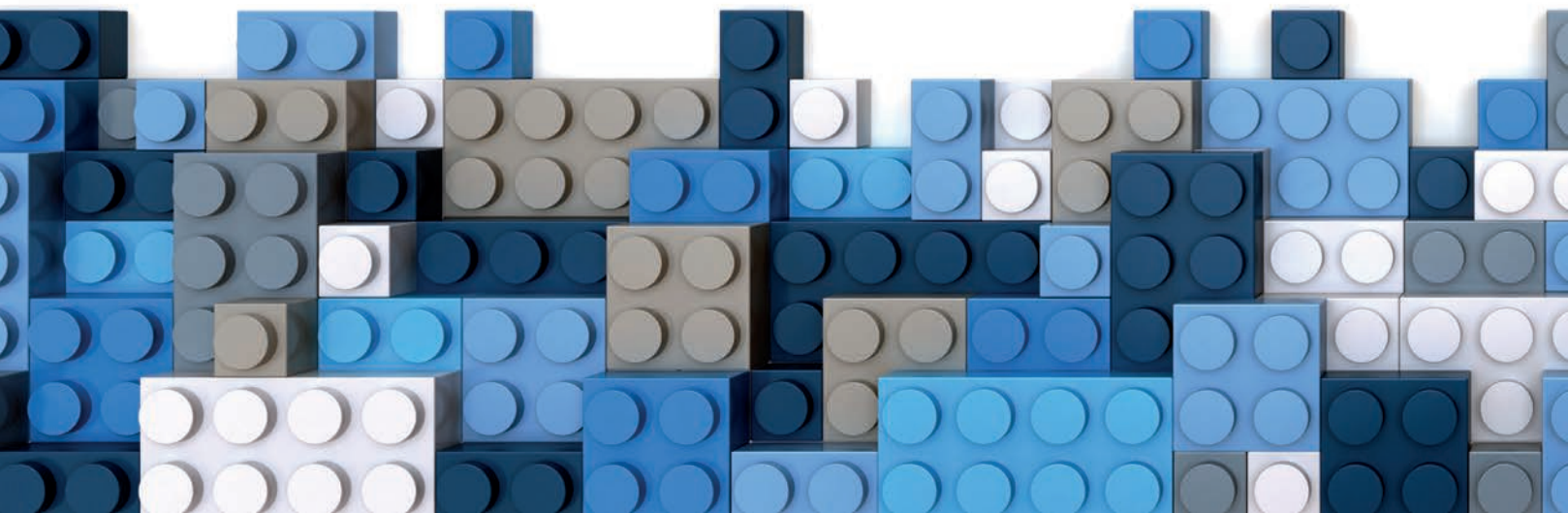
IT-Sicherheit anwenderfreundlich gestalten

Die Abteilung BL im BSI entwickelt anwenderfreundliche Sicherheitskonzepte für Bund, Länder und Kommunen

von Philipp Deuster, Referat Mindeststandards Bund, Claudia Gola, Referat Informationssicherheitsberatung Standort Sachsen, und Moritz Lechleuthner, Abteilung Beratung für Bund, Länder und Kommunen

Anwenderfreundlichkeit in der IT-Sicherheit steht spätestens seit der Cybersicherheitsstrategie für Deutschland 2021 im Fokus – auch das BSI beschäftigt sich verstärkt mit dem Thema. Denn klar ist, auch die sicherste Lösung oder das beste Konzept kann die IT-Sicherheit nur dann erhöhen, wenn Anwenderinnen und Anwender sie bzw. es nutzen. Die Abteilung Beratung für Bund, Länder und Kommunen (BL) entwickelt deshalb anwenderfreundliche präventive Anforderungen und Vorgaben für öffentliche Stellen.

Das Thema Anwenderfreundlichkeit beschäftigt das BSI seit Jahren. Auf einen Bericht über das inzwischen abgeschlossene Projekt „Neupositionierung des IT-Grundschutzes für die Bundesverwaltung“ (NIT-GSB) des Referats BL 13, Informationssicherheitsberatung Standort Sachsen, gab es große Leserresonanz. Es ging u. a. um die Förderung der Anwenderfreundlichkeit des IT-Grundschutzes im Bund. Zahlreiche Rückmeldungen aus den Bundesbehörden verdeutlichten hier den Wunsch nach mehr Unterstützung und schlicht einfacherer Anwendung. Das Referat BL 13 reagierte prompt und führt nun ausgewählte Kernpunkte aus dem NIT-GSB als eigenständige Aktivitäten fort. Sie werden über das neu gegründete „Koordinierungsgremium für die Bundesverwaltung zur Stärkung des IT-Grundschutzes“ – kurz KoBIG – gesteuert.



Zu den Maßnahmen zählen neben dem Aufbau einer Kollaborationsplattform für Informationssicherheitsbeauftragte (ISBs) die Erstellung und Bereitstellung anwenderfreundlicher Arbeitshilfen in der Form eines online abrufbaren Werkzeugkastens und die Erarbeitung von IT-Grundschutzprofilen. Ein großes Potenzial zur Entlastung der Bundesverwaltung steckt in der Automatisierung des Managementsystems für Informationssicherheit (ISMS) des Bundes und wird deshalb im Rahmen des KoBIG geprüft.

PASSGENAUE HILFESTELLUNGEN FÜR BUNDESBEHÖRDEN

Ein wichtiges Werkzeug sind die Mindeststandards Bund, die das gleichnamige BSI-Referat BL 35 seit 2014 in Abstimmung mit dem IT-Grundschutzreferat SZ 13 und den Fachreferaten des BSI koordiniert. Erstellt werden Mindestanforderungen für konkrete Anwendungsfälle im Bund unter Berücksichtigung seiner besonderen Rahmenbedingungen. Die Bundesbehörden erhalten so auf Basis des IT-Grundschutzes Vorgaben und passgenaue Hilfestellungen, um IT-Sicherheitsanforderungen in der Praxis umzusetzen. Durch umfangreiche externe und BSI-interne Abstimmungsprozesse wird sichergestellt, dass bereits veröffentlichte Regelungen berücksichtigt und bei Bedarf referenziert werden. Die Verweise auf den IT-Grundschutz werden dabei zusätzlich in einem bearbeitbaren Format zur Verfügung gestellt, das Anwendende nutzen können, um die Anforderungen in Tools zu integrieren. Mit dem NIS-2-Umsetzungsgesetz soll künftig auch die Anwendung des IT-Grundschutzes in der Bundesverwaltung verpflichtend werden. Da die Mindeststandards bereits eng an den IT-Grundschutz angelehnt sind und für die konkrete Anwendung praktische Hilfestellungen anbieten, dürfte den Bundesbehörden diese Anpassung zügig und nachhaltig gelingen. Zugleich arbeitet das BSI daran, Mindeststandards und IT-Grundschutz künftig noch besser zu verzahnen, um den Anwenderinnen und Anwendern im Bund die Umsetzung weiter zu erleichtern.

KOMPLEXE DIGITALISIERUNG ERFORDERT KOMPLEXE SICHERUNGSSYSTEME

Die ausgewählten Beispiele zeigen, wie nicht nur die Abteilung BL, sondern das gesamte BSI Anwenderfreundlichkeit in der Informationssicherheit versteht und ausgestaltet – heute und auch in Zukunft gemeinsam. Die Komplexität zunehmender Digitalisierung immer weiterer Arbeits- und Lebensbereiche macht auch vor deren Absicherung nicht halt. Als das Kompetenzzentrum für Cybersicherheit ist es daher unsere Aufgabe, Anwenderinnen und Anwender verstärkt zu unterstützen, Cyber- und Informationssicherheit wirksam umzusetzen, und dafür die Voraussetzungen in Form von anwenderfreundlichen Sicherheitsanforderungen zu schaffen. Dabei sind die ausgewählten Beispiele nur ein Ausschnitt. Während das Projekt „Weg in die Basis-Absicherung“ von BL 12 und SZ 13, das Kommunen beim Einstieg in den IT-Grundschutz unterstützt (s. Artikel auf S. 48), soll das Vorhaben einer Harmonisierung von Geheimschutzanforderungen und IT-Sicherheitsanforderungen in einem der kommenden BSI-Magazine thematisiert werden. ■

Usable Security als Qualitätsmerkmal von IT

BSI-Projekt entwickelt Grundsätze und Leitlinien nutzungsfreundlicher IT-Sicherheit aus Verbrauchersicht

von Dr. Matthias Korn und Kristina Unverricht, Referat Grundsatzfragen des Digitalen Verbraucherschutzes und Kooperationen, und Prof. Dr. Therese Mieth, Hochschule des Bundes für öffentliche Verwaltung

In einem gemeinsamen Projekt mit der Hochschule des Bundes für öffentliche Verwaltung beschäftigt sich das BSI mit dem Thema Usable Security aus Verbrauchersicht. Ziel ist es, bei der Gestaltung von Informationstechnologien Hilfestellungen zur Umsetzung von Usable Security zu geben. Im Fokus stehen dabei Gebrauchstauglichkeit, Zugänglichkeit und Barrierefreiheit, Transparenz sowie Akzeptanz. Diese vier Bereiche sind kritische Erfolgsfaktoren, wenn es darum geht, IT-Sicherheit in der praktischen Nutzung von Informationstechnologien umzusetzen.

IT-Sicherheit ist für Anwenderinnen und Anwender in der Regel kein Selbstzweck, sondern steht meist im Dienst anderer Handlungsziele. Sicherheitsmechanismen müssen daher so gestaltet sein, dass sie im Alltag gut umsetzbar und in die Lebenswelt und die Handlungsabläufe der Anwendenden integrierbar sind. So kann ein hohes Maß an praktischer IT-Sicherheit gewährleistet werden. Das ist das Ziel von Usable Security.

Usable Security ist dabei als Qualitätsmerkmal von IT-Sicherheit zu verstehen, welches durch Gebrauchstauglichkeit, Zugänglichkeit und Barrierefreiheit, Transparenz sowie ein positives Nutzungserlebnis zu mehr Akzeptanz bei den Anwendenden digitaler Technologien führt. Das wiederum erhöht die IT-Sicherheit in der Praxis.

EINFACHE BEDIENUNG IST VERBRAUCHERFREUNDLICH UND INKLUSIV

Verhältnismäßig wenige Verbraucherinnen und Verbraucher sind in der IT-Sicherheit versiert. Deshalb ist Usable Security auch ein wesentlicher Beitrag zum digitalen Verbraucherschutz. Denn viele Verbraucherinnen und Verbraucher sind im digitalen Raum auf die eine oder andere Art vulnerabel. Die Gründe für digitale Vulnerabilität sind vielfältig und können beispielsweise auf sozialen, demografischen oder körperlichen Faktoren beruhen. Um dennoch eine größtmögliche IT-Sicherheit zu erreichen, sind die Schnittstellen zu Verbraucherinnen und Verbrauchern so zu gestalten, dass Informationstechnologien ebenso wie IT-Sicherheitstechnologien im Alltag einfach zu bedienen sind.

Aufbauend auf aktuellen Forschungsergebnissen im Bereich Usable Security verfolgt das Projekt einen breiten Ansatz und betrachtet die vier Bereiche Gebrauchstauglichkeit, Zugänglichkeit und Barrierefreiheit, Transparenz sowie Akzeptanz.

Jeder einzelne der vier Bereiche kann Auswirkungen auf die IT-Sicherheit haben, beispielsweise:

- Eine geringe Fehlertoleranz von Systemen führt dazu, dass Anwendungsfehler einen direkten negativen Einfluss auf die IT-Sicherheit haben.
- Sicherheitstechnologien, die nicht barrierefrei sind, können mitunter nicht angewendet werden.
- Sicherheitsmechanismen, die für Nutzende nicht verständlich und transparent sind, können zur falschen oder fehlerhaften Verwendung führen.
- Ein generell schlechtes Nutzungserlebnis verringert die Akzeptanz von Sicherheitstechnologien und führt im schlimmsten Fall dazu, dass diese kreativ umgangen und überhaupt nicht mehr verwendet werden.

LEITFADEN FÜR ENTWICKLERINNEN UND ENTWICKLER

Im Projekt mit der Hochschule des Bundes werden die Erfolgsfaktoren für Usable Security zusammengetragen und in einem Leitfaden aufgearbeitet, der Entwicklerinnen und Entwickler bei der nutzungsfreundlichen Gestaltung von Produkten und Diensten unterstützt. Bei der Gestaltung von Standards und Spezifikationen, aber auch in Regulierungsprozessen sollen die entwickelten Leitlinien zukünftig ebenfalls unterstützen und Hilfestellung leisten. Ebenso können Kriterien für Usable Security als wichtige Erfolgskriterien bei Vergabeprozessen der öffentlichen Hand berücksichtigt werden.

Als erstes Projektergebnis wurde für das BSI ein systematischer Überblick erstellt, der die wichtigsten Fragestellungen für Usable Security aufzeigt. Hierfür wurden relevante Forschungsergebnisse sowie Standards und Spezifikationen im Bereich Usable Security ausgewertet. Die Systematik richtet sich in erster Linie an IT-Sicherheitsexpertinnen und -experten, um ihnen eine Hilfestellung bei der Adressierung von Anforderungen an Usable Security zu geben. Das Modell wird im nächsten Schritt an Beispielprojekten überprüft und weiterentwickelt, um langfristig die Entwicklung von nutzungsfreundlichen und sicheren Technologien zu fördern.

Nutzungsfreundlichkeit und IT-Sicherheit stehen nicht im Kontrast zueinander, sondern gehören zusammen. Denn eine höhere Nutzungsfreundlichkeit führt zu einer höheren IT-Sicherheit. ■

Usable Security als Qualitätsmerkmal: vier Grundprinzipien und zugehörige Richtlinien

Vorteile von „Infrastructure as Code“ in der Cloud

Die Bereitstellung, Konfiguration, Aktualisierung und Löschung von Cloud-Diensten per Code

von Jan Bings, Referat Virtualisierung und Cloud-Sicherheit

„Infrastructure as Code“ (IaC) erleichtert die Anwendung von Sicherheitsvorgaben maßgeblich: Die mithilfe von IaC erstellten Skripte können einzelne virtuelle Server bis hin zu komplexen Anwendungsszenarien bereitstellen und verwalten. So kann IaC Behörden und Unternehmen bei der sicheren Nutzung der Cloud unterstützen.

„Infrastructure as code“ (IaC) beschreibt ein Konzept, welches eine Bereitstellung von Ressourcen und der Konfigurationen dieser auf Grundlage von Skripten bzw. einem Code ermöglicht. Durch IaC können Cloud-Dienste von Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) bis zu Software-as-a-Service (SaaS) bereitgestellt, konfiguriert, aktualisiert und gelöscht werden. IaC ist kein neues Konzept und ebenfalls in On-Premises-Infrastrukturen etabliert. Ein Unterschied ist, dass bei den meisten Cloud-Anbietern die Anzahl der möglichen Ressourcen tendenziell höher ist, da Cloud-Plattformen meist virtualisierte Ressourcen bereitstellen und die Kunden nicht eigenständig Skripte zur Umsetzung von IaC erstellen müssen. Die Skripte basieren auf standardisierten Formaten wie der JavaScript Object Notation (JSON) sowie YAML Ain‘t Markup Language (YAML) und werden an die definierten API-Dienste der Cloud-Anbieter übermittelt. Der Code ist anbieterspezifisch, und es gibt unterschiedliche Pflichtparameter, sodass vor einer Übertragung zu anderen Anbietern die Skripte angepasst werden müssen.

CHANCEN DURCH IAC

Ein Vorteil des Ausbringens und der Weiterentwicklung der eigenen Infrastruktur über IaC-Skripte ist, dass viele Konfigurationen im Code enthalten sind und sich die Abhängigkeit zu manuellen Administrationen auf Basis von Expertenwissen reduziert. Beim Updaten von Skripten werden die Änderungen an den Ressourcen übersichtlich für den Administrator zusammengefasst, was unerwünschte Veränderungen wie Fehlkonfigurationen und Downtimes verhindern kann. Darüber hinaus können durch Versionierungen Rollbacks einfacher durchgeführt werden. Die Wiederverwendbarkeit wird ebenfalls erhöht und Bereitstellungsgeschwindigkeiten werden reduziert, da mit dem Skripten Umgebungen mehrfach bereitgestellt werden und sich die konfigurierten Ressourcen leichter in andere Anwendungsszenarien übertragen lassen. Durch die Möglichkeit der mehrfachen Bereitstellungen können Entwicklungsumgebungen bei Bedarf mit den Produktionsskripten ohne Inkonsistenzen aufgebaut und nach dem Testen wieder vollständig heruntergefahren werden. Die schnelle Bereitstellung der Ressourcen bei Bedarf kann zugleich Kosten für ungenutzte Ressourcen reduzieren.

Die Skripte sind vergleichbar mit traditionellen Vorgehensweisen aus den Bereichen Development und Operations (DevOps) bei der Entwicklung von Anwendungscode. Sie können ebenfalls kollaborativ und kombiniert mit Continuous-Integration-/Continuous-Delivery-Pipelines entwickelt werden.

Cloud-Anbieter stellen meistens Vorlagen für die Ressourcen in Repositorys und den zugehörigen Dokumentationen zur Verfügung, welche etablierte Härtungsmaßnahmen beinhalten. Dies vereinfacht die Entwicklung der IaC-Skripte sehr. Im Code können durch die Konfigurationsmöglichkeiten die Sicherheitsvorgaben umgesetzt werden, welche sich auch leichter überprüfen lassen, da sie in DevOps-Pipelines automatisiert gegen vordefinierte Policys getestet werden und Code-Reviews möglich sind. Neben den Skripten der Cloud-Anbieter könnten in öffentlichen Repositories weitere Skripte abgelegt werden, welche z. B. die korrespondierenden Kriterien für Kunden des Kriterienkatalogs C5 erfüllen und so die Umsetzung von Sicherheitsanforderungen bei den Anwenderinnen und Anwendern unterstützen.

VORTEILE EINER LANDING-ZONE IM KONTEXT VON IAC

Eine Landing-Zone ist ein Service in der Cloud, welcher für größere Organisationen eine Multi-Account-Struktur abbildet, sodass verschiedene Aufgaben (z. B. Entwicklung, Betrieb, Audit) mit minimalen Rechten ausgeführt werden. Innerhalb der Zonen ist es möglich, dass die Nutzerinnen und Nutzer nur vordefinierte Services und IaC-Vorlagen verwenden dürfen, was eine grundlegende Absicherung ermöglicht. Darüber hinaus können Richtlinien definiert werden, die bestimmte Konfigurationen verhindern oder bei Nichteinhaltung Alarme versenden. Nach den Vorgaben der Cloud-Anbieter sollen Landing-Zones ebenfalls mit IaC bereitgestellt werden, sodass diese nachvollziehbar und Änderungen leichter ersichtlich sind. Mit dieser Technik ergeben sich neue Möglichkeiten auch für Regulatoren, Vorgaben für betreffende Institutionen vorzugeben und skalierbar zu überprüfen. Zusammengefasst lassen sich die Vorteile von IaC durch zusätzliche Services erweitern und auch hier können Skripte bei der sicheren Bereitstellung unterstützen. IaC kann zusammengefasst Behörden und Unternehmen bei der sicheren Nutzung der Cloud unterstützen, da durch den codebasierten Ansatz Sicherheitskonfigurationen leicht überprüfbar sind und Fehlerkonfigurationen verhindert werden. ■

Weitere Informationen zum Kriterienkatalog Cloud Computing C5:

https://www.bsi.bund.de/dok/7685384

Unendliche Weiten – und warum sie globale Regeln brauchen

Cybersicherheit für Weltrauminfrastrukturen kann nur gemeinsam funktionieren

von Frank Christophori und Dr. Johanna Niecknig, Referat Sichere IT-Systeme für Luft- und Raumfahrt

Satelliten dominieren die digitale Vernetzung von Gesellschaft, Wirtschaft und Staaten weltweit. Maritime oder luftgestützte Anwendungen bei Interkontinentalflügen basieren ausschließlich auf satellitengestützten Diensten zur Navigation und Kommunikation. Auch globale Klimaforschung oder Aufklärung sind ohne Satelliten nicht vorstellbar. Da in der Regel mehrere Nationen eingebunden sind, kann Cybersicherheit für Weltraumsysteme nur mit grenzüberschreitenden Ansätzen gelingen.

Die Abhängigkeiten von weltraumgestützten Systemen steigen weiterhin rasant. Im Kontext New Space, der Kommerzialisierung der Raumfahrt, explodiert die Anzahl an Objekten (insbesondere im Low-Earth-Orbit) und der sich engagierenden Stakeholder. Damit erhöht sich aber auch die Gefahr von Cyberangriffen auf Satellitensysteme extrem – zumal mit überschaubarem Aufwand großer Schaden angerichtet werden kann. Gleichzeitig ist im Cyberraum eine Attribuierung der Angreifer schwer oder gar nicht möglich. Daher sind spezifische Cybersicherheitsstandards dringend erforderlich.

BSI ENTWICKELT RICHTLINIEN FÜR DEN WELTRAUM

Auch die Industrie drängt auf transparente und allgemeingültige Vorgaben, daher hat das BSI gemeinsam mit der Industrie und Forschungseinrichtungen nationale Anforderungen erarbeitet. Diese sind in einem IT-Grundschutz-Profil und einer Technischen Richtlinie für Weltraumsysteme veröffentlicht worden. Die Ergebnisse werden nun in internationalen Gremien eingebracht.

Zum einen geschieht dies projektspezifisch, z. B. im Kontext des Weltraumprogramms Secure Connectivity (IRIS²). Hier unterstützt das BSI die Europäische Kommission in Abstimmung mit anderen europäischen Staaten bei allen Belangen der Informationssicherheit. Der Umfang an Sicherheitsanforderungen hat direkte oder indirekte Auswirkungen auf Hersteller, Betreiber und Nutzende. Ziel ist deshalb ein für Nutzende, Betreiber und Hersteller gut umsetzbares Sicherheitsniveau für das gesamte System.

Zum anderen gilt es, international abgestimmte Mindestsicherheitsanforderungen in Form von Standards oder Regulierungen zu etablieren. Die Koordinierung der nationalen Standardisierungsaktivitäten ist eine Aufgabe des im Herbst 2023 ins Leben gerufenen Expertenkreises Informationssicherheit Weltraum der Allianz für Cyber-Sicherheit.

ein Wettbewerbsnachteil auf dem internationalen Markt, da zu erfüllende Auflagen mit höheren Kosten einhergehen. Es muss gewährleistet sein, dass derartige verpflichtende Anforderungen für alle Stakeholder gleichermaßen gelten.

SATELLITENSYSTEME ALS KRITISCHE INFRASTRUKTUR

Essenziell in diesem Zusammenhang ist die Frage, inwieweit Satellitensysteme kritische Infrastrukturen gemäß KRITIS-Verordnung sind oder werden. Mit der Umsetzung der europäischen Richtlinie Network and Information Security Directive 2 (NIS2) wird der Weltraum zwar als eigener kritischer Sektor betrachtet, jedoch mit Beschränkung auf das Bodensegment. Weiterhin werden lediglich Betreiber von den in der NIS2 oder KRITIS-Verordnung genannten Segmenten verpflichtet, dedizierte Maßnahmen für die Sicherheit umzusetzen, und dem BSI als zuständige Behörde die geforderten Nachweise vorzulegen. Somit wird die Phase der Entwicklung und des Baus der Satelliten ausgeblendet. Offen bleibt also, wie man mit den Systemen im Orbit umgeht. Im internationalen Raum ist hier oftmals die Rede von Satelliten als National Critical Functions (NCF), da sie einen kritischen Beitrag zu den definierten KRITIS-Sektoren, insbesondere für deren Verfügbarkeiten leisten. Im Gegensatz zu einer kritischen Infrastruktur besteht bei einer NCF jedoch keine konkrete gesetzliche Grundlage.

Zu den Themen Standardisierung, Regulierung, KRITIS versus NCF, IRIS² kooperiert das BSI derzeit mit verschiedenen Partnern weltweit und nimmt hierbei eine führende Rolle ein. Die Koordinierung der Aktivitäten im BSI ermöglicht es, Synergien zwischen Staat, Wirtschaft und Forschung einerseits und internationalen Partnern andererseits zu nutzen – mit dem Ziel, gemeinsam das Thema Cybersicherheit für Weltraumsysteme zu gestalten und weltweit Maßnahmen umzusetzen. ■

EXPERTENKREIS ARBEITET AN STANDARDS

Der Expertenkreis, eine Kooperation zwischen der Allianz für Cyber-Sicherheit, Behörden, der Industrie und Forschungseinrichtungen, bündelt verschiedene Aktivitäten mit dem Ziel, ein angemessenes Cybersicherheitsniveau in Weltraumsystemen zu definieren. Neben der Weiterentwicklung von Anforderungsdokumenten und deren Vermarktung im internationalen Kontext (internationale Standardisierung, Gremien zu europäischen Raumfahrtprojekten) werden aktuelle Trends und Entwicklungen mit Cybersicherheitsrelevanz in der Raumfahrt, insbesondere New Space, mitgeplottet und bewertet. Auch zum Thema Regulierung wird sich eine Projektgruppe herausbilden. Aus Sicht des BSI ist eine Regulierung mit verbindlichen Informationssicherheitsvorgaben dringend erforderlich. Regulierung funktioniert aber nur mit einem internationalen Ansatz. Eine rein nationale Regulierung wäre

Weitere Informationen:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/IT-Sicherheit-in-Luft-und-Raumfahrt/it-sicherheit-in-luft-und-raumfahrt_node.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Weltrauminfrastrukturen.html?nn=129136

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03184/TR-03184_node.html

Im Fokus: Vertrauensvolle Zusammenarbeit

Die Vorsitzenden des ENISA-Verwaltungsrates im Gespräch

Die European Union Agency for Cybersecurity (ENISA) wurde gegründet, um ein hohes gemeinsames Maß an Cybersicherheit der EU-Staaten zu gewährleisten. Die strategische Ausrichtung und die Prioritäten der ENISA werden vom Verwaltungsrat festgelegt. Im Herbst 2023 übernahm BSI-Fachbereichsleiterin Fabienne Tegeler den Vorsitz des Verwaltungsrates von Jean-Baptiste Demaison aus Frankreich. Im Interview sprechen die beiden über Herausforderungen der ENISA und neue Ziele.

Was sind die größten Herausforderungen für ENISA?
Jean-Baptiste Demaison: Angesichts der konstant angespannten Bedrohungslage im Cyberraum bleibt die größte Herausforderung für die ENISA die Förderung und Angleichung des Cybersicherheitsniveaus in der Europäischen Union, um auf den nächsten großen Cybervorfall in Europa vorbereitet zu sein. Dies geschieht sowohl durch die weitere Unterstützung der Mitgliedstaaten bei der Entwicklung ihrer nationalen Fähigkeiten als auch durch die Förderung einer effizienten zwischenstaatlichen Koordinierung.

Fabienne Tegeler: Wir stehen vor einer wachsenden Zahl an Aufgaben für die ENISA, verbunden mit zunehmenden Bedrohungen und Herausforderungen im Cyberraum und weiteren Gesetzgebungen auf europäischer Ebene. Wir müssen dafür sorgen, dass das Profil der ENISA als EU-Agentur für Cybersicherheit klar bleibt.

Welche Rolle spielt hier der Verwaltungsrat?
Demaison: Der Verwaltungsrat legt die strategische Ausrichtung und Prioritäten der ENISA fest und stellt sicher, dass die ENISA ihre Geschäfte im Einklang mit ihrem Mandat und der EU-Gesetzgebung ausführt. Aber darüber hinaus ist der Verwaltungsrat auch eine Gemeinschaft von Führungskräften im Bereich der Cybersicherheit aus den Mitgliedstaaten, die dazu beitragen, das Vertrauen untereinander zu stärken und gemeinsame Ansichten zu fördern.

Herr Demaison, was waren Ihre größten Erfolgsmomente als Vorsitzender des Verwaltungsrates?
Demaison: Mir ging es darum, den Verwaltungsrat zu einem effizienteren strategischen Führungsgremium zu machen, z. B. durch die Einführung der strategischen Sitzungen. Zweitens habe ich darauf hingearbeitet, die Agentur zu einer hochmodernen Plattform für Cybersicherheitsexpertise in all ihren Dimensionen zu entwickeln, wobei die Fähigkeiten und das Wissen der Mitgliedstaaten genutzt werden und die ENISA bei der Entwicklung und Umsetzung der Cybersicherheitspolitik der EU stärker in den Mittelpunkt rückt.

Frau Tegeler, was sind Ihre Ziele als Vorsitzende des Verwaltungsrates?
Tegeler: Es freut mich sehr, dass das BSI bzw. Deutschland erstmals diese Rolle übernimmt. Ich möchte aktiv zu einer besseren Abstimmung und Integration der Gremien auf europäischer Ebene beitragen, die sich mit Cybersicherheit befassen. Wichtig ist mir auch, die gute und konstruktive Diskussionskultur fortzuführen, in der jede Stimme zählt, egal, wie groß ein Mitgliedstaat ist. Im kommenden Jahr wird die Evaluierung des Cyber Security Act/ENISA-Mandats eine wichtige Aufgabe für mich und meinen Stellvertreter Stefan Lee sein.

Wie arbeitet das BSI mit der ENISA zusammen?
Tegeler: Kolleginnen und Kollegen des BSI beteiligen sich in Arbeitsgruppen der ENISA, unterstützen durch Beiträge zu Studien, Konferenzen, Fachpublikationen u. v. m. Wir schätzen die Rolle des National Liaison Officers als zentralem SPOC sehr, um als Multiplikator der ENISA ins BSI zu wirken und umgekehrt. Außerdem entsendet das BSI regelmäßig Mitarbeitende an die ENISA, derzeit sind Kolleginnen und Kollegen im ENISA-Stab und im operativen Bereich tätig, dies fördert Vertrauen und Austausch.

Wie arbeitet ANSSI mit der ENISA zusammen?
Demaison: ANSSI hat sich stets intensiv an den Arbeitsgruppen und Initiativen der ENISA beteiligt und wird dies auch in Zukunft tun. Aus meiner Sicht sollte das Netzwerk der National Liaison Officers in Zukunft noch gestärkt werden. Es könnte eine noch zentralere Rolle bei der Unterstützung der Koordination zwischen den Mitgliedstaaten spielen, um Expertise europaweit zu teilen.

Krzysztof Silicki (scheidender Vize-Chair, PL), Stefan Lee (neuer Vize-Chair, FI), Juhan Lepassaar (Exekutivdirektor der ENISA), Fabienne Tegeler, Jean-Baptiste Demaison am Tag der Wahl des neuen Vorsitzes des ENISA-Verwaltungsrates im Hauptsitz der ENISA in Athen

Jean-Baptiste Demaison ist Leiter des öffentlichen Innovationslabors und des Inkubators für digitale Dienste (FR) bei der französischen Agence nationale de la sécurité des systèmes d'information (ANSSI). Von 2016 bis 2023 war er Vorsitzender des ENISA-Verwaltungsrates.

Fabienne Tegeler ist Leiterin des Fachbereichs Kundenmanagement und Recht im BSI und wurde im Juni 2023 zur neuen Vorsitzenden des ENISA-Verwaltungsrates gewählt.

Wenn man das Verhältnis zwischen Deutschland und ENISA auf die nationale Ebene spiegelt, welche Parallelen sehen Sie?
Tegeler: Ich sehe hier Parallelen. Es braucht koordinierende Einheiten auf allen staatlichen Ebenen, um Zusammenarbeit zu fördern. Die ENISA trägt durch ihre Arbeit maßgeblich zur Angleichung des IT-Sicherheitsniveaus in der EU bei und respektiert dabei aber auch die Unterschiede zwischen den 27 Mitgliedstaaten. Ganz ähnlich ist die Idee zur Einrichtung einer Zentralstellenfunktion im Bund-Länder-Verhältnis beim BSI auf nationaler Ebene: Wir wollen stärker zusammenarbeiten, Doppelarbeiten vermeiden sowie bürokratische und rechtliche Hürden abbauen. Weder auf europäischer noch auf nationaler Ebene geht es darum, die Kompetenzen für die Fachaufgabe IT-Sicherheit auf die nächsthöhere staatliche Ebene zu verlagern.

Welche Rolle sollte ENISA künftig in der EU spielen?
Tegeler: Die ENISA hat eine Schlüsselrolle, wenn es darum geht, die Cybersicherheit der Union zu stärken. Diese Rolle sollte durch eine angemessene Ressourcenausstattung und die Zusammenarbeit mit allen relevanten Partnern weiter gestärkt werden. ■

Der Blick über den großen Teich

Wir müssen das Thema Cybersicherheit prominent auf die Agenda heben

Claudia Plattner, BSI-Präsidentin, über ihre USA-Reise nach Washington, D.C., und San Francisco

Anfang September ging es für das BSI für eine Woche in die USA. Im Gepäck jede Menge Themen: Standards harmonisieren, lebhaftes Ökosystem für digitale Produkte etablieren, Cybersicherheitsagenda besprechen, besseres Lagebild entwickeln, Auswirkungen des CRA erörtern und die Frage, wie heben wir Cybersicherheit prominent auf die Agenda?

Meine Terminserie startete am Montagabend mit dem Industry Dinner der Internet Security Alliance (ISA). Dort hatte ich die Gelegenheit, Larry Clinton, dem Leiter der ISA, für die gute Kooperation beim international erscheinenden Handbuch „Management von Cyber-Risiken" zu danken. Zudem haben wir das Dinner genutzt, um das Thema Cybersicherheit bei der Wirtschaft zu verankern.

Dienstagmorgen ging es bei einem Besuch der Deutschen Botschaft u. a. um die im März veröffentlichte US-Cybersicherheitsstrategie. Sie ist beneidenswert konkret. Reinschauen lohnt sich. Es ist z. B. geregelt, dass ein US-IT-Sicherheitskennzeichen initiiert werden soll. Umsetzen wird das die Federal Communications Commission (FCC), sodass Ende 2024 die ersten Kennzeichen vergeben werden können. Unser Ziel ist es – ähnlich wie mit unserem Abkommen mit Singapur –, eine Harmonisierung mit unserem IT-SiK zu erreichen. Mit diesen Kennzeichen für IT-Produkte bieten wir einerseits den Nutzerinnen und Nutzern ein Entscheidungskriterium beim Kauf – Sicherheit auf einen Blick – und andererseits führt es zu einem klaren Wettbewerbsvorteil auf Herstellerseite. Klassische Win-win-Situation.

Später am Vormittag traf ich Jen Easterly, Leiterin der Cybersecurity and Infrastructure Security Agency (CISA). Eine schillernde Persönlichkeit: Sie ist Rubix-Cube-Fanatikerin, hat Abschlüsse von West Point, Master in Philosophie, Politik und Ökonomie der University of Oxford und war 20 Jahre in der US Army. Inhaltlich haben wir u. a. über die US-Cybersicherheitsstrategie gesprochen. Die CISA übernimmt einige Aspekte des im Juli veröffentlichten Umsetzungsplans zur Strategie. Ein Punkt daraus: Das Teilen von Informationen zwischen den sektorspezifischen Aufsichtsbehörden verbessern.

Am Nachmittag ging es weiter ins Weiße Haus zu Kemba Walden, der amtierenden National Cyber Director der USA. Wir haben u. a. über die 69 „high-impact"-Initiativen des Umsetzungsplans der US-Cybersicherheitsstrategie gesprochen, mit denen u. a. die Hauptforderung nach einer engen Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor erreicht werden sollen.

Aus diesen Treffen habe ich zwei entscheidende Fakten für mich mitgenommen, die wichtig sind, um das Thema Cybersicherheit nach vorne zu bringen: Zum einen braucht es Menschen wie Jen und Kemba, die begeistern können und authentisch handeln. Zum anderen ist der offene und transparente Austausch entscheidend.

Gleich am Mittwochmorgen traf ich Jim Lewis, den Senior Vice President and Pritzker Chair vom Center for Strategic and International Studies (CSIS). Eine Erkenntnis: Die Kooperation zwischen Staat und privatem Sektor wird sich verändern müssen. Wir brauchen speziell zugeschnittene Hilfs- und Informationsangebote, um Cybersicherheit bedarfsgerecht zu verankern.

Im Rahmen des Bellington Summits spürte ich immer wieder viele Sympathien für Deutschland. So plant der Organisator der Konferenz, Tom Billington, eine Deutschlandreise. Eine Gelegenheit für uns, ihm vor Ort Einblicke in unsere Arbeit zu geben. Auch er offenbarte sich als Botschafter für das Thema Cybersicherheit. Auf dem Panel haben wir Wege diskutiert, wie einzelne Länder mit Cybersicherheitsprogrammen ihre Cyberabwehr aufbauen können. Mein Favorit: Politik, Wirtschaft und Wissenschaft müssen gemeinsam ein Umfeld schaffen, in dem modernste Technologien für Cybersicherheit sorgen können.

Donnerstag traf ich Paul Nakasone, Direktor der NSA, und sein Team. Dort habe ich einen Blick in das Cybersecurity Operations Center geworfen und konnte erleben, wie sie mit anderen Cybersicherheitsforen zusammenarbeiten. Bei einem Round Table mit Analystinnen und Analysten konnte ich u. a. unsere Kooperation bei Kryptologie und Zertifizierung herausstellen. Transparenter Austausch ist für mich das A und O für eine umfassende Lagebeobachtung.

Bevor es zurück nach Hause ging, noch ein Abstecher nach San Francisco: Wir haben mit dem Deutschen Wissenschafts- und Innovationshaus den Startschuss für die gemeinsame Projektarbeit gegeben. Zusammen mit Wissenschaft, Wirtschaft und dem öffentlichen Sektor wollen wir hier die Chancen nutzen, die sich beispielsweise durch KI ergeben. So können wir Forschung und Innovation zielgerichtet fördern. ■

Retrospektiv ist bei mir hängen geblieben, wie „vibrant“ das Cyberökosystem in den USA ist. Mir liegt daher am Herzen, auch in Deutschland ein ähnlich lebhaftes Ökosystem zu schaffen, in dem

- Produkte so nutzerfreundlich sind, dass Verwaltung, Wirtschaft und Gesellschaft sie auch wirklich nutzen,
- bedarfs- und anwendergerechte Hilfs- und Informationsangebote bestehen und
- ein transparenter Austausch der einzelnen Player die Grundlage für Cybersicherheit bildet.

Europäischer Austausch für mehr Cybersicherheit in der digitalen Verwaltung

Beim VIS!T-Symposium der Cybersicherheitsbehörden in Luxemburg informierte das BSI über sichere digitale Verwaltungsabläufe

von Clarissa Wilkie, Referat Internationale Beziehungen

Unter dem Motto „Digitale Verwaltung, aber bitte nicht ohne Cybersicherheit" tauschten sich Expertinnen und Experten der Cybersicherheitsbehörden sowie der öffentlichen Verwaltungen aus fünf Ländern aus. Das BSI war mit mehreren Beiträgen vertreten und berichtete über seine Erfahrungen und Erkenntnisse zum IT-Grundschutz, zu Clouds in Verwaltungen und europäischer Zusammenarbeit.

Alle zwei Jahre laden die Cybersicherheitsbehörden aus Deutschland, Österreich, der Schweiz und Luxemburg Entscheidungsträgerinnen und -träger sowie IT-Spezialistinnen und -Spezialisten aus öffentlichen Verwaltungen zum Austausch und zur Vernetzung ein. Erstmals war 2023 auch das Fürstentum Liechtenstein dabei. Das BSI beteiligte sich u. a. mit Beiträgen zum IT-Grundschutz, zum sicheren Einsatz von Clouds in den Verwaltungen sowie zur ebenenübergreifenden Zusammenarbeit in Deutschland und Europa.

IT-GRUNDSCHUTZ IN DER BUNDESVERWALTUNG

Dr. Astrid Schumacher, Leiterin des Fachbereichs Informationssicherheitsberatung und Geheimschutz beim BSI, stellte vor, welche neuen Wege zur pragmatischen Umsetzung des IT-Grundschutzes (IT-GS) in der Verwaltung das BSI gemeinsam mit der Bundesverwaltung beschreitet. Sie ging auf die für das Gelingen zwingend notwendigen Geschäftsprozesse zur effizienten Bewältigung des Ansatzes „Plan – Do – Check – Act" ein und betonte, wie unabdingbar Leitungsverantwortung im Rahmen eines ganzheitlichen Risikomanagements sei. Oftmals bleibe die Anwendung des IT-Grundschutz aufgrund des relativ hohen Aufwands auf dem Weg zum Ziel stecken. Der Fachkräftemangel und eine quantitativ unzureichende Stellenplanung seien zwei der identifizierten Stolpersteine. Bei zunehmender Komplexität der IT steige gleichzeitig der Handlungsdruck angesichts der hohen Gefährdungslage. Das BSI habe sich daher zum Ziel gesetzt, Hürden im Umgang mit Informationssicherheit für Verwaltungen sukzessive weiter abzubauen, um den Kosten-Nutzen-Aufwand für die Anwenderinnen und Anwender zu optimieren.

AUSTAUSCH UND WISSENSTRANSFER

Als einen der Lösungsansätze stellte Dr. Astrid Schumacher das Projekt „Neupositionierung des IT-GS in der Bundesverwaltung (NIT-GSB)" vor (s. Artikel auf S. 50). Ergänzt wird dies durch Maßnahmen für mehr Austausch und Wissenstransfer zwischen den Anwenderinnen und Anwendern. Zusätzliche Angebote der Weiterbildung sollen Hürden im Umgang mit Informationssicherheit minimieren.

In diesem Zusammenhang sind Plattformen wie das sich im Aufbau befindliche Netzwerk für das Informatiksteuerorgan des Bundes (ISB) oder das kommunale IT-SiBe-Forum zu nennen. Im BSI-Projekt „Neue Wege in die Basis-Absicherung" (s. Artikel auf S. 48) wird ein deutlich abgespecktes Einstiegslevel für den IT-Grundschutz entwickelt, um insbesondere sehr kleinen Institutionen die Realisierung der minimal notwendigsten Sicherheitsmaßnahmen zu erleichtern.

Der auf die Bedürfnisse der Anwenderinnen und Anwender ausgerichtete IT-Grundschutz ist somit weiterhin das richtige Werkzeug, um Informationssicherheitsmanagement einfach und effizient zu betreiben.

ZUSAMMENARBEIT IN DEUTSCHLAND UND EUROPA – AUF ALLEN EBENEN

Horst Samsel, BSI-Abteilungsleiter Beratung für Bund, Länder und Kommunen, betonte in seinem Vortrag zur ebenenübergreifenden Zusammenarbeit in Deutschland und Europa, dass Cybersicherheit in besonderem Maße ein Querschnittsthema sei und gleichermaßen Staat, Wirtschaft und Gesellschaft betreffe.

BSI-Expertinnen und Experten auf dem VIS!T-Symposium. *Oben links, zweite Person von links: Thomas Biere, Referatsleiter Informationssicherheitsberatung für den Bund und Grundsatz; oben rechts: Horst Samsel, Abteilungsleiter Beratung für Bund, Länder und Kommunen; unten links: Dr. Astrid Schumacher, Fachbereichsleiterin Informationssicherheitsberatung und Geheimschutz; unten rechts: Dr. Clemens Doubrava, Referatsleiter Virtualisierung und Cloud-Sicherheit*

Cybersicherheit ziehe sich horizontal durch alle politischen Themenfelder, wie z. B. Verkehr, Gesundheitswesen, Verwaltungsdigitalisierung und Telekommunikation. Um Cybersicherheit effektiv und effizient zu realisieren, komme es deshalb darauf an, Cybersicherheit als horizontales Querschnittsthema zu realisieren. Dem trage das BSI als ressortübergreifende Querschnittsbehörde bereits Rechnung. In föderalen Staaten wie Deutschland komme aber noch eine vertikale Ebene dazu, da hier den Bundesländern die öffentliche Verwaltung weitgehend obliegt. Cybersicherheit im föderalen Staat sei also zugleich eine horizontale und vertikale Querschnittsaufgabe.

GRUNDGESETZÄNDERUNG WIRD DISKUTIERT

Die Bundesregierung arbeitet derzeit daran, Grundlagen für die ebenenübergreifende Zusammenarbeit zu schaffen. Diskutiert wird eine Grundgesetzänderung mit dem Ziel, dem BSI eine koordinierende Rolle zuzuweisen und die rechtliche Grundlage zu schaffen, um die Bundesländer zu unterstützen.

Horst Samsel verwies auch auf die europäische Ebene. Mit horizontaler und vertikaler Regulierung der EU in den vergangenen Jahren und der Einrichtung der „Agentur der Europäischen Union für Cybersicherheit“ (ENISA) sei Cybersicherheit auch hier zu einem wichtigen Thema geworden. Auch das sei unerlässlich, stelle aber zugleich eine weitere Herausforderung dar.

Durch koordinierte und vertrauensvolle Zusammenarbeit könne es den Akteuren im Bereich der Cybersicherheit gelingen, mit dieser Komplexität umzugehen. Dazu gehöre insbesondere der intensive Austausch untereinander, gerade in Formaten wie dem VIS!T-Symposium.

FAZIT UND AUSBLICK

Das diesjährige Symposium bot den Teilnehmenden des BSI erneut die Möglichkeit, sich mit ihren Counterparts in den deutschsprachigen Ländern auszutauschen und aktuelle Entwicklungen zu diskutieren. Gerade im Licht der Zeitenwende ist dies wichtig, da so die Zusammenarbeit der Cybersicherheitsbehörden gestärkt wird. Insgesamt bleibt das VIS!T-Symposium ein wertvolles Format, denn es ermöglicht ein gegenseitiges Lernen im deutschsprachigen Raum sowie einen Austausch zu Best Practices und Kooperationsmöglichkeiten. Das nächste VIS!T-Symposium wird 2025 in Österreich stattfinden. ■

Eine Erfolgsgeschichte mit Potenzial

Das 2022 eingeführte IT-Sicherheitskennzeichen schafft Transparenz für Verbraucherinnen und Verbraucher. Im Interview spricht Sandro Amendola, BSI-Abteilungsleiter Standardisierung, Zertifizierung und Sicherheit von Telekommunikationsnetzen, über Meilensteine und Zukunftspläne.

Im Februar 2022 wurde das erste IT-Sicherheitskennzeichen für ein Produkt vergeben: Ist das IT-Sicherheitskennzeichen (IT-SiK) ein Erfolgsmodell?

Sandro Amendola: Das freiwillige IT-Sicherheitskennzeichen wurde eingeführt, um die Sicherheit von IT-Produkten transparenter und verständlicher für Verbraucherinnen und Verbraucher darzustellen. Dabei war von Beginn an klar, dass IT-Sicherheit nichts Statisches ist. Wir haben es geschafft, eine dynamische Komponente in das Kennzeichen zu integrieren, wodurch es sich von den meisten anderen Produktkennzeichen unterscheidet. Durch Scannen eines QR-Codes erhalten Konsumentinnen und Konsumenten Zugang zu aufbereiteten Sicherheitsinformationen, die bei Bedarf aktualisiert werden können. Das ist bei IT-Produkten besonders wichtig, da sich ihre Sicherheitsmerkmale im Laufe der Zeit verändern können. Deshalb prüfen wir die Produkte und Dienste auch über die Laufzeit durch die BSI-Marktaufsicht und nicht zu einem einzigen Zeitpunkt bei der Erteilung. Diese Prüfung läuft dann anlasslos, z. B. stichprobenartig oder anlassbezogen z. B. bei Bekanntwerden von Schwachstellen.

Für mich ist das IT-Sicherheitskennzeichen daher ein Erfolg. Darin fühle ich mich auch durch den positiven Zuspruch von Wirtschafts- und Verbraucherschutzverbänden und die Erfahrungen der bisherigen Kennzeicheninhaber bestätigt. Wichtig ist mir aber, dass wir uns auf dem Erfolg nicht ausruhen und das Kennzeichen kontinuierlich weiterentwickeln, damit es auch in Zukunft richtungsweisend ist.

Was sind aus Ihrer Sicht die wichtigsten Meilensteine, die das IT-SiK bislang genommen hat?

Amendola: Der erste Meilenstein war natürlich das erste erteilte Kennzeichen. Der Antrag kam wenige Tage nach der Einführung. Die Übergabe hat dann im Rahmen des 18. Deutschen IT-Sicherheitskongresses im Februar 2022 stattgefunden.

Ebenso bedeutend war für uns die Einführung der Produktkategorie „Smarte Verbrauchergeräte“ Ende 2022, durch die es uns gelungen ist, das IT-Sicherheitskennzeichen für eine Vielzahl von Produkten anzubieten. Seitdem kann für viele unterschiedliche vernetzte IoT-Geräte ein IT-Sicherheitskennzeichen beantragt werden. Das Kennzeichen hat es aber auch schon auf die internationale Bühne geschafft, so konnten wir im Oktober 2022 ein gegenseitiges Anerkennungsabkommen mit Singapur schließen. Das bestätigt die Bedeutung des IT-Sicherheitskennzeichens als Blaupause bei der Gestaltung europäischer und internationaler Kennzeichnungen.

Ein besonderes Highlight in diesem Jahr war der Messestand zum IT-Sicherheitskennzeichen auf der IFA, der weltgrößten Messe für Unterhaltungselektronik und Haushaltsgeräte. Hier haben wir das Interesse von Herstellern geweckt und viel Zuspruch von Verbraucherinnen und Verbrauchern bekommen.

Seit Oktober können interessierte Hersteller das IT-Sicherheitskennzeichen digital über das Portal zum Onlinezugangsgesetz des Bundes beantragen. Damit vereinfachen wir den Verwaltungsprozess noch weiter und ermöglichen eine medienbruchfreie Kommunikation im Antragsprozess.

Oben links: Ausstellung von gekennzeichneten Produkten am BSI-Stand auf der IFA 2023. | Oben rechts: Übergabe des IT-Sicherheitskennzeichens für das erste Gerät aus der Produktkategorie „Smarte Verbrauchergeräte“.

Unten links: Abbildung aus der Werbekampagne zum IT-Sicherheitskennzeichen für Verbraucherinnen und Verbraucher. | Unten rechts: Das IT-Sicherheitskenn-zeichen kann digital über das OZG-Portal des Bundes beantragt werden.

Welches Feedback erhalten Sie von Herstellern sowie von Verbraucherinnen und Verbrauchern?

Amendola: Wir haben positive Rückmeldungen von Wirtschafts- und Verbraucherschutzverbänden bekommen. Das bestätigt uns darin, dass das IT-Sicherheitskennzeichen einerseits für Hersteller attraktiv ist und andererseits als Mehrwert für Verbraucherinnen und Verbraucher empfunden wird. Auf der IFA haben wir viel Lob von Verbraucherinnen und Verbrauchern erhalten. Die meisten waren überrascht, dass es so ein Kennzeichen bisher nicht gab, und wünschen sich eine größere Verbreitung. Konsumentinnen und Konsumenten finden besonders die Transparenz zum Thema IT-Sicherheit gut und begrüßen, dass eine Marktaufsicht die Produkte über die Laufzeit prüft. Sie schätzen die leicht verständlichen und aktuellen Inhalte auf der dynamischen Produktinformationsseite.

„Auf der IFA haben wir viel Lob von Verbraucherinnen und Verbrauchern erhalten. Die meisten waren überrascht, dass es so ein Kennzeichen bisher nicht gab, und wünschen sich eine größere Verbreitung.“

Auch Hersteller und Dienstanbieter, die ihre Produkte bereits gekennzeichnet haben, berichten uns von positivem Feedback aus dem Kreis ihrer Kundinnen und Kunden und können positive Effekte auf die Kauf- und Nutzungsentscheidung feststellen. IT-Sicherheit wird damit immer mehr zum Kaufargument, sodass Verbrauchende und Hersteller gleichermaßen von einer freiwilligen Produktkennzeichnung profitieren.

Um das IT-Sicherheitskennzeichen in der Gesellschaft noch bekannter zu machen, haben wir im Herbst eine bundesweite Werbekampagne gestartet. Damit wird das Thema insbesondere Verbraucherinnen und Verbrauchern ins Bewusstsein gerufen, aber natürlich werden dadurch auch die bereits gekennzeichneten Produkte in den Fokus gesetzt.

Was sind die Ziele und Schwerpunkte für das IT-Sicherheitskennzeichen im kommenden Jahr?

Amendola: 2024 ist für uns besonders spannend, denn die erste Evaluation des IT-Sicherheitskennzeichens steht an. Dabei prüfen wir unter Beteiligung von Stakeholdern aus Staat, Wirtschaft und Gesellschaft, wie sich das Kennzeichen bewährt hat und wie wir es in Zukunft noch besser machen können. Dabei befassen wir uns auch mit den Standards, die wir für das Kennzeichen ausgewählt haben, und stellen das Labeldesign auf den Prüfstand. Wir beobachten natürlich auch die Entwicklungen, die sich mit dem europäischen Cyber Resilience Act abzeichnen, einer horizontalen Regulierung in Form eines CE-Kennzeichens für IT-Produkte. Da möchten wir, dass das IT-Sicherheitskennzeichen eine gute Vorbereitung ist und auch nach der Einführung eines CE-Kennzeichens einen besonderen funktionellen Mehrwert für Verbraucherinnen und Verbraucher sowie Hersteller bietet. Zwar sind wir in diesem Bereich heute schon gut aufgestellt, möchten ihn aber noch weiter ausbauen.

Hersteller wünschen sich von uns auch immer wieder ein freiwilliges Kennzeichen für den B2B-Bereich und eine Mehrstufigkeit. Ob das möglich ist, prüfen wir auch im Rahmen der Evaluierung. Unabhängig davon werden wir die Anwendungsbereiche für das IT-Sicherheitskennzeichen weiter ausbauen, derzeit sind drei neue Produktkategorien mit hoher Alltagsrelevanz in Entwicklung. International möchten wir mehr gegenseitige Anerkennungsvereinbarungen abschließen, wir sind bereits im Gespräch mit anderen Nationen, die ähnliche Kennzeichen einführen wollen. ■

Verbraucherperspektiven (er)kennen

Evaluationen für eine zielgerichtete Kommunikation im digitalen Verbraucherschutz nutzen

von Hanna Heuer, Referat Cyber-Sicherheit für Gesellschaft und Bürger

Wie bewerten Verbraucherinnen und Verbraucher Informationen zum Thema Cybersicherheit? Wie schützen sie ihre IT und ihre Daten, welche Erfahrungen haben sie schon mit Cyberkriminalität gemacht? Diesen Fragen wurde 2023 im BSI nachgegangen – zum einen mit dem Projekt LEIA, in dem Nutzerstudien zu BSI-eigenen Verbraucherinformationen im Fokus standen, zum anderen durch die repräsentative Bürgerbefragung „CyMon – der Cybersicherheitsmonitor" gemeinsam mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK).

Als herstellerunabhängige und kompetente technische Stelle unterstützt das BSI Verbraucherinnen und Verbraucher bei der Risikobewertung von Technologien, Produkten, Dienstleistungen und Medienangeboten. Neben einem besseren Schutz der/des Einzelnen wird damit gleichzeitig die gesellschaftliche Widerstandsfähigkeit gegen Cyberrisiken jeglicher Art erhöht. Dieses übergeordnete Ziel des digitalen Verbraucherschutzes gilt es in der täglichen Sensibilisierungsarbeit, auf den Informationsstand, die Bedürfnisse und die Interessen der Zielgruppe herunterzubrechen.

Und diese Zielgruppe ist so divers wie unser Land – die einen nutzen das Internet vor allem als Kommunikationsmedium, die anderen vernetzen ihr ganzes Zuhause oder verbringen ihre Freizeit auf Social-Media-Plattformen oder beim Onlinegaming. Während manche Menschen der digitalen Welt mit Zurückhaltung begegnen und erst einmal Informationen und Unterstützung suchen, testen andere neue Möglichkeiten aus – mal leichtfüßig, mal leichtsinnig.

Dieses Spektrum ließe sich noch detaillierter darstellen und führt zu der Frage, wie Informationen zur Cybersicherheit gestaltet sein sollten, damit sie für Verbraucherinnen und Verbraucher im digitalen Alltag anwendbar und hilfreich sind. Das BSI hat 2023 mehrere Ansätze verfolgt, um Antworten hierauf zu finden: Es ließ einerseits Informationsmaterialien strukturiert von Testpersonen prüfen und bewerten und befragte andererseits die Zielgruppe direkt nach ihrem Wissen, ihren Einstellungen und Erfahrungen zum Thema Cybersicherheit.

LEIA – AWARENESS-MASSNAHMEN AUF DEM PRÜFSTAND

Das Projekt LEIA – Längsschnittstudie Effektive IT-Security Awareness – hatte zum Ziel, unterschiedliche Produkte zur Sensibilisierung und Information von Verbraucherinnen und Verbrauchern durch Nutzerstudien zu evaluieren und so Potenzial zur Verbesserung dieser Produkte zu identifizieren. Mit Effektivität ist dabei gemeint, dass zu einzelnen Kommunikationsprodukten erhoben wurde, ob sie Verbraucherinnen und Verbraucher tatsächlich motivieren, sich mit dem Thema zu beschäftigen, ob diese die vermittelten Informationen verstehen und im Kopf behalten sowie entsprechende Maßnahmen schließlich auch umsetzen (wollen).

Die Produktauswahl für die Untersuchung spiegelt die multimediale Angebotsvielfalt aus der Verbraucherkommunikation des BSI wider: In einem Studiotest bewerteten Probandinnen und Probanden u. a. zwei unterschiedliche Versionen der Themenwebseite „Sichere Passwörter erstellen". Über Onlinebefragungen konnten Testpersonen in separaten Befragungen beispielsweise Rückmeldungen zum Verbraucherschutz-Newsletter „sicher • informiert" und zu unterschiedlichen Videoformaten geben. Um vergleichbare Aussagen über die einzelnen Produkte zu generieren, definierten die Projektverantwortlichen übergeordnete Messgrößen, sogenannte Key-Performance-Indicators (KPIs), die über eine Reihe von Aussagen zu den Produkten ermittelt wurden. Diese KPIs bezogen sich auf die Aspekte Nutzerbindung (u. a. „Das Medium würde ich auch anderen Personen weiterempfehlen"), Gestaltung (u. a. „Der Gesamteindruck des Mediums bzw. das Layout gefällt mir sehr gut") und Inhalt (u. a. „Das Medium hat einen hohen Informationsgehalt").

HINWEISE ZUR BENUTZERFREUNDLICHKEIT SCHON UMGESETZT

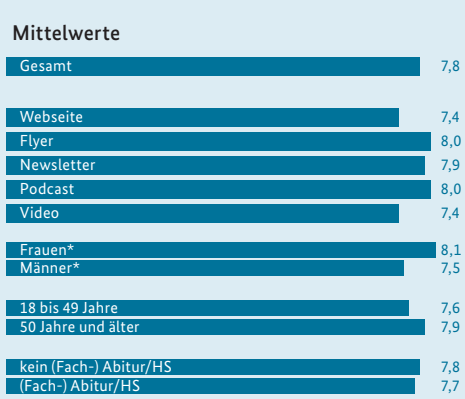
Die durchgeführten Befragungen haben gezeigt, dass die evaluierten Produkte hinsichtlich aller KPIs bereits gute Werte erzielen. Dies gilt insbesondere für den Inhalt. Daraus ergibt sich das Ziel, das Niveau der Aktualität, des Informationsgehalts und der Vertrauenswürdigkeit des Absenders zu halten. Wie relevant Cybersicherheit im digitalen Alltag ist und sein sollte, kann durch das BSI noch stärker hervorgehoben werden. Bei einzelnen Produkten konnten bereits Erkenntnisse aus den Befragungen mit Blick auf die Benutzerfreundlichkeit umgesetzt werden, bei anderen wird dies kontinuierlich erfolgen. Da ein Flyer mit „Tipps für ein sicheres Heimnetzwerk“ als Prototyp getestet wurde, ließen sich vor der Drucklegung zu den Veranstaltungen „Tag der offenen Tür der Bundesregierung“ und „Gamescom“ im August 2023 einige Anpassungen in der Gestaltung vornehmen. Bei den monatlichen Aufnahmen zum Podcast „Update verfügbar“ wird inzwischen auf einige inhaltliche Elemente verzichtet. Und positiv bewertete Gestaltungselemente aus dem Test der Webseite werden bewusst bei der Überarbeitung oder Planung von Themenseiten im Verbraucherbereich auf www.bsi.bund.de berücksichtigt.

LEIA – Bewertung der Gesamtzufriedenheit mit den getesteten Produkten

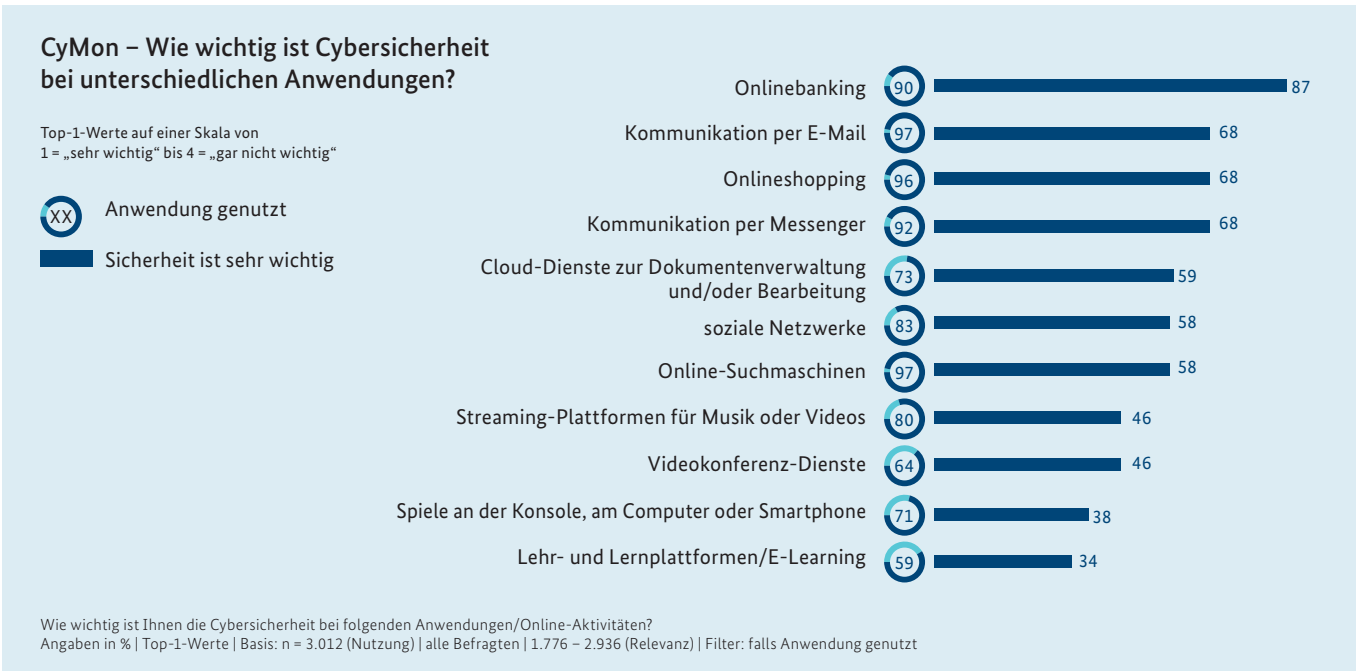
Die Webseite / der Flyer / das Video / der Podcast / der Newsletter hat mir insgesamt sehr gut gefallen.

Skala 0 = „stimme gar nicht zu“ bis 10 = „stimme voll und ganz zu“

Werte 8 bis 10 „stimme voll und ganz zu“
Werte 6 bis 7
Wert 5
Werte 3 bis 4
Werte 0 bis 2 „stimme gar nicht zu“



Angaben in % | Mittlerer Skalenwert | Basis: alle Befragten n = 243 | * signifikante Unterschiede zwischen den Untergruppen (Signifikanzniveau bei allen Tests p ≤ 0,05)



CyMon

CYMON – DER CYBERSICHERHEITSMONITOR 2023

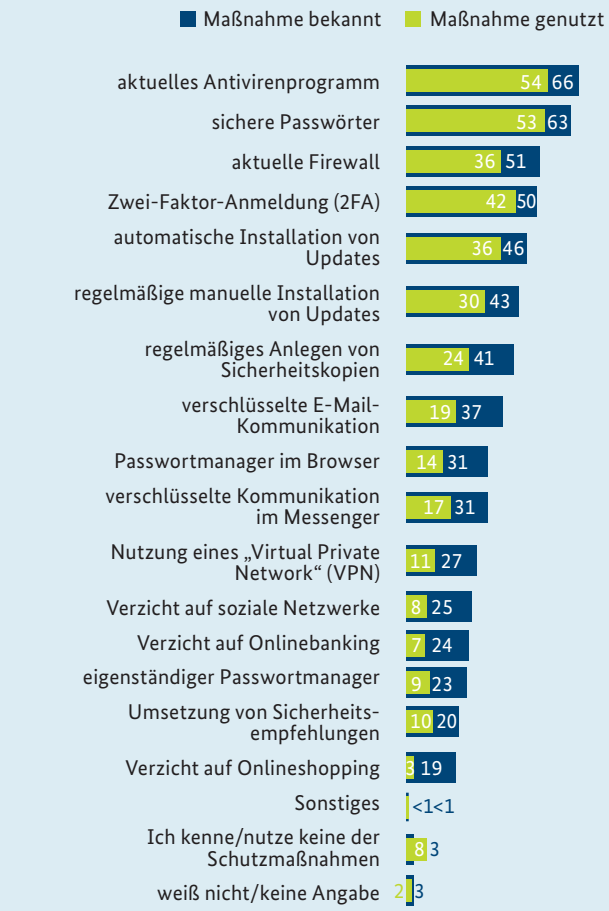
Eine andere Perspektive, die ebenfalls eine wichtige Arbeitsgrundlage in der Verbraucherkommunikation des BSI ist, eröffnet „CyMon – der Cybersicherheitsmonitor“. Die repräsentative Onlinebefragung, die bereits seit 2019 jährlich unter dem Namen „Digitalbarometer“ gemeinsam von BSI und der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) durchgeführt und veröffentlicht wird, stellt das Informationsverhalten, die Einstellungen und das Wissen zum Thema Cybersicherheit sowie Erfahrungen im Bereich Cyberkriminalität in den Fokus. 2023 stand eine Neuausschreibung an, durch die u. a. die Anzahl der befragten Personen erhöht wurde und mit der eine umfassende Überarbeitung des Fragebogens einherging. Dies nahmen BSI und ProPK zum Anlass, auch den Namen der Befragung anzupassen: Unter dem Titel „CyMon – der Cybersicherheitsmonitor“ rückt nun der inhaltliche Schwerpunkt Cybersicherheit in den Vordergrund.

INFORMATIONS- UND SCHUTZVERHALTEN

So zeigt sich in den Ergebnissen von 2023, dass sich gut die Hälfte der Befragten zumindest hin und wieder zum Thema Cybersicherheit informiert. Die Relevanz des Themas variiert abhängig vom Nutzungsverhalten stark und wird vor allem dann für wichtig gehalten, wenn es um Geldgeschäfte geht (Onlinebanking). Bei den eigenen Daten und genutzten Kommunikationsmitteln – von E-Mail-Kommunikation über soziale Netzwerke, Messenger, Videokonferenzen bis hin zu Lernplattformen – ist Cybersicherheit absteigend zum Teil deutlich weniger wichtig. Im Schnitt wenden die Befragten vier der abgefragten Cybersicherheitsmaßnahmen an, um sich vor Cyberkriminalität zu schützen. Besonders bekannt sind aktuelle Antivirenprogramme (66 %) und sichere Passwörter (63 %), diese werden mit 54 Prozent bzw. 53 Prozent auch am häufigsten genutzt.

CyMon – Bekanntheit und Nutzung von Schutzmaßnahmen

Welche der folgenden Schutzmaßnahmen vor Gefahren im Internet kennen Sie? Wie schützen Sie sich vor Gefahren im Internet?



Angaben in % | Mehrfachnennung | Basis: n = 3.012 (bekannt) | 3.012 (genutzt) | alle Befragten

ERFAHRUNGEN MIT CYBERKRIMINALITÄT

Mehr als jede/-r Vierte ist schon einmal von Cyberkriminalität betroffen gewesen (27 %). Rund vier von zehn Betroffenen (44 %) erlebten eine solche Straftat mindestens einmal in den vergangenen zwölf Monaten. Fasst man diese Vorfälle in übergeordneten Kategorien zusammen, waren in den vergangenen zwölf Monaten Datendiebstahl (35 %), Betrug allgemein (32 %) und Betrug beim Onlineshopping (27 %) die am häufigsten erlebten Straftaten. Insgesamt haben im vergangenen Jahr acht von zehn Betroffenen durch Cyberangriffe einen Schaden hinnehmen müssen (80 %). Dabei handelte es sich vorrangig um Vertrauensverlust in die entsprechenden Onlinedienste (33 %), zeitliche Schäden (26 %), emotionale Schäden wie Kränkung oder Angst (23 %) und um den Verlust von Daten (22 %). Einen direkten finanziellen Schaden erlitt fast jede/r Fünfte (18 %).

SORGE VOR BETRUG DURCH KÜNSTLICHE INTELLIGENZ

CyMon enthielt ebenfalls einige Fragen zum aktuellen Thema Künstliche Intelligenz (KI). Dabei zeigte sich, dass fast alle Befragten bereits von KI gehört haben (96 %) – sechs von zehn Befragten geben zudem an, genau zu wissen, was mit dem Begriff gemeint ist (60 %). Viele haben bereits von kriminellen Methoden gehört, bei denen KI eingesetzt wird. Vergleichsweise wenig bekannt sind hingegen Angriffe auf KI-Anwendungen. Darüber hinaus macht sich eine deutliche Mehrheit der Befragten große Sorgen wegen möglicher Manipulationen bzw. Betrug durch KI-Anwendungen.

Die Ergebnisse von CyMon werden insbesondere im ersten Quartal 2024, in dem der digitale Verbraucherschutz kommunikativ einen besonderen Schwerpunkt für das BSI darstellt, aufgegriffen und in der Ansprache von Verbraucherinnen und Verbrauchern berücksichtigt. ■

Weitere Informationen:

https://www.bsi.bund.de/dok/1078326

BSI-Basis-Tipp

Schritt für Schritt zum Gäste-WLAN

Haben Sie eigentlich einen Überblick, wem Sie schon einmal das Passwort für Ihr WLAN gegeben haben? Ein eigenes WLAN für Gäste schafft Ordnung und trennt Ihre Online-aktivitäten von denen Ihres Besuchs. Der Clou: Mit wenigen Handgriffen und ganz ohne Kosten lässt sich das Extranetzwerk in modernen Routern einrichten.

DAS KANN EIN ZWEITES NETZWERK ZU HAUSE

Ein Gäste-WLAN ist eine kabellose Netzwerkverbindung, die zusätzlich zum bestehenden Heimnetzwerk eingerichtet werden kann. Sobald Sie also ein Gäste-WLAN aktiviert haben, verfügen Sie über zwei voneinander getrennte Netze.

Ein eigenes WLAN für Gäste hat gleich mehrere Vorteile:

- Gäste können kaum Schaden im eigentlichen Heimnetzwerk anrichten. Selbst wenn sich z. B. Schadsoftware auf dem Laptop oder Smartphone eines Gastes befindet und sich der Besuch mit Ihrem Gäste-WLAN verbindet, bleiben Ihre Daten sicher. Denn Sie wickeln das Onlinebanking oder den Versand persönlicher Daten im gesicherten Heimnetzwerk ab.

- Sie können Rechte vergeben, z. B. festlegen, welche Seiten besucht werden dürfen oder wie viel Bandbreite zur Verfügung steht. Das bedeutet, Sie können bestimmen, welche Funktionen Ihre Gäste verwenden dürfen, und so die Kontrolle über Ihre Internetverbindung behalten.

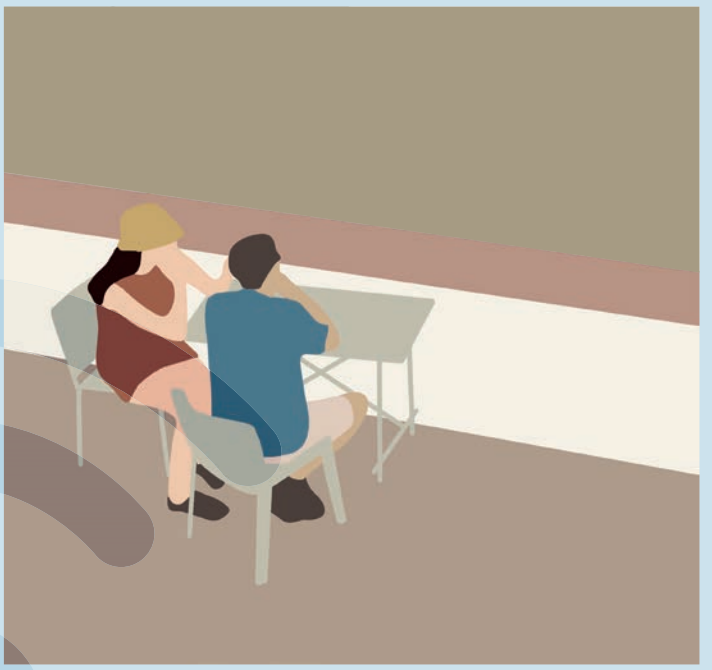
- Es ist praktisch im Alltag: Häufig bieten Router die Möglichkeit, einen QR-Code erstellen zu lassen, den Ihr Besuch dann einfach scannt und so Zugang zum Netzwerk erhält.

- Außerdem eignet sich das Gäste-WLAN bzw. ein separates WLAN gut, um smarte Geräte einzubinden. Ein womöglich unsicherer Saugroboter oder eine nicht entsprechend eingerichtete Rollladensteuerung können dort weniger Schaden anrichten.

DAS NETZWERK FÜR GÄSTE EINRICHTEN

Bevor Sie das Gäste-WLAN einrichten, stellen Sie sich die Frage: „Welchen Router habe ich?“ Zwar funktioniert die unten stehende Anleitung bei den gängigsten Modellen, allerdings kann es sein, dass Menüpunkte anders heißen, unter anderen Einstellungen zu finden sind oder dass Funktionen fehlen.

Die Aktivierung eines Netzwerks für Gäste ist jederzeit möglich, auch nach der Ersteinrichtung des Routers. Das bedeutet, dass Sie das zusätzliche WLAN ein- und ausschalten können, wann immer Sie möchten.



1) Öffnen Sie die Einstellungen Ihres Routers. Das funktioniert entweder über eine vom Hersteller vorgegebene Kurzadresse oder über eine IP-Adresse, die Sie in den Internet-Browser eingeben. Häufig ist das beispielsweise 192.168.0.1 oder 192.168.178.1.

2) Dort wählen Sie den Menüpunkt „WLAN“ (dieser Punkt kann auch „Netzwerk“ oder „Gastnetzwerk“ heißen) und klicken darunter auf „Gastzugang“.

3) Hier aktivieren Sie, meistens über ein Häkchen oder einen Schieber, den Gastzugang.

4) Vergeben Sie nun noch einen Namen für Ihr neues Netzwerk, der keine Rückschlüsse auf Sie, andere Personen oder das Routermodell zulässt.

5) Vergeben Sie ein starkes Passwort. Das Kennwort kann lang und komplex sein, weil Ihre Gäste das Passwort in der Regel nur einmal eingeben und es dann für den nächsten Besuch speichern können. Deshalb sollte das WLAN-Passwort aus mindestens 20 zusammenhanglosen Zeichen bestehen.

6) Schauen Sie nach, ob Sie hier auch die Verschlüsselung der Verbindung einstellen können. Diese sollte mindestens WPA2 lauten – wenn möglich sogar WPA3.

7) Bestätigen Sie die Einstellungen. Nun können Sie die Zugangsdaten mit Ihren Gästen teilen, und Ihr eigentliches Heimnetz bleibt geschützt. Auch smarte Geräte wie Saugroboter, Rollladensteuerungen oder intelligente Türklingeln sollten Sie in dieses separate Netzwerk einbinden und somit von sensiblen Diensten wie Onlinebanking oder Homeoffice-Anwendungen trennen.

ZUGANGSDATEN SICHER WEITERGEBEN

Es gibt viele Möglichkeiten, Freunden und Familienangehörigen das Passwort für das Gäste-WLAN mitzuteilen, aber nicht alle sind sicher. Die wichtigste Regel lautet: Geben Sie WLAN-Kennwörter nur an Personen weiter, denen Sie vertrauen. Hier vier Varianten, wie Sie Gästen Zugang in Ihr Netzwerk gewähren:

- Das Wichtigste zuerst: Hängen Sie Ihre Zugangsdaten nirgendwo aus, sondern verteilen Sie den Zugang nur auf Nachfrage.
- Der Klassiker: Schreiben Sie das WLAN-Passwort auf einen Zettel, den Sie sicher und nicht einsehbar verstauen. So können Ihre Gäste das Kennwort direkt vom Zettel abtippen.
- Die Komfortvariante: Lassen Sie Ihren Router einen QR-Code erstellen, den Ihr Besuch dann nur noch scannt. So können sich die Gäste nicht vertippen.
- Ohne Papier: Moderne Smartphones können WLAN-Kennwörter mit nahen Smartphones (des gleichen Betriebssystems) teilen.

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

Weitere Informationen:

https://www.bsi.bund.de/dok/10651618

https://www.bsi.bund.de/dok/6596788

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 x im Jahr, Print)
☐ Die Lage der IT-Sicherheit in Deutschland (1 x im Jahr, Print)

Name, Vorname

Organisation

Straße, Hausnr.

PLZ, Ort

E-Mail

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

Datum/Unterschrift:

Verantwortliche Stelle für die Verarbeitung Ihrer oben genannten personenbezogenen Daten ist das Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, 53133 Bonn. Die von Ihnen angegebenen Daten werden ausschließlich für die Verwaltung des Versands bzw. die Übermittlung der Informationen verwendet, denen Sie oben zugestimmt haben. Sie können diese Einwilligung jederzeit widerrufen. Hierzu genügt eine E-Mail an bsi-magazin@bsi.bund.de. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Weitere Informationen darüber, wie wir Ihre personenbezogenen Daten bei uns verarbeiten und welche Rechte Ihnen diesbezüglich zustehen, können Sie den beigefügten „Datenschutzrechtlichen Hinweisen“ zur Bestellung von BSI-Publikationen entnehmen. Einfach das Formular per Fax oder E-Mail einsenden:
Telefax: 0228 99 9582-5455 | E-Mail: bsi-magazin@bsi.bund.de

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

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

Datenschutzrechtliche Hinweise:
https://www.bsi.bund.de/DE/Service/Datenschutz/datenschutz_node.html

Impressum

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI) 53175 Bonn
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik Öffentlichkeitsarbeit Godesberger Allee 185–189 53175 Bonn Telefon: +49 (0) 228 999582-0 E-Mail: bsi-magazin@bsi.bund.de Internet: www.bsi.bund.de
Stand:	Dezember 2023
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-Mag23/717-2
Bildnachweise:	Titel: AdobeStock © Worawut; Seite 3: © BMI/Henning Schacht; Seite 4 – 5 (von links nach rechts): AdobeStock © KanawatTH, AdobeStock ©Marco, Anne Albert c/o kombinatrotweiss.de, AdobeStock © Ensar Durguti, AdobeStock © MNStudio, AdobeStock © Rawpixel.com; Seite 6 – 7: BSI, BSI, AdobeStock © pixelalex, AdobeStock © AdobeStock; Seite 9 bis 11: AdobeStock © KanawatTH, Seite 12 – 13: BSI; Seite 14 – 15: BSI; Seite 16 – 17: AdobeStock © jozefmicic; Seite 18 – 19: AdobeStock © Marco; Seite 20 – 21: AdobeStock © Marc; Seite 22 – 23: AdobeStock © Futuristicpixel, BSI; Seite 24 – 25: AdobeStock © Robert Herhold, BSI; Seite 26 – 27: AdobeStock © ginstudio; Seite 28 – 29: Landesmedienanstalt Saarland, AdobeStock © joelia; Seite 31: © bundesfoto/Uwe Völkner; Seite 32: © bundesfoto/Uwe Völkner; Seite 34: AdobeStock © Yeti Studio; Seite 35: BSI; Seite 36 – 37: Anne Albert c/o kombinatrotweiss.de; Seite 38 – 39: BSI; Seite 40 – 41: BSI; Seite 42 – 43: AdobeStock © enzozo; Seite 44 – 45: AdobeStock © Sunny studio, © bundesfoto/Uwe Völkner, privat; Seite 47: AdobeStock © Sunny studio, privat; Seite 48: AdobeStock © XtravaganT; Seite 49: AdobeStock © Jakub Cejpek; Seite 50 – 51: AdobeStock © gearstd, AdobeStock © giadophoto, AdobeStock © Polat Alp; Seite 53: AdobeStock © AI Images, AdobeStock © AI Images; Seite 54 – 55: AdobeStock © Bo Dean; Seite 56 – 57: AdobeStock © Ensar Durguti; Seite 59: ENISA, AdobeStock © koya979; Seite 61: BSI; Seite 63: Dr. Astrid Schumacher, Horst Samsel; Seite 64: privat; Seite 65: BSI; Seite 67: AdobeStock © Rawpixel.com; Seite 68: AdobeStock © Rawpixel.com; Seite 69: AdobeStock (c)Rawpixel.com; Seite 70: AdobeStock © Warunporn, AdobeStock © Warunporn; Seite 71: AdobeStock © Warunporn; Seite 72: AdobeStock © Warunporn; Seite 73: 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:

BSI
20. Deutscher IT-Sicherheitskongress

SAVE THE DATE

7. – 8. Mai 2024

Das BSI lädt zum 20. Deutschen IT-Sicherheitskongress ein!

An den zwei Kongresstagen machen Live-Vorträge, Podiumsdiskussionen und virtuelle Messestände IT-Sicherheit erlebbar und ermöglichen einen umfassenden fachlichen Einblick in aktuelle Themen der Cybersicherheit. Die Veranstaltung findet in digitaler Form statt und bietet den Teilnehmerinnen und Teilnehmern eine Plattform für den Austausch.

Jetzt vorab über die Webseite des Kongresses registrieren und über die Freischaltung des Anmeldeportals informiert werden!
www.bsi.bund.de/IT-Sicherheitskongress

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•