Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

BSI-Magazin 2021/01

Mit Sicherheit

CYBER-SICHERHEIT

Vom Weltraum abhängig:
Neue Bedrohung für Staat,
Wirtschaft und Gesellschaft

IT-SICHERHEIT IN DER PRAXIS

Cyber-Sicherheitsnetzwerk:
Unterstützung bei
IT-Sicherheitsvorfällen

DIGITALE GESELLSCHAFT

Bundesweite Kampagne
des BMI und BSI gestartet

EDITORIAL

Chance mit Risiko

Der Digitalisierungsschub, den wir bedingt durch die Corona-Pandemie in den letzten Monaten erlebt haben, ist Ergebnis einer großen Kraftanstrengung. Damit haben sich die Menschen in Staat, Wirtschaft und Gesellschaft auf die neue Situation eingestellt. Dieser Schub bringt unser Land voran, denn viele der spontan aufgesetzten Digitalisierungsprojekte werden uns auch nach der Pandemie erhalten bleiben.

Dennoch gilt nach wie vor: Wir stehen erst am Anfang eines umfassenden Digitalisierungsprozesses. Die transformative Kraft der Digitalisierung ist ungebrochen und birgt ein enormes Chancenpotenzial. Diesen Chancen stehen aber auch Risiken gegenüber – und diese Risiken liegen vor allem in der wachsenden Gefahr durch Cyber-Angriffe. Auch das hat die Pandemie wie unter dem Brennglas gezeigt: Mehr Digitalisierung braucht mehr Informationssicherheit. Denn Cyber-Kriminelle passen sich flexibel an neue Situationen an und nutzen die zusätzlichen Angriffsmöglichkeiten, die durch den vermehrten Einsatz digitaler Lösungen entstehen.

Der Grundsatz „Informationssicherheit ist Voraussetzung einer erfolgreichen Digitalisierung“ gilt deshalb mehr denn je. Deshalb freue ich mich sehr über das nun in Kraft getretene IT-Sicherheitsgesetz 2.0 und über das Vertrauen von Bundestag und Bundesrat in das BSI. Dieses Gesetz stärkt das BSI als zentrales Kompetenzzentrum der Informationssicherheit und ist ein Meilenstein auf dem Weg zu einer sicheren Digitalisierung.

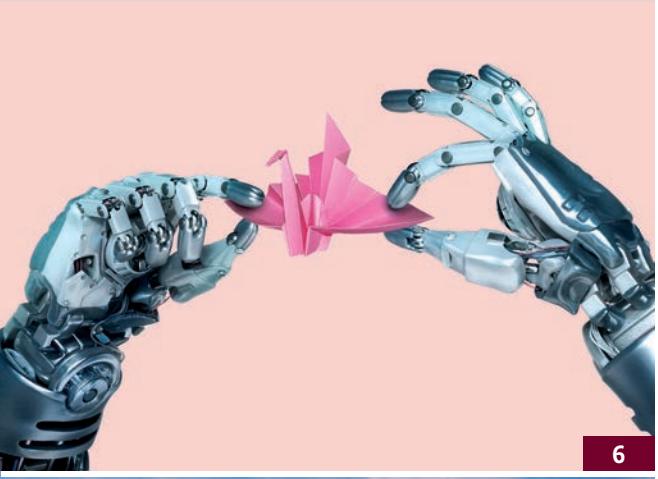
Damit kommen neue Kompetenzen und Herausforderungen auf das BSI zu, von denen ich mir sicher bin, dass unsere engagierten und kompetenten Mitarbeiterinnen und Mitarbeiter sie gut meistern werden. Wir blicken in dieser Ausgabe des Magazins auf 30 Jahre BSI zurück, die in vielfältiger Weise gezeigt haben, dass Veränderung gleichsam in der DNA des BSI angelegt ist. Als die Cyber-Sicherheitsbehörde des Bundes machen wir es uns auch in Zukunft zur Aufgabe, Digitalisierung in Deutschland sicher zu gestalten. Denn Informationssicherheit und Digitalisierung gehören untrennbar zusammen.

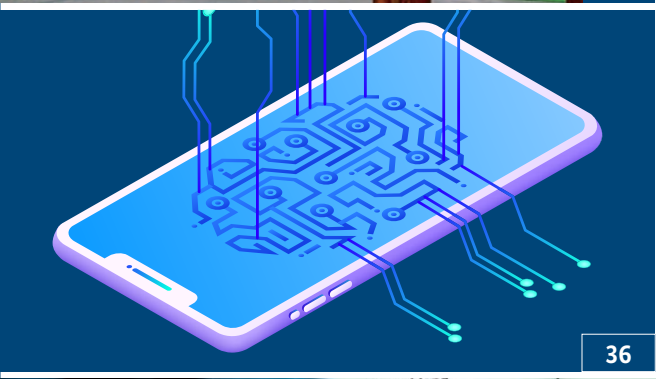
Über den umfangreichen Rückblick zum 30-jährigen Jubiläum des BSI hinaus informieren wir Sie in dieser Ausgabe unter anderem über die Bedeutung der IT-Sicherheit für Satellitensysteme, die Künstliche Intelligenz als Digitalisierungsmotor und die neue Kampagne des BSI #einfachaBSIchern.

Ich wünsche Ihnen eine interessante Lektüre.

Ihr

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik





INHALT

AKTUELLES

VERBRAUCHERSCHUTZ WIRD DIGITAL

Novum: Der Bericht zum Digitalen Verbraucherschutz 2020

Am 16. Juni ist erstmalig der „Bericht zum Digitalen Verbraucherschutz 2020“ des BSI veröffentlicht worden. In seiner ersten Ausgabe liegt der inhaltliche Schwerpunkt auf der „Cybersicherheit im Gesundheitswesen“. Vorgestellt werden unter anderem die Ergebnisse einer BSI-eigenen Studie rund um bestehende IT-Sicherheitsrisiken von Gesundheits-Apps und deren Markt. Ferner informiert der Bericht über die wesentlichen Sicherheitsvorfälle am digitalen Verbrauchermarkt 2020. Weitere Informationen zur neuen Jahrespublikation des Digitalen Verbraucherschutzes in der kommenden Ausgabe des BSI-Magazins und unter: www.bsi.bund.de.

VERTRAUEN: ROLLE DES BSI GESTÄRKT

IT SiG 2.0 ebnet Weg für eine moderne Cyber-Sicherheit in Deutschland

Mit der Verkündung im Bundesgesetzblatt trat am 28. Mai das IT-Sicherheitsgesetz 2.0 in Kraft. Das BSI erhält damit neue Kompetenzen, die seine Arbeit als Cyber-Sicherheitsbehörde des Bundes deutlich stärken, u. a. bei der Detektion von Sicherheitslücken und bei der Abwehr von Cyber-Angriffen. Damit wird die gesetzliche Aufgabe des BSI zur Information, Warnung und Beratung von Betroffenen gestärkt und das Ziel unterstützt, Sicherheitslücken in IT-Systemen jederzeit schnellstmöglich zu schließen.

Auch für Unternehmen wird Cyber-Sicherheit von noch größerer Bedeutung: Betreiber Kritischer Infrastrukturen und künftig auch weitere Unternehmen im besonderen öffentlichen Interesse müssen IT-Sicherheitsmaßnahmen nach dem Stand der Technik umsetzen. Zudem werden die Vorgaben zur Cyber-Sicherheit in den Mobilfunknetzen erweitert: Das Gesetz enthält eine Regelung zur Untersagung des Einsatzes kritischer Komponenten, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. So sorgt das Gesetz u. a. für die Informationssicherheit in den 5G-Mobilfunknetzen. Auch der digitale Verbraucherschutz wird durch das IT-Sicherheitsgesetz gestärkt und in den Aufgabenkatalog des BSI aufgenommen. So wird das BSI die unabhängige und neutrale Beratungsstelle für Verbraucherinnen und Verbraucher in Fragen der IT-Sicherheit auf Bundesebene.

AUSGEZEICHNETER ANSPORN

Das BSI erneut als Top-Arbeitgeber im Bereich IT im öffentlichen Dienst ausgezeichnet

Jedes Jahr befragt das Berliner Trendence Institut Studierende, Absolventen und Professionals aus den Bereichen Wirtschaft, Ingenieurwissenschaften, Informatik und Naturwissenschaft zum Berufseinstieg und Jobmöglichkeiten. Im Bereich IT konnte sich das BSI auch in diesem Jahr bei beiden Gruppen Platz 1 als bester Arbeitgeber im öffentlichen Sektor sichern. Im Gesamtranking schneiden wir mit Platz 14 bzw. Platz 11 ab. Insbesondere freuen wir uns über den von IT-Frauen gewählten 7. Platz im Vergleich zu Platz 14 im Vorjahr.

Mit verschiedenen kommunikativen Aktivitäten sowie dem Engagement unserer Kolleginnen und Kollegen und Cyberwomen möchten wir mehr Frauen ermutigen, in der IT-Branche Fuß zu fassen. Als Cyber-Sicherheitsbehörde des Bundes vereinen wir spannende Aufgaben am Puls der Digitalisierung mit sicheren Karriereperspektiven und Entwicklungsmöglichkeiten. Die Corona-Pandemie hat uns alle vor neue Herausforderungen gestellt, hat aber auch für einen Digitalisierungsschub gesorgt, den es nun zu verstetigen und abzusichern gilt. Wir möchten auch zukünftig Nachwuchstalenten und Berufserfahrenen ein abwechslungsreiches Arbeitsfeld bieten.

MEILENSTEIN

Allianz für Cyber-Sicherheit mit mehr als 5.000 Mitgliedern

„Netzwerke schützen Netzwerke“ ist das Motto der Allianz für Cyber-Sicherheit (ACS). Und das Netzwerk wächst weiter. Im April konnte die ACS ihr 5000. Mitglied begrüßen. Im Schulterschluss mit über 150 Partnern und 100 Multiplikatoren aus der Wirtschaft bietet die ACS zahlreiche Informations- und Austauschangebote an. Dabei richtet sie sich an alle IT-anwendenden Unternehmen und Organisationen in Deutschland, nicht nur an IT-Unternehmen und Experten auf diesem Gebiet. Die Allianz feiert im kommenden Jahr ihr 10jähriges Jubiläum.

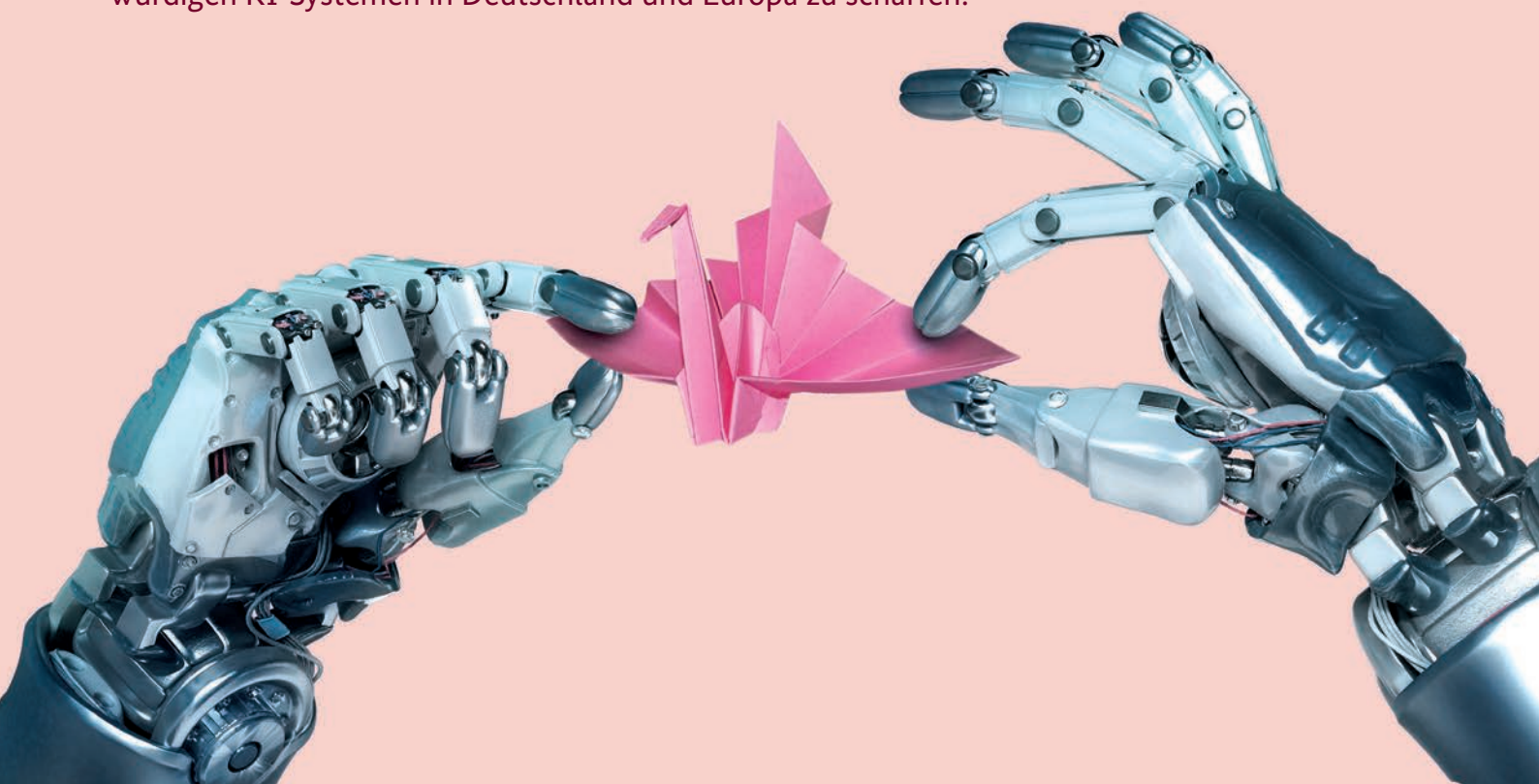
CYBER-SICHERHEIT

KI: zwischen Digitalisierungsmotor und Regulierung

Der Beitrag des BSI zu einem vertrauenswürdigen Einsatz Künstlicher Intelligenz

von Daniel Loevenich und Dr. Arthur Schmidt, Referat Technik-Kompetenzzentrum für Künstliche Intelligenz

IT-Systeme mit Künstlicher Intelligenz (KI) werden den technischen Fortschritt in den nächsten Jahren weiter beschleunigen. Für (teil-)autonom entscheidende oder selbständig agierende Systeme ergeben sich neue Aspekte der Informations- und Funktionssicherheit, Robustheit, Verlässlichkeit, Transparenz und Nichtdiskriminierung. Standards und Prüfverfahren für KI-Systeme müssen jedoch erst entwickelt werden. Diese Entwicklung begleitet das BSI im Rahmen seines gesetzlichen Auftrags. Unser Ziel ist es, Rahmenbedingungen zur Entwicklung von nachweislich resilienten und vertrauenswürdigen KI-Systemen in Deutschland und Europa zu schaffen.



KI UND DIGITALISIERUNG

KI ist eine Kerntechnologie in der digitalen Transformation von Staat, Wirtschaft und Gesellschaft. Sie erlaubt nicht nur eine Optimierung und Verbesserung bestehender Produkte, Dienstleistungen und Prozesse, sondern ermöglicht die Entwicklung neuer Produkte und Dienstleistungen. Die Zukunftsfähigkeit unserer Gesellschaft hängt im Wesentlichen von der erfolgreichen Digitalisierung und der intelligenten Integration der KI-Technologie ab, die nach unseren ethischen, sozialen und rechtlichen Vorstellungen entwickelt und eingesetzt wird. Das Thema IT-Sicherheit muss bei dieser Entwicklung von Anfang an eine wichtige Rolle spielen, um die Akzeptanz der neuen Technologie zu verbessern und die Resilienz unserer digitalen Gesellschaft zu stärken.

KI-ZERTIFIZIERUNG ALS VORAUSSETZUNG FÜR VERTRAUENSWÜRDIGE KI

An die Entwicklung und den Einsatz von KI-Systemen werden anwendungsspezifische und technologische Sicherheitsanforderungen gestellt. Die Prüfung solcher Anforderungen bildet die Voraussetzung für einen verantwortungsvollen Einsatz solcher Systeme. Zertifikate für KI-Lösungen sollen gewährleisten, dass die Sicherheitsanforderungen nachweislich eingehalten werden. Das BSI gestaltet die Entwicklung und Etablierung der notwendigen Prüfstandards und Zertifizierungsverfahren aktiv mit und bringt seine langjährige Erfahrung auf diesem Gebiet in den Prozess ein.

NORMUNGSROADMAP KI

Im Dezember 2020 veröffentlichten DIN und DKE die deutsche Normungsroadmap KI (NRM KI), in der eine umfassende Analyse des Bestandes und des Bedarfs an Normen und Standards für KI vorgelegt wurde. Ziel ist die frühzeitige Entwicklung eines Handlungsrahmens für die Normung und Standardisierung, der die internationale Wettbewerbsfähigkeit der deutschen Wirtschaft unterstützt. Das BSI wirkte bei der Entwicklung der NRM KI aktiv mit.

Die Version 1.0 der NRM KI definiert auch Handlungsempfehlungen an die Bundesregierung, die unter anderem die Aufgaben des BSI unmittelbar betreffen: Die Entwicklung von Normen und Standards für nachweisbar sichere KI-Systeme sowie die Entwicklung der dazu notwendigen Prüfverfahren.

NATIONALE UMSETZUNGSINITIATIVE „TRUSTED AI“

Die Handlungsempfehlung mit der höchsten Priorität betrifft die Einrichtung einer nationalen Umsetzungsinitiative Trusted AI (Artificial Intelligence / Vertrauenswürdige KI). Im Rahmen dieser Initiative sollen unter anderem:

- Kriterien, Methoden und die erforderlichen Grundlagen zur Prüfung der Robustheit, Funktions- und IT-Sicherheit, Verlässlichkeit, Integrität, Transparenz, Erklärbarkeit, Interpretierbarkeit und Nichtdiskriminierung von KI-Systemen entwickelt und an einer Auswahl von marktreifen KI-Anwendungen untersucht werden.
- Forschungs- und Entwicklungsbedarf zur Erweiterung bestehender Prüfmethoden und Prüfwerkzeuge sowie Prüfsysteme und Infrastrukturen identifiziert werden.
- Prüfverfahren in bestehende Normen und Standards eingebettet werden.

Das Konzept zur Bündelung ausgewählter Use Cases, die projektübergreifende Auswertung der Ergebnisse, ihre Generalisierung in Branchenstandards und ihre Einbettung in übergeordnete Normenwerke geht auf gemeinsame Überlegungen von DIN, Fraunhofer IAIS und BSI zurück.

AI CLOUD SERVICE COMPLIANCE CRITERIA CATALOGUE (AIC4)

KI-Lösungen, insbesondere aus dem Bereich des Maschinellen Lernens, sind eng an die Verarbeitung von Massendaten geknüpft und werden oft in Cloud-Umgebungen entwickelt und eingesetzt. Neben der Beratung und Unterstützung durch eigene KI-Experten bieten die Cloud Provider ihren Kunden auch KI-Frameworks und KI-Bibliotheken zur Entwicklung von Kundenlösungen an. Um Sicherheit und Transparenz in einem solchen Szenario zu schaffen, entwickelte das BSI den AIC4-Kriterienkatalog, der den etablierten BSI-Anforderungskatalog an Cloud-Dienste (C5) um spezielle KI-Kriterien erweitert. AIC4 stellt den ersten Schritt auf dem Weg zur Entwicklung eines integrierten Zertifizierungsverfahrens für KI-Systeme dar.

FAZIT

Vertrauenswürdige KI ist keine Vision. Weltweit steigt der Bedarf an regulativen Verfahren und Prüfverfahren. Das BSI stellt sich den Herausforderungen von Beginn an. Vertrauenswürdige KI ist für uns eine Chance, die digitale Transformation im partnerschaftlichen Dialog mit Politik, Wirtschaft, Forschung und Gesellschaft richtungsweisend zu begleiten. ■

Weiterführende Links:

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

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/AIC4/AI-Cloud-Service-Compliance-Criteria-Catalogue_AIC4.html

https://www.din.de/de/forschung-und-innovation/themen/kuenstliche-intelligenz/fahrplan-festlegen

Prüf- und Zertifizierungsverfahren für KI-Systeme

Im Interview: Prof. Dr. Stefan Wrobel, Institutsleiter Fraunhofer IAIS

Systeme der Künstlichen Intelligenz (KI) gewinnen immer weiter an Bedeutung. In diesem wichtigen Technologiebereich arbeiten das BSI und das IAIS gemeinsam für einheitliche Standards. Hintergründe dieser Kooperation erläutert Prof. Dr. Stefan Wrobel im Gespräch.

■ **Gemeinsam mit dem BSI arbeitet das Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS an Prüf- und Zertifizierungsverfahren für Systeme der KI – warum ist dieses Thema wichtig?**

Unsere Wirtschaft und unsere Gesellschaft haben die Relevanz der Künstlichen Intelligenz erkannt und diese Technologie hält nach und nach Einzug in Unternehmen, Infrastrukturen und unseren Alltag. Eine kürzlich publizierte Umfrage von Capgemini zeigt, dass heute schon mehr als die Hälfte aller Menschen weltweit täglich mit KI interagieren. Das zeigt, dass die Entwicklung von KI-Systemen keine akademische Fingerübung ist, sondern eine große Relevanz für den Alltag der Menschen sowie unserer Unternehmen erreicht hat. Wichtig ist deshalb, dass KI-Technologien das Vertrauen der Bürgerinnen und Bürger genießen. Gleichzeitig müssen KI-Anwendungen verlässlich funktionieren. Diese Faktoren bilden die Basis der Kooperation zwischen dem Bundesamt für Sicherheit in der Informationstechnik und Fraunhofer IAIS: Vertrauen und Akzeptanz in der Gesellschaft ist für die Entwicklung der Künstlichen Intelligenz in Deutschland und Europa unabdingbar, wenn wir technologisch souveräne und zukunftsfähige Technologien in die Fläche bringen und global wettbewerbsfähig sein wollen. Gleichzeitig bedeutet KI Investitionen – und damit wirtschaftliche Chancen. Doch dazu müssen KI-Systeme sicher sein und verlässlich funktionieren, sonst können sie diese Wertschöpfung nicht erbringen. Im Gegenteil: Wenn Unternehmen KI-Technologien überhastet und unabgesichert implementieren, kann dies zu Misserfolgen im Geschäft und sogar zu Schäden führen, die für Unternehmen existenzbedrohend sein können. Deshalb brauchen wir in Deutschland und Europa Prüfverfahren, die KI-Systeme verlässlich absichern und zertifizieren – denn nur so kann die Technologie ihr Potenzial entfalten, die Wettbewerbsfähigkeit unserer Wirtschaft steigern und Vertrauen in der Gesellschaft weiter aufbauen.

■ **Welche Ziele haben Sie sich für die Zusammenarbeit gesetzt und wie gestalten Sie die Kooperation? Welche Rolle spielt dabei die DIN-Normungsroadmap KI?**

Die kürzlich vom DIN veröffentlichte Normungsroadmap Künstliche Intelligenz, an der wir aktiv mitgearbeitet haben, aber auch aktuelle öffentliche Diskussionen, wie sie etwa auf der Plattform Lernende Systeme geführt werden, zeigen deutlich den Bedarf an Qualitätsstandards für KI-Systeme. Genau hier setzt die Kooperation zwischen dem BSI und Fraunhofer IAIS an: Gemeinsam werden wir diese Qualitätsstandards weiter definieren und Prüfverfahren entwickeln, die technische Eigenschaften von KI-Systemen validieren und sicherstellen, dass diese Qualitätsstandards eingehalten werden.

Und das ist im Fall von KI-Systemen tatsächlich eine Herausforderung. Denn das Besondere an KI ist, dass sie anders erzeugt wird als klassische IT-Systeme. KI basiert heute oft auf Maschinellem Lernen. Das bedeutet, KI wird erzeugt, indem das System aus Trainingsdaten lernt. Somit ist die Qualität dieser Trainingsdaten für die Entwicklung solcher Systeme entscheidend. Eine weitere Herausforderung ist es, Transparenz und Verständlichkeit von KI-Systemen sicherzustellen. Das ist nicht nur für gesellschaftliche Akzeptanz von Bedeutung, sondern vor allem damit menschliche Expertinnen und Experten überprüfen können, ob die KI das tut, was sie tun soll – ob sie Entscheidungen also verlässlich und im Sinne des Menschen trifft. Eine dritte Herausforderung ist das Selbstlernen im Betrieb. Wir wollen natürlich,

dass unsere KI-Systeme besser werden. Wir wollen, dass sie zukünftige Computerviren automatisch erkennen, weil sie lernen. Aber wir wollen natürlich nicht, dass die KI das Falsche lernt. Wir brauchen also Leitplanken. Und wir brauchen KI-Systeme, die mit anderen Systemen kombiniert werden können. Wir sprechen hier von hybriden Systemen.

Um diese Herausforderungen erfolgreich zu adressieren und adäquate Prüfsysteme auf den Weg zu bringen, vereinen Fraunhofer IAIS und das BSI über 20 Jahre Erfahrung in der angewandten KI-Forschung mit der langjährigen behördlichen Expertise für sichere IT-Technologie. Wir sind überzeugt davon, dass wir gemeinsam mit einer breitflächig anerkannten Prüfung und Zertifizierung einen deutschen Standard „AI made in Germany“ als Basis für Europa etablieren werden.

■ **Warum ist es wichtig, technische Eigenschaften von KI-Systemen zu validieren? Wie läuft so eine Prüfung ab?**

Wie auch für andere Software und IT-Systeme ist eine Prüfung von KI-Systemen ein Zusammenspiel aus der Validierung von zugesicherten Produkteigenschaften und der Auditierung von Prozessen. Besonders für KI-Systeme, die in sensiblen Bereichen zum Einsatz kommen, sind technische Prüfungen äußerst relevant. Schließlich ist es wichtig zu bestätigen, dass etwa ein autonomes Fahrzeug keine Unfälle verursacht, oder eine KI zur Diagnostikunterstützung in der Medizin keine intransparenten Entscheidungen trifft.

Werfen wir konkret einen Blick auf den Ablauf von KI-Prüfungen: Im ersten Schritt der Prüfung muss zunächst der Prüfgegenstand bestimmt werden. Hierzu gehört auch die Spezifikation der Betriebsumgebung. Als nächstes müssen die Ziele der Prüfung festgelegt werden – das heißt, welche Qualitätsstandards sollen geprüft werden, und welche Anforderungen an das KI-System ergeben sich aus dem konkreten Einsatzkontext? Schließlich erfolgt die eigentliche Prüfung, bei der Entwicklungsdokumentationen begutachtet, und wichtige Systemeigenschaften mithilfe von KI-Prüfwerkzeugen getestet werden. Die eingesetzten Prüfwerkzeuge helfen uns, Prüfschritte zu automatisieren, etwa indem wir systematisch nach Schwachstellen des KI-Systems suchen oder diese mit bestimmten Referenzdatensätzen testen.

■ **Wie stellen Sie die Marktfähigkeit der KI-Prüfung und -Zertifizierung sicher und bringen die Prüfverfahren konkret in die Fläche?**

Bei dem Thema KI-Prüfung und -Zertifizierung sollten wir, wie eingangs erwähnt, nicht nur an regulatorische Anforderungen und gesellschaftliches Vertrauen denken, sondern auch an Wertschöpfung und den wirtschaftlichen Erfolg von Unternehmen. Daher ist wichtig, dass entsprechende Prüfverfahren marktfähig sind und den Bedarf der Industrie adressieren. Ein gutes Beispiel ist das Projekt „KI-Absicherung“, das wir gemeinsam mit Volkswagen leiten. Dort arbeitet ein großes Konsortium, bestehend aus Automobilindustrie, Zulieferern, Forschungspartnern und Prüforganisationen daran, Standards für KI-Module des hochautomatisierten Fahrens zu entwickeln, damit diese im realen Straßenverkehr eingesetzt werden können. Genauso werden wir dies in unserer gemeinsamen Kooperation mit dem BSI auch für andere Branchen durchführen. Das heißt, wir werden in Anwenderkreisen Bedarfe für KI-Prüfungen ermitteln und gleichzeitig die entwickelten Prüfgrundlagen auf ihre Praxistauglichkeit testen. So stellen wir sicher, dass die Verfahren schnell ihren Weg in die praktische Anwendung finden, und Unternehmen von einer Zertifizierung profitieren können.

Kurzprofil Prof. Dr. Stefan Wrobel

Prof. Dr. Stefan Wrobel ist Professor für Informatik an der Universität Bonn und Leiter des Fraunhofer-Instituts für Intelligente Analyse- und Informationssysteme IAIS. Er ist der Bonner Direktor des Bonn-Aachen International Center for Information Technology (b-it) und einer der beiden Sprecher des Kompetenzzentrums Maschinelles Lernen Rhein-Ruhr (ML2R). Als Sprecher der »Fraunhofer-Allianz Big Data und Künstliche Intelligenz«, Direktor des »Fraunhofer-Forschungszentrums Maschinelles Lernen«, stellvertretender Vorsitzender des »Fraunhofer-Verbundes für Informations- und Kommunikationstechnologie« und Sprecher der Fachgruppe »Knowledge Discovery, Data Mining und Machine Learning« der Gesellschaft für Informatik engagiert sich Prof. Wrobel national und international für die intelligente Nutzung von Big Data und Künstliche Intelligenz und ihren Einsatz im Rahmen der Digitalisierung. Prof. Wrobel wurde von der Gesellschaft für Informatik als einer der prägenden Köpfe der deutschen KI-Geschichte ausgezeichnet.

Weitere Informationen:

https://www.iais.fraunhofer.de/

Umsetzung der Normungsroadmap KI

Im Interview: Christoph Winterhalter, DIN e.V.

■ Die Koordinierungsgruppe „KI-Normung und -Konformität“ verantwortet u.a. die Umsetzung und Fortschreibung der Normungsroadmap KI. Welche Kernaufgaben erfüllt die Koordinierungsgruppe in diesem Zusammenhang?

Die Koordinierungsgruppe wird die Umsetzung der Handlungsempfehlungen der KI-Roadmap vorantreiben. Dazu wird sie verschiedene Leuchtturmprojekte aufsetzen und koordinieren. Unter anderem geht es um eine Umsetzungsinitiative zur Prüfung und Zertifizierung von KI-Systemen. Im Herbst beginnt dann die Fortschreibung der Roadmap – mit neuen Schwerpunktthemen und unter Beteiligung neuer Stakeholder. Stärker als bisher wollen wir uns in die gesellschaftliche Diskussion zum Thema einbringen, und Empfehlungen zu wichtigen innovationspolitischen Entwicklungen und zur Gestaltung des KI-Standorts Deutschland aussprechen.

■ Was soll die von Ihnen angesprochene Umsetzungsinitiative leisten?

Um das Vertrauen von Zivilgesellschaft und Wirtschaft in KI zu stärken und so eine noch breitere Anwendung zu ermöglichen, benötigen wir Qualitätskriterien und Prüfverfahren. Diese können dann als Grundlage für Zertifizierungen und Konformitätsbewertungen dienen. Hierfür braucht es neue Ansätze - und die möchten wir gerne im Rahmen der Umsetzungsinitiative entwickeln.

■ Wie lässt sich die Marktdurchdringung von KI-Standards erreichen? Welche Rolle sehen Sie für das BSI im Hinblick auf die Weiterentwicklung der Normungsroadmap KI und ihre kontinuierliche Umsetzung?

Standards müssen den Bedarf ihrer Anwenderinnen und Anwender erfüllen. Das bedeutet, sie müssen praxisnah anhand anwendungstypischer und branchenrelevanter Fallbeispiele entwickelt werden. Entscheidend ist, dass die KI-Standardisierung der hohen Dynamik von KI-Forschung und industrieller Entwicklung und Anwendung Rechnung tragen muss, und Standards damit kontinuierlich angepasst werden. Als Vertreter der öffentlichen Hand ist das BSI hier mit seiner Expertise für eine sichere Digitalisierung in Deutschland ein maßgeblicher und wichtiger Partner – sowohl für die Umsetzungsprojekte als auch für die Fortschreibung der Roadmap. ■

Kurzprofil Christoph Winterhalter

Christoph Winterhalter ist Vorstandsvorsitzender von DIN Deutsches Institut für Normung e. V. Zuvor war er über 20 Jahre in der Industrie für den ABB Konzern tätig - zuletzt verantworte er seit 2013 global das Konzerngeschäftsfeld Maschinensteuerungen und Automation.

Seit Juli 2016 ist er Vorsitzender des Vorstandes von DIN, um Kundenorientierung und digitale Transformation innerhalb des international vernetzten Normungssystems voranzutreiben. Seit 2017 ist er als deutscher Vertreter Mitglied des ISO Council.

Neben seinen Aufgaben bei DIN ist Christoph Winterhalter u.a. im Beirat der VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik sowie in verschiedenen Funktionen innerhalb des ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V. und der Plattform Industrie 4.0 engagiert.

Vom Weltraum abhängig

Neue Bedrohung für Staat, Wirtschaft und Gesellschaft

Von Frank Christophori, Leiter des Referats Sichere IT-Systeme für Luft- und Raumfahrt

Das Funktionieren unseres Staates, unserer Wirtschaft und unserer Gesellschaft ist immer mehr abhängig von digitalen Diensten – in der Kommunikation, Navigation, Zeit- und Positionsbestimmung sowie in der Klimaüberwachung und Wettervorhersage.

Aufgrund der globalen Vernetzung ist die Realisierung dieser Dienste immer häufiger nur durch satellitengestützte Infrastrukturen möglich. Die übermittelten Informationen bilden die Grundlage für Planungen, Wissen und Entscheidungen im täglichen Leben. Sie müssen daher angemessen geschützt werden. Die Verfügbarkeit, aber auch die Integrität und Vertraulichkeit der Systeme, Dienste und Informationen sind dabei essenzielle Faktoren.

Diese Tatsache reizt natürlich immer mehr Hacker oder ähnliche Gruppierungen.

SATELLITENGESTÜTZTE INFRASTRUKTUREN - WICHTIG FÜR UNSERE ZUKUNFT

Seit 1955 arbeiten die USA und die UdSSR an Weltraumprogrammen. Am 04. Oktober 1957 startete der erste Satellit in den Weltraum: Sputnik 1.

Damit begannen das Zeitalter der Raumfahrt und das Wettrennen, insbesondere zwischen der UdSSR und den USA, um die Vorherrschaft im Weltraum.

Nach der „Demonstrationsphase“ zur Machbarkeit erfolgte Anfang der 60er Jahre der Aufbau der ersten Satellitenkommunikationsinfrastrukturen mittels GEO-Satelliten.

Die erste große, operativ genutzte, komplexe MEO-Konstellation war GPS NavStar, die in den 1980er Jahren entwickelt wurde und Mitte der 90er Jahre in den operationellen Betrieb ging.

Die ersten SatCom-Dienste waren kostspielig, daher wurden sie überwiegend von behördlichen Anwendern genutzt.

Das wachsende Verlangen nach immer schnelleren (Internet-) Diensten und höchster Mobilität erforderten alternative Infrastrukturen. Die Generation 5G/IoT ist die Antwort auf diese Heraus-forderungen. Die Architektur

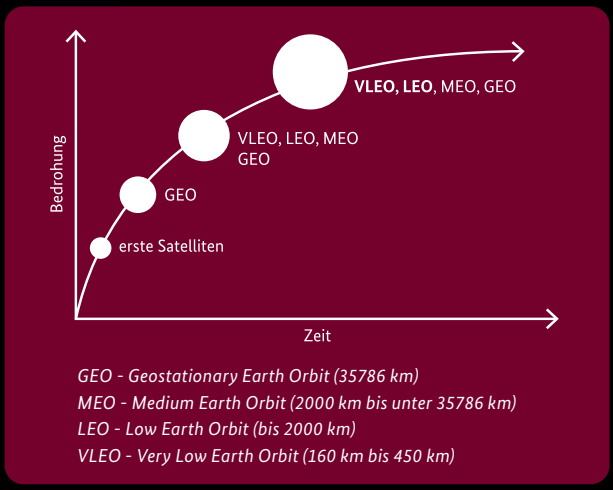


Abbildung 1: Entwicklung der Satelliten

und Organisation unterscheiden sich vollständig von denen der bis dato vorhandenen GEO- / MEO-Systemen. Ein einfacher Ausbau der vorhandenen Infrastrukturen ist daher nicht ausreichend.

Die Versorgung von maritimen, luftgestützten, ländlichen oder verlassenen bzw. dünn bis gar nicht besiedelten Gebieten mit zuverlässigen, breitbandigen und kostengünstigen Diensten läutete die Geburtsstunde der LEO- / VLEO-Satelliten ein.

Inzwischen gibt es mehrere Anbieter: TeleSat, IRIDIUM, OneWeb und SpaceX, um nur einige zu nennen

Diese Satelliten besitzen sehr viel kleinere Formfaktoren, wie z. T. eine Kantenlänge von nur wenigen Zentimetern (Mini-, Micro-, Nanosatellites etc.). Dadurch können viele der „Würfel" auf einmal gestartet werden. Dieser positive Aspekt und der niedrige Orbit ermöglichen eine kostengünstige Installation der Systeme.

BEDROHUNGEN FÜR SATELLITENSYSTEME

Grundsätzlich sind Satellitensysteme ähnlichen Bedrohungen wie klassische terrestrische Systeme ausgesetzt. Die sich daraus ergebenden Risiken sind allerdings anders zu bewerten.

Dabei sind drei Segmente zu betrachten, die bzgl. der Auswirkungen unterschiedlich zu gewichten sind:

- die Infrastruktur im Weltraum (Raumsegment),
- die zugehörige Infrastruktur am Boden (Bodensegment) und
- die angebotenen Dienste (Dienstesegment) bzw. Informationen.

Die Bedrohungen adressieren alle Segmente, allerdings in variierenden Anteilen. Sie können in vier Kategorien unterteilt werden:

- physikalische,
- elektronische und
- Cyber-Bedrohungen (umfasst die Übernahme von Komponenten oder Systemen, das Eindringen und die unautorisierte Nutzung), sowie
- Weltraumschrott.

Die Ursachen für diese Bedrohungen können Angreifer, Innentäter sowie Umwelt und Natur oder von technischer bzw. struktureller Art sein.

Zu den physikalischen Bedrohungen gehören u.a. bodengestützte Anti-Satelliten-Systeme (ASAT), EMP oder andere Satelliten. Neben diesen Bedrohungen durch Angreifer nimmt die Bedrohung durch Weltraumschrott immer mehr zu. Die Gefahr ist hoch, dass bei der Beschädigung oder Zerstörung im Nachgang weitere Systeme – auch eigene – geschädigt werden, z.B. durch Trümmerteile.

Elektronische Bedrohungen beeinflussen vorübergehend die Funkverbindungen zwischen Satelliten untereinander oder mit den Bodeninfrastrukturen. Das können natürliche (weltraum-) wetterbedingte oder absichtlich herbeigeführte Störungen sein, z. B. Jamming oder Spoofing. Derartige Unterbrechungen können schwerwiegende Konsequenzen nach sich ziehen. Durch zusätzliche Sicherheitsfunktionen oder Signalstrukturen kann die Robustheit der Signale und Dienste gegenüber diesen Störungen erhöht werden.

Der Cyber-Raum (CR) spielt in den letzten Jahren auch für Satellitensysteme eine immer größere Rolle. Nicht nur die Verfügbarkeit, sondern auch die Vertraulichkeit und Integrität bzw. Authentizität der Systeme oder Dienste sind hier betroffen. Im Gegensatz zu den anderen Bedrohungen adressieren die Bedrohungen im CR alle drei Segmente. Sie sind mit einfachen Mitteln und mit vergleichbar geringen Ressourcen durchführbar. Daher muss nicht zwingend eine staatliche oder international agierende Organisation mit entsprechenden finanziellen und personellen Ressourcen dahinterstehen.

Dass Angriffe auf Satellitensysteme im CR eine sehr reale Bedrohung darstellen, hat sich in der Vergangenheit bereits

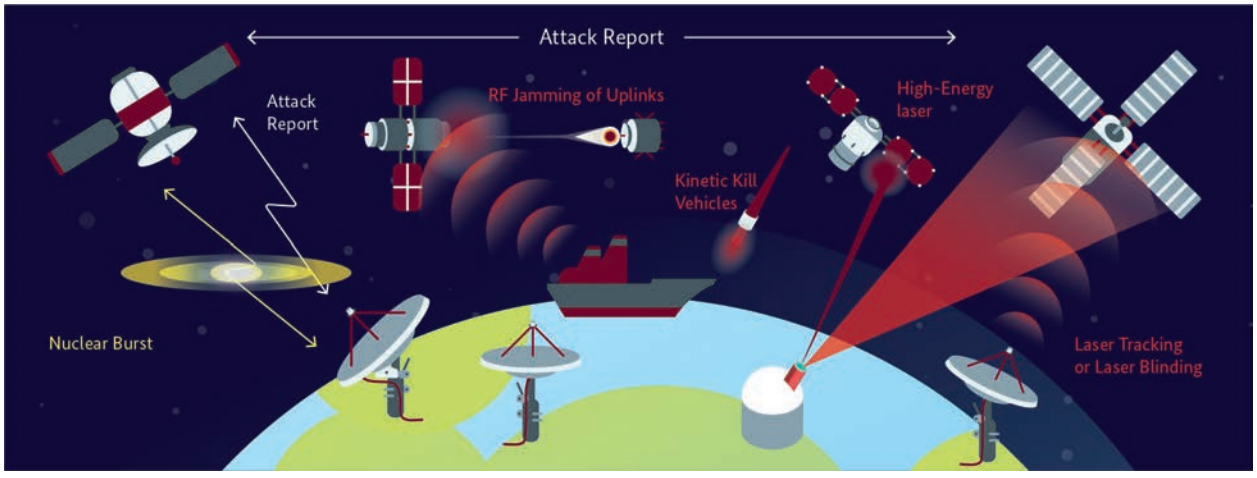


Abbildung 2: Bedrohungen für Satellitensysteme (Quelle: US Verteidigungsministerium, 2013)

gezeigt. Als Reaktion darauf hat die US Air Force den Wettbewerb Hack-a-Sat ins Leben gerufen (www.hackasat.com). Hacker aus aller Welt erhielten legal die Möglichkeit, ihr Können unter Beweis zu stellen. Neben Teams aus den USA und Polen stand auch ein deutsches Team auf dem Siegerpodest. Letztendlich ist dieser Wettbewerb nicht nur eine Spielwiese für Hacker.

„[...] The Air Force is opening up systems and hardware to hackers to discover vulnerabilities before their adversaries. [...]“

Diese Aussage unterstreicht, welch große Bedeutung die USA diesem Aspekt beimessen. Angriffe im CR werden nicht immer oder erst (zu) spät erkannt. Dem Schutz von Satelliten vor Angriffen im CR kommt damit eine völlig neue Bedeutung zu. Allumfassender Schutz, idealerweise auch gegen noch nicht identifizierte konkrete Bedrohungen im CR, ist das oberste Ziel.

KONSEQUENZEN FÜR DIE SICHERHEIT

Die immer größere Abhängigkeit unseres Staates, der Wirtschaft und der Gesellschaft von digitalen Diensten fordert zuverlässige Kommunikationssysteme. Die Globalisierung verlangt passende, weitereichende Infrastrukturen. Ohne vielfältige Satellitendienste wäre eine weltweit vernetzte Gesellschaft nicht denkbar.

Nahezu alle Sektoren unserer Kritischen Infrastrukturen (KRITIS) bedienen sich in der einen oder anderen Weise satellitengestützter Dienste. Seien es Position und Navigation für Verkehrsanwendungen, Zeit für Finanzwelt und Energieversorger oder Telekommunikation für Sprach-, Daten- und Videoübertragungen, ohne Satelliten wären diese Dienste gar nicht oder nur eingeschränkt verfügbar.

Für die überwiegende Anzahl der Anwendungen ist eine eingeschränkte Verfügbarkeit unkritisch, da neben den Satellitensystemen andere alternative Systeme einen Ausfall kompensieren können. Terrestrische Netze bieten dieses Backup. In anderen Szenarien bedeutet der Wegfall oder die Degradierung eines Dienstes oder der Integrität der Informationen ein hohes Risiko. Entscheidend ist der Ort, an dem wir auf die Dienste zugreifen wollen oder müssen.

Flugzeuge und Schiffe sind heute hochkomplexe IT-Systeme, die während ihrer Missionen nicht auf Bodeninfrastrukturen zugreifen können. Der Erfolg und die Sicherheit verlangen funktionierende Kommunikationsstrukturen, einschließlich der Integrität und z.T. Vertraulichkeit der Daten. Für Flugzeuge und Schiffe stellen weltraumgestützte Systeme teilweise die einzige Möglichkeit dar, mit der Außenwelt zu kommunizieren oder von ihr Informationen zu erhalten.

Die verschiedenen Anwender, z. B. zivile Flugunternehmen, das Militär, Banken oder die Wissenschaft, nutzten in mehr oder weniger großem Umfang satellitengestützte Dienste. Wie schwerwiegend die Konsequenzen bei Störungen dieser Dienste sind, ergibt sich aus der Wichtigkeit der Mission für die Nutzerinnen und Nutzer und dem möglichen Schaden, z.B. Verlust oder Gefährdung von Menschenleben, finanzielle Verluste oder kritische politische bzw. militärische Situationen.

ZUNEHMENDE ABHÄNGIGKEIT

Ohne satellitengestützte Anwendungen ist eine globale Kommunikation und Vernetzung nicht mehr denkbar. Mit Blick auf die zukünftigen Anwendungen im Kontext 5G / IoT wird die Abhängigkeit zunehmen.

Infrastrukturen für Satelliten sowohl die weltraumbasierten als auch die terrestrischen sind in Deutschland noch nicht als nationale Kritische Infrastruktur definiert. Andere Nationen beschäftigen sich mit dem Thema schon länger sehr intensiv.

Die US-Regierung erklärt: Sie ***“[...] will foster practices within Government space operations and across the commercial space industry that protect space assets and their supporting infrastructure from cyber threats and ensure continuity of operations [...]”***. Satellitensysteme sind somit eine der tragenden Säulen für die Kommunikation in Staat, Wirtschaft und Gesellschaft.

Auch in Deutschland sollte es das Ziel sein, Satelliteninfrastrukturen nationalen kritischen Infrastrukturen vollständig gleichzustellen. Die rechtlichen Grundlagen dazu fehlen noch. Entsprechende Formulierungen können im Rahmen der nächsten Novellierungen der BSI KRITIS-VO, des IT-SIG, oder bei der Entwicklung des nationalen Weltraumgesetzes eingebracht werden. Unabhängig davon will das BSI zusammen mit ausgewählten Herstellern Sicherheitsanforderungen an Satelliteninfrastrukturen erarbeiten. Diese fließen anschließend in eine technische Richtlinie (TR) für Satelliten ein und dienen als Richtschnur für die Hersteller von Satelliten. ■

Weiterführende Links:

Chatham House, Cyber Security of NATO‘s Space-Based Strategic Assets, 07/2019
https://www.chathamhouse.org/

DNV GL - Maritime cyber security
https://www.dnvgl.com/maritime/insights/topics/maritime-cyber-security/index.html

CSIS – Space Threat Assessment, April 2019, Todd Harrison and Partners
www.csis.org

International Maritime Organization (IMO)
https://www.imo.org/en/MediaCentre/Pages/WhatsNew-932.aspx

30 JAHRE BSI

Zurück in die Zukunft: 30 Jahre BSI

Vom Zukunftskonzept Informationstechnik zum Gestalter der sicheren Digitalisierung

30 Jahre sind in der realen Welt eine lange Zeit - in der digitalen fast eine Ewigkeit. Deshalb ist 30 für eine Behörde, die sich mit Informationssicherheit, mit Cybersicherheit beschäftigt auch ein bemerkenswertes Alter. Wir möchten Sie anlässlich des Jubiläums in diesem Sonderteil des Magazins auf eine Zeitreise mitnehmen. Nicht aus nostalgischen Gründen, sondern weil sich mit dem Blick auf die rasante technologische Entwicklung zeigt, wie wichtig Geschwindigkeit, Anpassungsfähigkeit und Innovation auch und gerade für die zentrale Cyber-Sicherheitsbehörde des Bundes sind.

INNOVATION-HUB – DAS GEGENTEIL EINER BEHÖRDE?

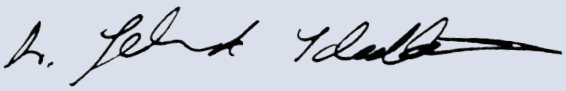
Zum üblichen und viel bemühten Klischee über Behörden, in dem sicher wie immer ein wenig Wahrheit steckt, gehören traditionell langsame Abläufe und unnötige Bürokratie. Und doch ist für mich das BSI eher ein Innovation-Hub als eine normale Behörde. Das liegt an dem dynamischen Themenfeld, in dem wir uns bewegen, an unserer in 30 Jahren gewachsenen offenen Diskussionskultur – und vor allem an unseren Mitarbeiterinnen und Mitarbeitern, die sich weit über den üblichen Arbeitsalltag hinaus und mit großer Leidenschaft mit innovativen Technologien und sicherer Digitalisierung beschäftigen. Nur so war und ist es möglich, den vielfältigen und sich immer wieder wandelnden Aufgaben als zentrale Cyber-Sicherheitsbehörde des Bundes und Gestalter der sicheren Digitalisierung gerecht zu werden.

VON DEN ANFÄNGEN DES WWW BIS KI-GESTEUERTER MOBILITÄT

Zum Zeitpunkt der Gründung des BSI machte das Internet gerade seine ersten Schritte, „Mobile Devices“ waren koffergroße D-Netz-Telefone. Heute arbeitet das BSI als tragende Säule der Sicherheitsarchitektur in Deutschland maßgeblich an zentralen Digitalisierungs- und Zukunftsthemen mit: von sicherem Einsatz künstlicher Intelligenz, über den digitalen Verbraucherschutz, die sichere Nutzung von 5G, Cyber-Sicherheit der digitalen Verwaltung, autonomes Fahren bis zur digitalen Absicherung der Kritischen Infrastrukturen.

Nie war die Digitalisierung gleichzeitig so präsent in unser aller Alltag und so wichtig für den Erfolg des Wirtschaftsstandortes Deutschland. Der Grundsatz „Informationssicherheit ist Voraussetzung einer erfolgreichen Digitalisierung“ gilt heute und zukünftig noch mehr als vor 30 Jahren bei der Gründung des BSI.

Ich wünsche Ihnen eine unterhaltsame Lektüre des 30 Jahre BSI-Sonderteils.



Dr. Gerhard Schabhüser

Vizepräsident des Bundesamts für Sicherheit in der Informationstechnik

Ein Blick zurück – von außen

Die neuen Abteilungsleiterinnen und Abteilungsleiter stellen sich vor.

In den vergangenen Jahren hat das BSI immer wieder neue Aufgaben erhalten, um die Cyber-Sicherheit in der Digitalisierung zu gewährleisten. Aus diesem Grund wurden neue Abteilungen eingerichtet, deren Leitungen mit Kandidatinnen und Kandidaten besetzt wurden, die nicht bereits im BSI tätig waren. Das 30-jährige Jubiläum der Behörde nehmen sie nun zum Anlass für einen Rückblick aus externer Perspektive.

Sandro Amendola
Leiter der Abteilung Standardisierung, Zertifizierung und Sicherheit von Telekommunikationsnetzen (SZ)

Seit Beginn meines Berufslebens in den 90er Jahren habe ich Kontakt mit dem BSI. Die Prüfstelle meines damaligen Arbeitgebers war beim BSI als Prüfstelle zur Durchführung von Evaluationen anerkannt. Sehr schnell stellte ich fest, dass die Nachvollziehbarkeit einer Prüfung für das BSI von großer Bedeutung ist: Prüfberichte waren schon damals sehr umfangreich und ich hatte pflichtbewusste BSI-Beamte vor Augen, die jede Seite dieser Dokumente nach der Vorgabe „Gründlichkeit geht vor Schnelligkeit“ äußerst gewissenhaft nachvollzogen und kommentierten. Diese Wahrnehmung war eine Konstante in meiner 25-jährigen Tätigkeit als Prüfstellenmitarbeiter.

Die Rückmeldungen des BSI bewiesen, dass das BSI über große technische Kompetenz verfügt, was aber – einer zahnärztlichen Tiefenbohrung vergleichbar – schmerzhaft sein konnte. Jede Aufforderung, zusätzliche zeitaufwändige Prüfungen durchzuführen oder Beschreibungen zu vertiefen, nagten an meinem Selbstwertgefühl als Prüfer.

Ich evaluierte vor allem Chipkarten, wie z. B. den elektronischen Personalausweis. Genau diese Gründlichkeit des BSI, die ebenso bei der französischen Partnerbehörde praktiziert wird, stellte sich bei der Zertifizierung von Halbleitern als Erfolgsrezept dar. Auf Druck der Zertifizierungsstellen verbesserten sich die Sicherheitseigenschaften von in Chipkarten eingesetzten Halbleitern von Zertifizierung zu Zertifizierung. Bis heute werden trotz immer neuer oder weiterentwickelter Angriffstechniken Halbleiter mit hoher Angriffsresistenz erfolgreich zertifiziert und BSI-Zertifikate genießen international ein hohes Ansehen.

Schließlich arbeitete ich über einen Zeitraum von zehn Jahren hinweg mit dem BSI auch bei der Standardisierung von Angriffstechniken eng zusammen und unterstützte das BSI bei der internationalen Verankerung seiner sicherheitstechnischen Vorstellungen.

Als Sicherheitsexperte für den elektronischen Zahlungsverkehr beriet ich das BSI außerdem bei der Erstellung von Studien. Diese Tätigkeit eröffnete mir eine neue Seite des BSI: Ich arbeitete jetzt mit BSI-Kolleginnen und -Kollegen zusammen, die die Wirkung regulatorischer Vorgaben untersuchten und daraus ihre Schlüsse für die Verbraucherinnen und Verbraucher zogen.

Als ich im September 2019 auf die ausgeschriebene Stelle des Abteilungsleiters „Standardisierung und Zertifizierung“ aufmerksam gemacht wurde, zögerte ich nicht, mich zu bewerben. Ich war fasziniert von der Aussicht, bei der Weiterentwicklung der Prüfmethoden Gründlichkeit mit Schnelligkeit in Einklang bringen zu können, aber auch davon, meine erfahrenen Ansprechpartnerinnen und -partner nun als Kolleginnen und Kollegen zur Seite zu haben.

„Ich war fasziniert von der Aussicht (...) meine erfahrenen Ansprechpartnerinnen und -partner nun als Kolleginnen und Kollegen zur Seite zu haben.“ – *Sandro Amendola*

Dr. Silke Bargstädt-Franke
Leiterin der Abteilung Cybersicherheit in der Digitalisierung und für elektronische Identitäten (DI)

Noch nie waren Digitalisierung, elektronische Identitäten und Cyber-Sicherheit so wichtig wie in der aktuellen Situation. Daher ist es mir eine besondere Freude, im Jahr des 30-jährigen Bestehens des BSI, seit dem 01.03.2021, nach 22-jähriger erfolgreicher Tätigkeit in Industrie und Wirtschaft, als Abteilungsleiterin DI im BSI zu sein, um meine Erfahrungen aus den Themenfeldern sichere Identitäten und Cyber-Sicherheit, in die zukünftige Gestaltung der Digitalisierung der Bundesrepublik Deutschland einzubringen.

Seit 2009 war ich im internationalen Regierungsgeschäft bei Giesecke + Devrient und der Veridos GmbH in verschiedenen Führungspositionen im Projekt- und Produktmanagement tätig. Unter anderem habe ich langjährige und erfolgreiche interkulturelle Beziehungen zu Kunden insbesondere im arabischen Raum aufgebaut. In meiner letzten Funktion als Global Head of Product Management bei der Veridos GmbH verantwortete ich das gesamte

Produktportfolio, welches das klassische hochsichere Reisedokument sowie komplette Systemlösungen – beispielsweise für mobile Identitäten und Verifikation - umfasste. In dieser Rolle gab es bereits zahlreiche Berührungspunkte mit dem BSI. Hierbei haben sich die Expertinnen und Experten kontinuierlich durch eine hohe Expertise und als nachhaltige Treiber neuer Ideen, Normen und Spezifikationen ausgezeichnet – wie z. B. bei der Implementierung von SAC/PACE für die dritte Generation der elektronischen Reisepässe. Von internationalen Regierungskunden, wurde das BSI stets als weltweit anerkannte Institution – insbesondere als Repräsentant Deutschlands in internationalen Gremien - federführend bei der Definition europäischer und weltweiter Sicherheitsstandards wahrgenommen. Bei der Etablierung des elektronischen Personalausweises, einer elektronischen ID-Karte mit höchster Sicherheit, konnte die Veridos GmbH das BSI begleiten und schätzte die Erhöhung der Sicherheit durch einheitliche Zertifizierungsvorgaben und Zertifizierungen. In diesem Zusammenhang wurde auch der wachsende Zielkonflikt des BSI zwischen Gewährleistung höchster Sicherheit und hoher technischer Fortschrittsgeschwindigkeit deutlich.

Die Themen sichere Identitäten und Digitalisierung werden durch zahlreiche Gesetzesinitiativen unterstützt und damit im nächsten Jahrzehnt noch wichtiger und allgegenwärtiger. Außerdem werden sie durch ein ständig wachsendes Netzwerk verbundener Geräte, eine unglaubliche Rechenkapazität aus der Cloud, den Erkenntnissen aus Big Data und der Intelligenz aus maschinellem Lernen beschleunigt.

Ich freue mich, im Rahmen meiner Tätigkeit beim BSI, diese Veränderung zu gestalten, und wünsche mir für die Zukunft mehr und mehr Botschafterinnen und Botschafter für die Digitalisierung in Deutschland.

Meine ersten Berührungspunkte mit dem BSI hatte ich im Jahr 2010, als ich nach etwa 10 Jahren in der IT-Branche erstmals mit der Bearbeitung von Verschlusssachen (VS) in Berührung kam. Als Chief Information Security Officer (CISO) und Sicherheitsbevollmächtigte beim IT-Dienstleiter der Bundeswehr, der BWI Systeme GmbH, war ich dort insbesondere für die Nutzung zugelassener IT-Produkte im VS-Umfeld zuständig, mit deren Prüfung und Freigabe sich das BSI befasst.

Die Gründung der Allianz für Cyber-Sicherheit (ACS) im Jahr 2013 war dann Startschuss für eine engere Zusammenarbeit mit dem BSI. Für mich stand von Anfang an fest, dass ich dem Netzwerk beitreten würde, um dessen Angebote zu nutzen und gleichzeitig selbst mitgestalten zu können. Als herstellerneutrale Kooperationsplattform besetzt die ACS bis heute eine Schlüsselrolle in der IT-Sicherheit und ist mittlerweile eines der größten Sicherheitsnetzwerke Europas. Der Expertenkreis Cyber-Sicherheit ist eines der Gremien der ACS, in dem ich von Beginn an mitgewirkt habe.

Von 2016 bis 2018 engagierte ich mich beim European Cyber Security Month, der durch seine zahlreichen unterschiedlichen Aktionen rund um IT-Sicherheit eine optimale Möglichkeit für einen thematischen Austausch darstellt. Eine engere Verbindung zum BSI entstand zusätzlich durch meine regelmäßige Teilnahme am Deutschen IT-Sicherheitskongress.

Auch in meiner anschließenden Tätigkeit in der Geschäftsleitung eines vom BSI zertifizierten IT-Sicherheitsdienstleisters und später, nachdem ich mich als Cyber-Sicherheitsberaterin selbständig gemacht hatte, begleiteten mich die Angebote des BSI und ich zertifizierte mich als Cyber Security Practitioner für die Durchführung von Cyber-Sicherheits-Checks.

Nadine Nagel
Leiterin der Abteilung Cyber-Sicherheit für Wirtschaft und Gesellschaft (WG)

Nachdem sich meine Wege mit dem BSI vielfach gekreuzt haben, bin ich nun stolz, selbst Teil dieser Behörde zu sein. Seit April 2020 leite ich die Abteilung „Cyber-Sicherheit für Wirtschaft und Gesellschaft“. Damit verantworte ich nun selbst die Allianz für Cyber-Sicherheit, die Ausrichtung von Events wie den IT-Sicherheitskongress, die Koordination des European Cyber Security Month, den Bürger CERT-Newsletter und vieles mehr.

Jetzt liegt es an mir, gemeinsam mit meinem Team die Angebote des BSI für Bürgerinnen und Bürger sowie die Wirtschaft so weiterzuentwickeln, dass sie auch weiterhin unsere Zielgruppen dabei unterstützen, Informationssicherheit bei jedem Schritt der Digitalisierung mitzudenken. Neben den Betreibern Kritischer Infrastrukturen und der Wirtschaft fokussieren wir uns künftig noch stärker auf den Digitalen Verbraucherschutz. Dabei verbindet uns in der Abteilung stets die Maxime, dass Cyber-Sicherheit eine Gemeinschaftsaufgabe ist, die Staat, Wirtschaft und Gesellschaft verbindet. ■

Lauschabwehr im BSI

High-Tech für die Suche nach elektronischem „Ungeziefer“

Von Uwe Beckert, Referent Lauschabwehr, Joachim Opfer, Leiter des Fachbereichs Vorgaben, Entwicklung und Prüfung von Krypto-, VS- und IT-Sicherheitssystemen, und Dr. Astrid Schumacher, Leiterin des Fachbereichs Informationssicherheitsberatung und Geheimschutz

Schon seit der Antike haben die Menschen aus den verschiedensten Gründen das Bestreben, sich geheime Informationen über ihre Mitmenschen zu verschaffen, zum Beispiel durch Belauschen von vertraulichen Gesprächen. Die Erfindung des Fernsprechers durch Graham Bell und der Funkübertragung durch Guglielmo Marconi machte die riskante persönliche Anwesenheit eines Spions als „Lauscher an der Wand“ überflüssig, der Lauschangriff konnte, nun ohne besonderes Entdeckungsrisiko, aus der Ferne erfolgen.

Im Bereich des staatlichen Geheimschutzes ist die Lauschabwehr fester Bestandteil von Sicherheitskonzepten. Bis zur Gründung des BSI war die beim damaligen Bundesgrenzschutz angesiedelte „Ingenieurgruppe des BMI“ für die Lauschabwehrprüfungen in den Behörden und Ministerien zuständig. Kurz nach der Gründung des BSI wurde diese Einheit dann in das BSI eingegliedert.

Die Aufgabe der Lauschabwehr liegt darin, solche Abhöreinrichtungen - gemeinhin auch als „Wanzen“ bezeichnet - aufzuspüren. Mittels hochspezialisierter Aufklärungssysteme wird im Rahmen einer Lauschabwehrprüfung ein Raum bzw. ein Fahrzeug untersucht. Zu den hochkomplexen Untersuchungsmethoden gehören beispielsweise Hochfrequenzanalyse, Wärmebildanalyse, Halbleiterdetektion, Röntgenanalyse und Endoskopie.

WISSEN, WAS LÄUFT: DER WETTLAUF ZWISCHEN ANGRIFF UND ABWEHR

Seit den Erfindungen von Bell und Marconi hat sich die Abhörtechnik rasant in Richtung Miniaturisierung und Digitalisierung entwickelt. Eine wirksame Lauschabwehr erfordert daher einerseits die genaue Kenntnis der mit fortschreitender Technik immer raffinierteren Angriffsmethoden und andererseits technische Kreativität bei der Weiterentwicklung der Detektionsmethoden. Auch die Abwehr profitiert dabei vom technischen Fortschritt. Detektionsmethoden, die vor 30 Jahren nur theoretisch denkbar waren oder einen unrealistischen Prüfaufwand erfordert hätten, sind heute praxistauglich verfügbar. Die James-Bond-Methode, mit einem kleinen Handdetektor ein verstecktes Abhörgerät im Raum zielstrebig zu orten, ist allerdings für eine ernst zu nehmende Lauschabwehrprüfung noch immer Utopie.

NACH DER WIEDERVEREINIGUNG: DIE ABHÖRAKTIVITÄTEN DES MFS WERDEN OFFENBAR

Im Zuge der Wiedervereinigung erlangte die Lauschabwehr des neu gegründeten BSI Zugang zu den Asservatenkammern des Ministeriums für Staatssicherheit (MfS). Die Analyse der zahlreichen Wanzen brachte interessante Einblicke in die Abhörmethoden eines totalitären Staates. Die erstaunliche Erkenntnis war, dass diese Technik eher „hausbacken“ war und man sich offenbar bei Lauschangriffen gegen die eigenen Bürger auf heimischem Terrain wenig Mühe mit der Tarnung gab.

MINIATURISIERUNG DURCH DIGITALISIERUNG: HIGH-TECH-WANZEN – HEUTE IM SPY-SHOP FÜR WENIG GELD ERHÄLTLICH

Die Digitalisierung begann mit der ersten Mondladung im Jahre 1969, als drei amerikanische Astronauten mit Unterstützung eines 8-bit-Mikrorechners erfolgreich auf dem Mond landeten und wieder zur Erde zurückkehrten. Mit der Zeit hielt diese Neuerung auch in der Abhörtechnik Einzug. War der Einsatz von Abhöreinrichtungen vor etwa 30 Jahren – von den simplen Minispionen für Elektronikbastler einmal abgesehen - noch Geheimdiensten und finanzstarken, kriminellen Organisationen vorbehalten, kamen zu Beginn der 90er Jahre mit dem einsetzenden Fortschritt der Mikroelektronik auch technisch anspruchsvolle und stark miniaturisierte Geräte auf den Markt, die in Spy-Shops für jedermann verfügbar und erschwinglich waren.

Im gleichen Maß wuchs die potenzielle Bedrohung durch Lauschangriffe, der die Lauschabwehr begegnen musste.

LAUSCHABWEHR VOR 30 JAHREN UND HEUTE

Viele Wanzen nutzen Radiowellen als Übertragungsmedium. Ein fester Bestandteil der Lauschabwehrprüfung war und ist daher die Beobachtung des Funkbetriebs im „Äther". War es vor 30 Jahren noch üblich, die Suche auf den Frequenzbereich unterhalb von 1 GHz zu beschränken und in verdächtige Signale „hineinzuhören" (demodulieren), würden heute viele Lauschsender mit dieser Methode unentdeckt bleiben.

Moderne Lauschsender senden auf Frequenzen bis in den hohen Gigahertz-Bereich und nutzen Verschlüsselungs- und digitale Übertragungsverfahren. Manche tarnen ihre Aussendung als Mobilfunksignal (GSM, UMTS, LTE oder 5G), als WLAN- oder Bluetooth-Signal oder sie verstecken sich hinter digitalen Rundfunksignalen (wie DAB und DVBT). Um unter den in großer Zahl im Äther präsenten legalen Sendern dieser Art einen Lauschsender zu erkennen, werden Spezialempfänger und hochkomplexe Signalanalysemethoden eingesetzt, die auch Algorithmen der Künstlichen Intelligenz nutzen.
Eine weitere Entwicklung, mit der die Lauschabwehr Schritt halten muss, ist die immer schnellere Weiterentwicklung der Mobilfunkstandards.

LASER-LAUSCHEN: SCIENCE-FICTION ODER REALITÄT?

Anfang der 90er Jahre kursierten in Fachkreisen Gerüchte über eine neuartige Lauschtechnik: Mit unsichtbaren Laserstrahlen könne man Fensterscheiben abtasten und so aus der Ferne die minimalen Schwingungen, die durch den Schall im Innenraum verursacht werden, hörbar machen. So könne man Gespräche mithören, ohne den Raum je zum Einbau einer Wanze betreten zu müssen.

Mittlerweile ist diese Methode gut untersucht. Das Risiko ist real, und die entsprechende Technik ist kommerziell verfügbar. Folglich musste sich die Lauschabwehr auch dieser Herausforderung durch bauliche Schutzmaßnahmen und die Entwicklung geeigneter Detektoren stellen.

PRÄVENTION DURCH BAULICHEN ABHÖRSCHUTZ

Auch die zunehmende Digitalisierung unserer Arbeitswelt ist eine Herausforderung für die Lauschabwehr: In einem modernen Büro oder Besprechungszimmer mit Smartphone, Tablet, PC, Telefon, Beamer und Videokonferenzanlage, die alle mit Mikrofonen und Kameras ausgestattet sind, gleicht die Lauschabwehrprüfung der Suche nach der Stecknadel im Heuhaufen. Ein wichtiger Bestandteil des Sicherheitskonzepts gegen Lauschangriffe ist daher die präventive Lauschabwehr: Für vertrauliche Gespräche werden besondere Räume eingerichtet, die durch ihre spezielle bauliche Ausgestaltung und Beschränkung der technischen Ausstattung einen erfolgreichen Lauschangriff erschweren und die Lauschabwehrprüfung erleichtern sollen. Der Umzug vieler Ministerien von Bonn nach Berlin bot für die Lauschabwehr im Zusammenhang mit den dortigen Baumaßnahmen die große Chance, die Einrichtung von abhörgeschützten Räumen vom Beginn der Planungen bis zur Inbetriebnahme intensiv zu begleiten und diese schon in der Bauphase regelmäßig zu untersuchen. ■

Mit diesem Artikel möchten wir auch Herrn Volker Fricke gedenken, der seit dem 01.01.1991 zunächst als Referent und seit 2001 als Referatsleiter im jetzigen Referat der Lauschabwehr tätig war. Er hat die Lauschabwehr des BSI maßgeblich vorangebracht und die Arbeit des BSI in allen Veränderungsprozessen aktiv mitgestaltet. Mit seinem Tod am 7.8.2020 haben wir einen ausgewiesenen Fachexperten, einen sehr geschätzten und überaus engagierten Kollegen und Freund verloren.

Malware im Wandel der Zeit

30 Jahre Viren, Würmer und Co.

Von Dr. Merle Hattenhauer und Alexander Härtel, Referat Nationales IT-Lagezentrum, Analysen und Prognosen

80er

DIE WURZELN IN DEN 80ERN

Als das BSI am 1.1.1991 gegründet wurde, hatte die IT-Welt bereits Erfahrungen mit Programmen gemacht, die schädliche Operationen auf Computersystemen ausführen konnten. Bereits 1985 hatte das erste Computer-Virus *GOTCHA* wahr werden lassen, wovor Computerexperten schon Jahre zuvor gewarnt hatten: Das tückische Programm schrieb „Arf, Arf!, *GOTCHA!*“ auf den Bildschirm und löschte Daten von der Festplatte.

Nur ein Jahr später tauchte an amerikanischen Hochschulen mit *BRAIN* das erste Bootsektor-Virus für DOS-Betriebssysteme auf. Austauschstudenten hatten den Schädling eingeschleppt. Er war zwar relativ harmlos, verbreitete sich aber rasend schnell; Grund genug für einige Pioniere, erste Firmen für Antivirensoftware zu gründen. Zugleich begannen Virus-Entwickler damit, systematisch nach Schwachstellen in Computersystemen zu suchen und diese für Schadsoftware-Angriffe auszunutzen.

MICHELANGELO war 1992 der erste Computerschädling, der weltweit breite öffentliche Aufmerksamkeit auf sich zog. Denn im Gegensatz zu einer Vorläufervariante konnte er von der damaligen Antivirensoftware nicht erkannt werden. Auch wenn die tatsächlichen Datenverluste am Ende überschaubar waren, ging die durch die verbreitete mediale Berichterstattung ausgelöste öffentliche Angst vor dem Schädling als *MICHELANGELO*-Hysterie in die Geschichte ein.

95

1995: JETZT GEHT ES RICHTIG LOS

Mit der Markteinführung von Windows 95 brach die Zeit der Makroviren an. Seitdem nutzten Angreifer zunehmend die Funktionalität von Word und Excel, um ausführbare Programmcodes in Dokumenten wie z. B. Tabellen oder Briefen zu hinterlegen. In den zehn Jahren zuvor waren durchschnittlich täglich etwa 30 neue Computerschädlinge bekannt geworden. Zwischen 1995 und 2000 hat sich die Anzahl neuer Schadsoftware-Varianten mehr als verzehnfacht: auf durchschnittlich täglich gut 470 Varianten.

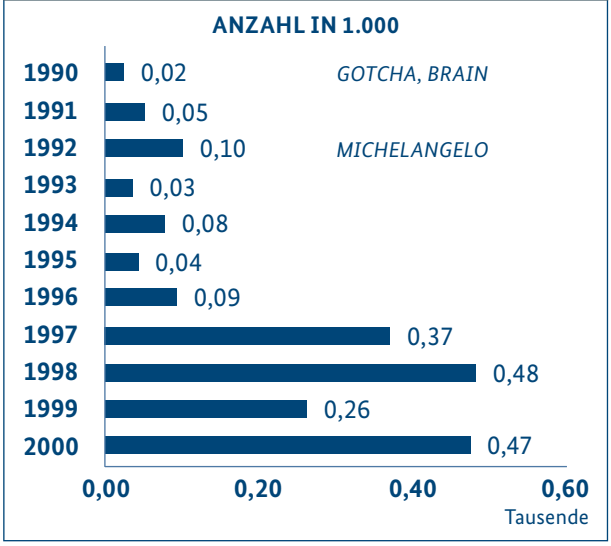
2000

2000: DIE GROSSE ZEIT DER WÜRMER BEGINNT

Ein Computerwurm ist eine Schadsoftware, die sich automatisiert, selbstständig weiterverbreitet. Als das bis dato bösartigste Virus der Computergeschichte ging *LOVELETTER* im Jahr 2000 in die Geschichte ein. Mit der Betreff-Zeile „I love you“ suggerierte es, ein Liebesbrief zu sein, veranlasste viele Empfängerinnen und Empfänger zum Klick auf den Anhang und löschte anschließend alle Dateien mit .jpg, .jpeg, .js, .css und ähnlichen Endungen. *LOVELETTER* verbreitete sich über Outlook selbstständig, explosionsartig weiter. Nach Schätzungen lag der Gesamtschaden bei 5,5 Milliarden Dollar weltweit.

SQL-SLAMMER war 2003 der erste Wurm, der sich gezielt gegen SQL-Server richtete. In einer Stunde infizierte er mindestens 75.000 SQL-Server. In Amerika brachte er so das Geldautomatennetz einer Großbank, Notrufdienste und das Flugverkehrskontrollsystem zum Absturz.

Durchschnittlicher täglicher Zuwachs neuer Malware-Varianten **1990 bis 2000**



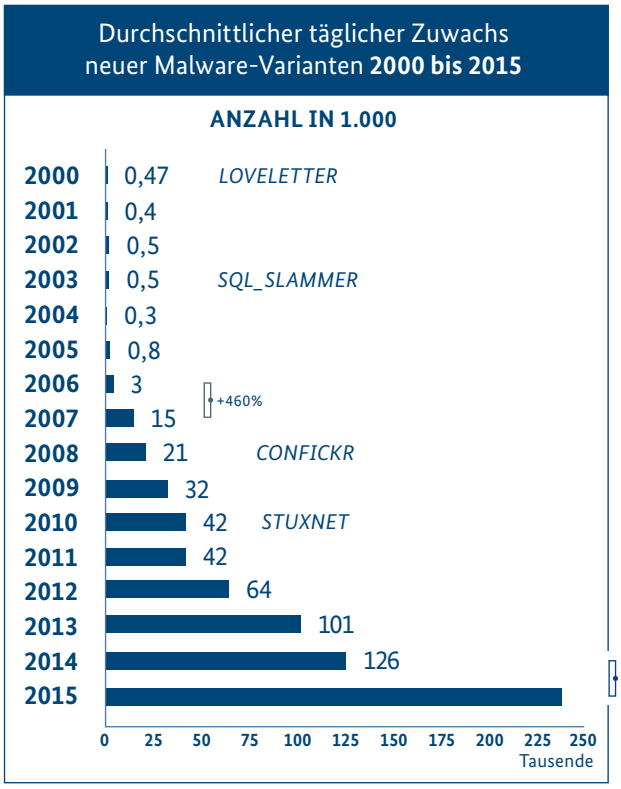
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

2005

2005: CYBERCRIME – VIREN WERDEN ZUR GELDDRUCKMASCHINE

Seit 2005 wächst die Zahl der durchschnittlich täglich bekanntwerdenden Malware-Varianten rasant. Bis 2015 hat sie sich auf 240.000 Varianten pro Tag nahezu verdreihundertfacht. Der stärkste jährliche Zuwachs neuer Malware-Varianten war mit einem Plus von fast 460% gegenüber dem Vorjahr im Jahr 2007 zu verzeichnen und fast vollständig auf Varianten zurückzuführen, die sich gegen das neue Betriebssystem Windows 7

richteten. Trojaner spionierten Passwörter und Identitätsdaten aus, infizierte Rechner wurden von Angreifern zu ferngesteuerten Botnetzen zusammengeschlossen. Während des deutschen Fußball-Sommermärchens 2006 brachten DDoS-Angriffe die Server von Online-Wettbüros zu Fall. Immer stärker wuchs nun die Möglichkeit, mit Cybercrime illegal viel Geld zu verdienen. Im Jahr 2008 verbreitete sich mit *CONFICKR* ein Wurm mit Nachladefunktion weltweit rasend schnell. Immer mehr wandelte sich der Hacker vom imageorientierten Technikspezialisten hin zum profitorientierten Verbrecher.



Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

2010: VIREN WERDEN ZUR WAFFE

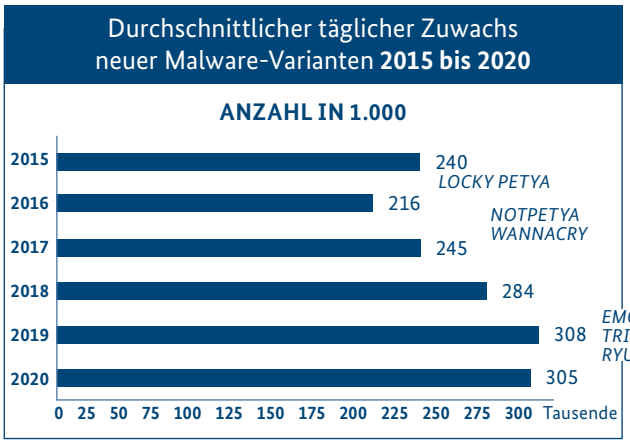
2010 verbreitete sich der Wurm *STUXNET*, der die Zentrifugen der iranischen Urananreicherung zeitweilig außer Betrieb gesetzt hatte, weit über Ländergrenzen hinweg. Damit wurde die Möglichkeit der Sabotage von Kritischen Infrastrukturen mit IT-Mitteln fulminant bestätigt. Zusätzlich wurde Computerspionage zu einem etablierten Mittel der Nachrichtendienste weltweit, wie u. a. Wikileaks 2013 enthüllte.

2015 BIS 2020: RANSOMWARE EVERYWHERE

Das erste Erpresservirus wurde bereits 1989 bekannt. Zahlreiche Nachahmer fand die Idee, Daten auf infizierten Systemen zu verschlüsseln und dann ein Lösegeld zu erpressen, jedoch erst in den letzten fünf Jahren. *LOCKY* und *PETYA* kamen 2016 und 2017 im Anhang von E-Mails als vermeintliche Bewerbungsschreiben auf den PC oder Mac, verschlüsselten Daten und richteten weltweiten Schaden an. Eine bis dahin ungeahnte Verbreitung erreichten Angreifer mit den Ransomwares *NOTPETYA* und *WANNACRY,* indem sie die Schwachstelle EternalBlue in Windows Vista und neueren MS-Betriebssystemen ausnutzten. Schätzungen zufolge wurden allein durch *WANNACRY* mehr als 230.000 Computer weltweit automatisiert infiziert. Die nächste Stufe der Industrialisierung des Cybercrime wurde 2018 mit der Schadsoftware *EMOTET* erreicht. Bis zum Takedown seiner Infrastruktur Anfang 2021 las der Trojaner Outlook-Postfächer aus, exfiltrierte die Daten an die Angreifer und verbreitete sich unter Rückgriff auf bestehende E-Mailkorrespondenz an Kontakte des Opfers weiter. Mit seiner Downloader-Funktionalität war er das Einfallstor für weitere Schadsoftware anderer Angreifergruppen, wie etwa die Spyware *TRICKBOT* oder die Ransomware *RYUK*.

UND WIE GEHT ES WEITER?

Professionelle Angreifer nutzen mehr und mehr die legitimen Werkzeuge von Systemen, die schon die Funktionalitäten mitbringen, die bisher Malware bereitstellte: Persistenz und Verbreitung im internen Netz, Kopieren von Daten u. s. w. Ob eine „Malware“ vorliegt, wird zunehmend von den Unternehmen und deren Definition abhängen: Nutzen sie bestimmte Adminwerkzeuge auch selbst und stufen sie daher nicht als bedrohlich ein? Oder wird beim Fund eines bestimmten Werkzeugs im Netzwerk Alarm ausgelöst?



Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

Weiterhin zeigt sich ein Trend, öffentlich verfügbare Frameworks wie CobaltStrike, Powershell Empire etc. zu verwenden. Malware wird dagegen zunehmend komplexer. Modulare und flexible Softwarearchitektur zeichnen erfolgreiche Malware-Varianten aus. Sie erlauben den Angreifern eine Vielzahl an Funktionalitätsstufen, von Dropper über Loader bis hin zu Backdoors, gezielt und bedarfsgerecht zum Einsatz zu bringen. Diese Abbildung von Funktionalitäten in einzelnen Modulen macht es Angreifern möglich, ihre Malware den sich ändernden Anforderungen leicht anzupassen. Insgesamt zeigt sich eine zunehmende Komplexitätssteigerung sowie eine deutliche Professionalisierung und Industrialisierung bei der Entwicklung und dem Einsatz neuer Malware. Mit welcher Art von Malware das BSI in den nächsten 30 Jahren konfrontiert wird, hängt trotz aller Professionalisierung maßgeblich von der Kreativität der Täter ab. ■

30 Jahre Regierungsnetze

Ein Rück- und Ausblick

Von Olaf Erber, Leiter des Fachbereichs Informationssicherheit der konsolidierten Bundes-Rechenzentren und -Netze

Am 20. Juni 1991 fasste der Deutsche Bundestag den Beschluss zur Vollendung der Einheit Deutschlands, mit der Folge, dass die bisher in Bonn angesiedelten Bundesbehörden auf Berlin und Bonn verteilt wurden. Damit war klar, dass eine leistungsfähige Kommunikationsinfrastruktur geschaffen werden musste, die das räumlich verteilte Arbeiten unterstützt.

Zu dieser Zeit existierte als „Regierungsnetz“ nur das Bundesbehördennetz (BBN) – ein auf den Bonner Raum begrenztes Telefonnetz, das 1994 eilig via ISDN auf Berlin erweitert wurde.

Ab 1993 wurde mit den Planungen für eine moderne Kommunikationsinfrastruktur, dem Informationsverbund Berlin-Bonn (IVBB) begonnen. Die Planungen wurden durch das Bundesministerium des Innern (BMI) geleitet, dort durch die Koordinierungs- und Beratungsstelle in der Bundesverwaltung im BMI, kurz KBSt.. Das BSI war hierbei von Anfang an mit eingebunden, gestaltete die Sicherheitsarchitektur mit und erstellte das IT-Sicherheitskonzept. Dies erfolgte zu dieser Zeit nach dem IT-Sicherheitshandbuch des BSI, der IT-Grundschutz war noch nicht erfunden.

1996: INFORMATIONSVERBUND BERLIN-BONN

Im Jahr 1996 fiel die Entscheidung zum Aufbau des IVBB durch die Deutsche Telekom AG, 1998 begann der Pilotbetrieb, am 1. Januar 1999 der Wirkbetrieb. Das Basisnetz bestand aus Glasfaserringen in Bonn sowie Berlin und

versorgte etwa 100 Standorte. Verbunden wurden die Städte durch einen redundanten Backbone. Als Übertragungstechnik wurde ATM (Asynchronous Transfer Mode) auf SDH-Technik (Synchrone Digitale Hierarchie) eingesetzt, die Bandbreiten betrugen 155 Mbit/s in den Glasfaserringen in Bonn und Berlin sowie 622 Mbit/s zwischen den Städten. Über dieses Netz konnten die angeschlossenen Behörden die lokalen Netze und Telefonanlagen ihrer Liegenschaften verbinden. Darüber hinaus wurden verschiedene Kommunikationsdienste zentral bereitgestellt, wie

- Telefonie und Fax (ISDN)
- E-Mail (X.400 und SMTP)
- Zentrale, gesicherte Internetübergänge
- Verzeichnisdienst
- Videokonferenzen (ISDN)

SICHERHEIT ALS MASSGABE VON BEGINN AN

Das BSI war bei der Konzeption dieser und neuer Dienste stets beteiligt, Sicherheitsmaßnahmen wurden von Anfang an mit umgesetzt, z. B. durchgängige Verschlüsselung im Datenbereich oder Firewalls an den zentralen Netzübergängen.

Über die Jahre wuchs das Netz in Bandbreiten und Anzahl der zentralen Dienste. Bereits 1999 musste die Bandbreite der zentralen Internetübergänge von 2 Mbit/s um zusätzliche 10Mbit/s auf 12 Mbit/s erweitert werden, heute ist es etwa das 3000-fache. Es wurden Einwahllösungen für mobiles Arbeiten geschaffen und Dienste modernisiert.

Im Jahr 2004 wurde die Zuständigkeit für Betrieb und Weiterentwicklung des IVBB per Erlass vom BMI weitgehend auf das BSI übertragen. Der Betrieb selbst verblieb bei der Telekomtochter T-Systems.

2005: ANSTIEG VON SPAM-MAILS ALS HÄRTETEST

Seine erste Feuertaufe hatte der IVBB kurz darauf im Jahr 2005 zu bestehen. Mit dem massenhaften Auftreten von Spam-Mails hatte sich der Mailverkehr quasi über Nacht vervielfacht und die zentralen Mailsysteme fast zum Erliegen gebracht. Nach ersten Sofortmaßnahmen wurden die Mailsysteme aufgerüstet, der interne Mailverkehr vom externen getrennt und eine gestaffelte Spam-Filterung aufgebaut. In Spitzenzeiten lag der Anteil des regulär eingehenden Mailverkehrs bei gerade einmal 1% des Gesamtverkehrs.

Auf Spam folgten Denial of Service Angriffe, insbesondere DDoS-Wellen, die mit immer größeren Bandbreiten auftraten. Durch den Aufbau leistungsfähiger DDoS-Mitigation Systeme konnte größerer Schaden verhindert werden.

Auch technologisch musste der IVBB permanent an sich wandelnde Technologien angepasst werden. ATM wurde als Übertragungstechnik abgelöst, ISDN durch Voice over IP (VoIP) ersetzt. Dies waren jeweils aufwendige, mehrjährige Projekte. Ferner wuchs der IVBB durch Integration des Informationsverbundes der Bundesverwaltung (IVBV), ein Netz das vorwiegend durch Bundespolizei und das Technische Hilfswerk genutzt wurde. Die Zahl der Standorte erhöhte sich enorm auf über 1.000 und diese verteilten sich jetzt auf ganz Deutschland.

AUS DEM IVBB WERDEN DIE NETZE DES BUNDES

In den letzten ca. 5 Jahren wurde der IVBB sukzessive durch die Netze des Bundes (NdB) ersetzt. Die Technik zog in andere Liegenschaften und die Verbindung zwischen Berlin und Bonn, der sogenannte WAN-Backbone, wurde durch das von der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) betriebene Kerntransportnetz (KTN) des Digitalfunks ersetzt.

Seit etwas über zwei Jahren wird der Betrieb der NdB durch die BDBOS verantwortet, die hierbei vom BSI unterstützt wird. Das BSI bleibt weiterhin für die IT-Sicherheit zuständig. Die genaue Aufteilung der Zuständigkeiten wird durch eine Verwaltungsvereinbarung geregelt.

Die Pandemie sorgte im letzten Jahr für die nächste Feuertaufe. Die Mitarbeiter der Behörden wechselten ins Home-Office, die Verkehrsströme wechselten von „innen nach außen“ auf von „außen über innen nach außen“. Hinzu kam der stark ansteigende Bedarf nach Videokonferenzlösungen. Durch eine gemeinsame Kraftanstrengung von BDBOS und BSI konnte auch diese Situation bewältigt werden.

UND WIE GEHT ES WEITER?

Durch die IT-Konsolidierung in der Bundesverwaltung steigt der Bedarf an Bandbreite und auch an IP-Adressraum weiter an. NdB muss auf IPv6 migriert und die Anschlusstechnik muss modernisiert werden. Im Rahmen der Netzstrategie 2030 des BMI soll NdB zum Informationsverbund der öffentlichen Verwaltung (IVÖV) weiterentwickelt werden und weitere Netze der Bundesverwaltung in einer einheitlichen Struktur integrieren. Es bleibt spannend! ■

Weitere Informationen:

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/oeffentliche-verwaltung_node.html

Ausbildung im BSI

Damals und heute

Von Christine Hau (Ausbildung im BSI 1995 - 1998), Referat Zertifizierung nach Technischen Richtlinien, und Antonia Gössel (Ausbildungsabsolventin 2020), Geschäftszimmer Abteilung Standardisierung, Zertifizierung und Sicherheit von Telekommunikationsnetzen

Wenn man die Ausbildung im BSI von vor 25 Jahren mit der heutigen vergleicht, stellt man doch so einige Unterschiede fest. Daher würden wir Ihnen gerne mehr darüber erzählen.

Nach Abschluss der Höheren Handelsschule im Jahr 1995 bewarb ich mich beim Technischen Hilfswerk (THW) in Bonn auf eine Ausbildungsstelle als Fachangestellte für Bürokommunikation. Am Tag des Einstellungstest waren nicht nur die Ausbildungsleiter des THW vor Ort, sondern auch eine Mitarbeiterin des BSI. Diese erklärte uns, dass es seit 1991 eine neue Behörde namens Bundesamt für Sicherheit in der Informationstechnik gab, die nun ebenfalls auf der Suche nach ihren ersten Auszubildenden sei.

Im September 1995 begann meine Ausbildung im BSI. Zunächst verlief die Ausbildung etwas holprig, da das BSI zum ersten Mal eine Auszubildende hatte und die Kolleginnen und Kollegen in den Referaten nicht wirklich etwas mit mir anzufangen wussten. Dank eines Ausbildungsplanes spielte sich jedoch alles recht schnell ein. Berufsbegleitend hatte ich Unterricht im Bundesverwaltungsamt (BVA) in Köln sowie in der Berufsschule. Während sich der Unterricht im BVA mehr auf die Rechte der öffentlichen Verwaltung, wie z. B. Beamtenrecht, Tarifrecht, Besoldungs- und Urlaubsrecht konzentrierte, übernahm die Berufsschule eher kaufmännische Fächer, wie Volks- und Betriebswirtschaftslehre, Finanzmathematik und Wirtschaftsenglisch sowie damals sogar noch Stenografie.

Im August 1998 beendete ich meine Ausbildung erfolgreich und wurde vom BSI übernommen.

Ich verblieb zunächst, wie auch schon kurz vor Ende meiner Ausbildung, im Referat Z5 und war dort in das Pilotprojekt „DOMEA“ involviert, das heute besser als „CAZE“ bekannt ist.

Nur durch einen Zufall wurde ich nach etwa 2 Jahren zur Beauftragten für das Internet – sowohl für das Intranet, als auch für den externen Internetauftritt des BSI.
In dieser Zeit habe ich sehr viele Fortbildungen besucht und nach etwa einem Jahr meinen „Professionellen Webmaster“ gemacht. Nach weiteren 4 Jahren begleitete ich unter anderem die Koordinierung des BSI-Kongresses. Eine sehr große und verantwortungsvolle Aufgabe, die mir jedoch großen Spaß gemacht hat. Mit der Einstellung des damaligen Abteilungsleiters Bernd Kowalski, wechselte ich im Jahr 2005 in sein Geschäftszimmer.

Seit nunmehr 10 Jahren habe ich das Gefühl endlich angekommen zu sein. Ich bin im Referat Technische Richtlinien tätig, und die Aufgaben, insbesondere im Bereich der Technischen Richtlinien, liegen mir sehr.

Am 01. September 2020 feierte ich tatsächlich schon mein 25. Dienstjubiläum – es ist Wahnsinn, wie die Zeit vergeht. Abschließend kann ich jedoch ganz ehrlich sagen, dass es in den vergangenen 25 Jahren nicht einen Tag gab, an dem ich nicht gerne ins Amt gekommen bin.

„In nur drei Jahren hat sich im BSI so viel verändert, dass ich sehr gespannt auf alles Weitere bin.“

Als ich 2017 im BSI meine Ausbildung in der Abteilung Zentrale Aufgaben begann, war ich 18 Jahre alt und hatte kurz zuvor mein Abitur gemacht. Ich hatte keinerlei behördliche Berufserfahrung und wenig Ahnung von dem, was mich erwarten würde.

In meiner ersten Woche verschaffte ich mir einen Überblick über den Aufbau des BSI. Zu den Highlights der Woche gehörte mein erstes Treffen mit Herrn Schönbohm und der Besuch im Haus der Geschichte, durch den ich die Ausbildungsjahrgänge vor mir kennenlernen konnte.

Zwei Wochen nach der Eingewöhnungsphase begann die dienstbegleitende Unterweisung im BVA (Bundesverwaltungsamt) und kurz darauf der Berufsschulunterricht im LEB (Ludwig-Erhard-Berufskolleg). Von da an wechselte ich stetig zwischen meinen praktischen Einsätzen im BSI, meinem theoretischen Unterricht und diversen Schulungen.

Während meinen praktischen Einsätzen im BSI durfte ich viele Stationen durchlaufen – von den Referaten der Abteilung für Zentrale Aufgaben über verschiedene Geschäftszimmer bis hin zu einzelnen Fachreferaten. Je nach Einsatz musste ich die Liegenschaft wechseln. Zu Beginn meiner Ausbildung hatte das BSI drei Liegenschaften, zum Ende hin waren es fünf (ohne die Verbindungsbüros und die sich noch im Bau befindende Liegenschaft mitzuzählen). Kurz vor meinem Abschluss verkomplizierte die Corona-Pandemie die Ausbildungsabläufe. Die Vorbereitungen für meine Abschlussprüfung fanden online statt, die Prüfungen konnten jedoch unter Beachtung von Hygienemaßnahmen geschrieben werden. Eine Abschlussfeier konnte bedauerlicherweise bis heute nicht stattfinden, da eine Umsetzung einfach nicht möglich ist. Mein Abschlusszeugnis musste mir zugeschickt werden. Nach meiner Ausbildung begann ich, im Geschäftszimmer der Abteilung Standardisierung, Zertifizierung und Sicherheit von Telekommunikationsnetzen zu arbeiten.

Zusammenfassend lässt sich sagen, dass ich in drei Jahren Ausbildung einen Büro- bzw. Liegenschaftswechsel, zwei BSI-Umorganisationen und zwei Dienstreisen (u. a. nach Berlin) erlebt habe. Ich konnte viel Erfahrung sammeln und viele interessante und nette Menschen kennenlernen. Viele davon haben einen bleibenden Eindruck bei mir hinterlassen.

In nur drei Jahren hat sich im BSI so viel verändert, dass ich sehr gespannt auf alles Weitere bin. ■

Interessante Aufgaben, nette KollegInnen, sicherer Job

30 Jahre im BSI

Nach erfolgreichem Abschluss als Diplom Ingenieur (FH) für Nachrichtentechnik, las Andreas Kirchgässner 1990 eine Stellenausschreibung von einer neuen Behörde - dem Bundesamt für Sicherheit in der Informationstechnik. „Das roch nach Pionierarbeit“, so der geborene Essener. Er war sofort Feuer und Flamme. Das Bewerbungsgespräch fand in einer alten Villa in Bonn-Mehlem statt. Insider nannten die Liegenschaft „Das kryptografische Dorf“, mit vielen Fluren voller Labore, technischem Flair und Laborleitern in weißen Kitteln.

DER ERSTE ARBEITSTAG

Nach seiner Einstellung wurde Andreas Kirchgässner erst einmal in die organisatorischen Grundlagen eingeführt und ihm die Lochkarte für die Zeiterfassung übergeben. Er erinnert sich noch gut daran, wie ihn sein damaliger Kollege, ein hochgewachsener, schlanker Mann in einem weißen Kittel, ins Lager für die erste Arbeitsausstattung führte. Mit Bleistift, Locher und Radiergummi bezog Andreas Kirchgässner sein erstes Büro. Heute sei das Onboarding-Konzept ausgereifter und neben Schreibutensilien bekommt man auch noch sein wichtigstes Werkzeug - einen Laptop. Doch Computer gab es damals noch nicht. Aber ein graues Wählscheibentelefon hatte er. An seine erste Durchwahl erinnert er sich der Angestellte bis heute.

PIONIERARBEIT IN DER ERSTEN IT-SICHERHEITSBEHÖRDE

Schnell konnte Andreas Kirchgässner in die Materie einsteigen. Die Zusammenarbeit in seinem Referat „Verschlüsselungssysteme“ in der Abteilung „Technische Sicherheit“ klappte gut und er war überrascht über die Kollegialität im BSI. „Schließlich befand ich mich doch in einer Behörde“ sagt er lachend. Die Arbeit gestaltete sich damals allerdings ganz anders als heute. Im Vergleich zu heute wirke es, „als hätte man in einem Museum gearbeitet“: Schreibmaschinen und Fernschreiber waren üblich, die Labore waren Werkstätten mit Werkzeugen, Messgeräten und Lötstationen. Eine seiner ersten Aufgaben war es, ein Evaluierungskonzept für Verschlüsselungsgeräte zu erstellen, das im Laufe der Jahre immer an die neusten technischen Standards angepasst wurde.

DIE ARBEIT HEUTE

Heute ist das BSI von damals etwa 250 auf mittlerweile 1300 Mitarbeitende angewachsen und einige Liegenschaften sind hinzugekommen. Andreas Kirchgässner schaut mit Ehrfurcht darauf, was aus der „kleinen Behörde“ in Bonn-Mehlem geworden ist, in der der Präsident auf demselben Flur sein Amt führte. Er beschreibt das BSI als „Inselgruppe mit Brücken und Wegen“, die durch die Kooperation der Kolleginnen und Kollegen verbunden ist. „Aber vor allem: Das BSI ist eine Community. Eine Gemeinschaft aus vielen netten, interessierten Menschen mit dediziertem Fachwissen, aber auch mit Persönlichkeit“. ■

> „Das BSI ist ein besonderer Arbeitgeber. Viele, die hier arbeiten, bleiben dem Bundesamt lange Jahre treu. Andreas Kirchgässner, ein BSI-Urgestein, arbeitet seit der ersten Stunde im BSI.“

Gesucht:

Digitale Talente

(w/m/d)

an den Standorten Bonn und Freital

Scannen und bewerben!

bsi.bund.de/jobs

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

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

Was Sie dafür mitbringen: Ein abgeschlossenes Studium in den Fachrichtungen Informatik, Wirtschafts- oder Verwaltungsinformatik, IT-Sicherheit oder IT-Management bzw. einen Abschluss aus einem vergleichbaren Fachbereich gepaart mit einschlägiger Berufserfahrung in der IT-Sicherheit sowie Engagement für spannende Themen der Cyber-Sicherheit.

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

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

30 Jahre BSI – 30 Jahre Digitalisierung

1991

D-Netz

Geburt des WWW

1993

Präsident Dr. Dirk Henze

Gründung des BSI unter Dr. Otto Leiberich

1994

Common Criteria 1.0

1996

Einführung des IT-Grundschutz

CERT Computer Emergency Response Team

1996

IVBB

1999

„Jahr 2000-Problem“

2000

LoveLetter-Wurm

2001

BSI für Bürger

2002

Zentraler IT-Sicherheitsdienstleister des Bundes

2003

Elektronischer Reisepass

2005

Präsident Dr. Udo Helmbrecht

2007

iPhone

Zeus

2009

Präsident Michael Hange

Novellierung BSI-Gesetz

2010

Stuxnet

2010

Elektronischer Personalausweis

2011

- Elektronische Gesundheitskarte
- Cyber-Abwehrzentrum
- Cyber-Sicherheitsstrategie des Bundes

2012

- IT-Sicherheitsgesetz tritt in Kraft

2013

- NSA-Affäre

2015

- Gründung Allianz für Cyber-Sicherheit (ACS)

2016

- Smart Meter Gateway
- Zerschlagung der Bot-Infrastruktur Avalanche
- Präsident Arne Schönbohm

2017

- 5G
- 2. BSI-Dienstsitz in Freital
- Nationales Verbindungswesen

2017

- Ransomware WannaCry

2018

- Digitaler Verbraucherschutz
- NIS-Richtlinie
- Modernisierung des IT-Grundschutz

2018

- Emotet

2019

- Künstliche Intelligenz
- Cyber-Angriff auf Uniklinik
- Deutsche EU-Ratspräsidentschaft
- Corona-Warn-App
- ACS: über 4.000 Teilnehmer
- 1. Cyber Security Directors' Meeting
- 1.000 Mitarbeitende

2019

- #Collection 1
- Netze des Bundes

2020

- BSI *17. Deutscher IT-Sicherheitskongress*
- und BSI-Jubiläum über 8000 Teilnehmende
- Neuer BSI-Standard 200-4

2021

Weitere Informationen:

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

Viel passiert bei KRITIS

Von den Anfängen des Fachbereichs

von Isabel Münch, Christina Börner und Holger Siebentritt, Fachbereich Cyber-Sicherheit für Kritische Infrastrukturen

Exemplarisch für die rasante Entwicklung des BSI in den letzten dreißig Jahren ist die Geschichte des KRITIS-Fachbereichs, der sich mit der IT-Sicherheit in Kraftwerken, Kliniken und anderen Kritischen Infrastrukturen befasst.

EU-KOMMISSION ERKENNT DIE BEDEUTUNG DER KRITISCHEN INFRASTRUKTUREN

1995 stellte die Referatsleiterin Marit Blattner-Zimmermann das topaktuelle Thema „Schutz Kritischer Infrastrukturen“ im BMI vor, das gerade in einem EU-Workshop in Brüssel heiß diskutiert worden war. Die Diskussion fokussierte sich auf das Thema „Schutz Kritischer Infrastrukturen unter IT-Aspekten“, denn allen war klar, dass Kraftwerke und andere wichtige Anlagen auch durch Computerviren oder die Verwendung schadhafter Hardware lahmgelegt werden könnten. Der Automatisierungsgrad in diesen Anlagen war seinerzeit allerdings noch vergleichsweise gering. Marit Blattner-Zimmermann „promotete“ das neue Thema unter der Bezeichnung KRITIS mit Verve im BMI und machte es in zahlreichen Gremien gewissermaßen „politisch hoffähig“.

Die Kolleginnen und Kollegen von BMI und BSI brachten sich auf europäischer Ebene gemeinsam in die internationale „Szene“ ein. Zudem gab es einen intensiven Austausch mit den USA, wo das Thema „CIP“ (Critical Infrastructure Protection) bereits seit zwei oder drei Jahren

von der FEMA (Federal Emergency Management Agency, eine heute dem Department of Homeland Security nachgeordnete Behörde) behandelt worden war. Es gab auch Kontakte zu CIA und NSA, die ebenfalls begannen, sich über den Schutz der heimischen Infrastrukturen Gedanken zu machen.

So entwickelte sich in der zweiten Hälfte der 90er Jahre das KRITIS-Thema international auf politischer Ebene weiter. Auch in Deutschland fanden erste Stabsrahmenübungen statt, die sich mit CIIP (Critical Information Infrastructure Protection) befassten.

GRÜNDUNG EINES KRITIS-REFERATS IM BSI

Marit Blattner-Zimmermann wechselte im Dezember 1997 zum BSI, ihr Kollege Joachim Weber folgte ihr im Januar 1998 und übernahm den Aufbau des neu gegründeten KRITIS-Referats. Vor dem Hintergrund der Ereignisse vom 11. September 2001 rückten mögliche Angriffe auf Kritische Infrastrukturen weiter in den Fokus.

DIE ERSTEN KRITIS-SEKTORSTUDIEN

Sieben KRITIS-Studien mit einheitlicher Struktur wurden bei externen Dienstleistern in Auftrag gegeben. Im Zusammenhang mit diesen „Sektorstudien“ wurden – in Anlehnung an die US-amerikanische Einteilung – die neun bis heute verwendeten KRITIS-Sektoren mit ihren Branchen definiert. Durch einen arbeitsintensiven Kraftakt konnten die – je Sektor 300 bis 500 Seiten starken – Studienergebnisse bereits nach wenigen Monaten vorgelegt werden.

Wichtigstes Ergebnis der Auswertung der Sektorstudien war eine „Giftliste“ – eine insgesamt 330 Punkte umfassende Liste der identifizierten Schwachstellen, die in einem Panzerschrank sicher verwahrt wurde.

Nationaler Plan
zum Schutz der Informationsinfrastrukturen

NATIONALER PLAN ZUM SCHUTZ DER INFORMATIONSINFRASTRUKTUREN (NPSI)

Der hieraus abgeleitete Handlungsbedarf führte 2005 zur Entwicklung des Nationalen Plans zum Schutz der Informationsinfrastrukturen (NPSI), der unter anderem den Aufbau eines „Krisenreaktionszentrums IT“ im BSI vorsah.

Das 2004 gegründete Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) wurde zuständig für den physischen Schutz Kritischer Infrastrukturen und im BMI wurde das Referat „Schutz Kritischer Infrastrukturen“ gegründet.

Die Weiterentwicklung des NPSI resultierte 2007 im Umsetzungsplan KRITIS, einer Sammlung von Empfehlungen zum Schutz Kritischer Infrastrukturen. Mit dem Umsetzungsplan KRITIS wurden die strategischen Ziele Prävention, Reaktion und Nachhaltigkeit des NPSI für den Bereich der Kritischen Infrastrukturen ausgestaltet.

UP KRITIS

KRITIS-STRATEGIE UND UP KRITIS

Im Juni 2009 verabschiedete das Bundeskabinett die Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Sie thematisiert Risiken und Gefährdungen für Informationsinfrastrukturen, denen insbesondere durch die verstärkte Zusammenarbeit öffentlicher Stellen mit den überwiegend privatwirtschaftlichen KRITIS-Betreibern begegnet werden soll.

Die länderübergreifende Krisenmanagementübung LÜKEX befasste sich Ende 2011 mit zielgerichteten Angriffen auf IT-Infrastrukturen. Sie war ein wichtiger Meilenstein, um auf das Thema KRITIS und die entscheidende Rolle der IT-Sicherheit und des BSI aufmerksam zu machen.

Die aus dem Umsetzungsplan KRITIS hervorgegangene öffentlich-private Zusammenarbeit zum Schutz Kritischer Infrastrukturen verwendet seit 2014 die Bezeichnung „UP KRITIS“ als Eigennamen. Ende 2020 waren mehr als 700 Organisationen Teilnehmer im UP KRITIS.

KRITIS BEKOMMT EINE GESETZLICHE GRUNDLAGE

2015 trat das IT-Sicherheitsgesetz in Kraft und eine neue Ära des Schutzes Kritischer Infrastrukturen in Deutschland begann, die vom BSI als Aufsichtsbehörde über Informationssicherheit maßgeblich gestaltet wird.

2016 war aus dem KRITIS-Referat ein Fachbereich mit etwa 30 Mitarbeiterinnen und Mitarbeitern unter der Leitung von Isabel Münch geworden.

Im Frühjahr 2021 ist das IT-Sicherheitsgesetz 2.0 verabschiedet worden. Für KRITIS wird dies einige Erweiterungen mit sich bringen, wie die Verpflichtung für KRITIS-Betreiber, Systeme zur Angriffserkennung einzusetzen. Die mittlerweile mehr als 50 im KRITIS-Fachbereich WG 1 Beschäftigten erwarten gespannt die neuen Aufgaben. ■

Weitere Informationen:

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

https://www.kritis.bund.de

Das BSI geht in die Fläche

Ein Resümee der verstärkten regionalen Präsenz des BSI

Die Präsenz in der Fläche stand in den Gründungsjahren des BSI nicht auf der Agenda. Erst mit der wachsenden Bedeutung des Themas IT-Sicherheit im Zuge der voranschreitenden Digitalisierung erfuhr der Aspekt der Kooperation – auch im föderalen Verbund – einen Bedeutungszuwachs.

Horst Samsel:
Leiter der Abteilung Beratung für Bund, Länder und Kommunen im BSI

■ **Horst Samsel:**
Das BSI blickt schon auf eine längere Zusammenarbeit mit den Ländern zurück, zum Beispiel bei der gemeinsamen Durchführung von Geheimschutztagungen. Die Zusammenarbeit gründet sich grundsätzlich auf Artikel 91c GG und den darauf aufbauenden IT-Staatsvertrag zwischen Bund und Ländern. Dieser bildet die Grundlage der Zusammenarbeit bezüglich der IT in der Verwaltung von Bund und Ländern, die in der Praxis im Rahmen des IT-Planungsrates und seiner Arbeitsgruppen, wie der AG Informationssicherheit (AG InfoSic), erfolgt. Hier ist das BSI seit 2013 aktiv.

■ **Stefanie Euler:**
2016 habe ich die AG InfoSic mit den Vertretern aus Bund und Ländern das erste Mal kennengelernt. Wir unterstützen den Vertreter des Bundes und die AG InfoSic bei der Umsetzung der politischen Vorgaben des IT-Planungsrates. Unter anderem wirkte das BSI aktiv an der initialen Informationssicherheitslinie der öffentlichen Verwaltung 2013, deren Fortschreibung 2019 und der jeweiligen Umsetzungsplanung mit. Mit der Leitlinie wurde zwischen Bund und Ländern ein verbindliches Mindestsicherheitsniveau der IT-gestützten, ebenenübergreifenden Zusammenarbeit in der Verwaltung vereinbart.

Fabienne Tegeler:
Leiterin des Referats Nationales Verbindungswesen

■ **Fabienne Tegeler:**
Ich erinnere mich noch an den ersten Besuch der Staatssekretäre der Länder-Arbeitsgruppe „Cybersicherheit“ als Gremium der Innenministerkonferenz im Jahr 2012. Damals stand bereits ein Austausch mit dem BSI auf dem Plan. Im Rahmen der zweiten Sitzung stand damals bereits ein Austausch mit dem BSI auf dem Plan. Sehr eng wurde der Austausch aber erst ab 2017 – auch im Lichte der EU-Richtlinie zur Netzwerk- und Informationssicherheit.

Stefanie Euler:
Leiterin des Referats Informationssicherheitsberatung für Länder und Kommunen

NEUE GRUNDLAGEN FÜR DIE BUND-LÄNDER-ZUSAMMENARBEIT

Horst Samsel:
Durch die Erweiterung des BSI-Gesetzes erlangte das BSI 2017 auch die rechtliche Grundlage, die zuständigen Stellen der Länder auf deren Ersuchen in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik zu unterstützen und technische Expertise zur Verfügung zu stellen.

- **Stefanie Euler:**
  Auch die Cyber-Sicherheitsstrategie für Deutschland der Bundesregierung aus dem Jahr 2016 setzte sich zum Ziel, eine leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur zu schaffen, und betonte die Stärkung der Bund-Länder-Zusammenarbeit.

- **Fabienne Tegeler:**
  Das war auch der Ausgangspunkt für das Nationale Verbindungswesen. Die Geschichte des Verbindungswesens im BSI reicht zurück ins Jahr 2012, als die erste Verbindungsperson zum Bundeskriminalamt nach Wiesbaden entsandt wurde. Auf Basis der guten Erfahrungen haben wir diese Idee dann im Jahr 2017 größer gedacht und den Aufbau von regionalen Verbindungsstellen an verschiedenen Standorten in Deutschland vorangetrieben.

- **Horst Samsel:**
  Damit ging das BSI erstmals stärker in die Fläche. Vorbild hierfür war auch die „Action territoriale“ unserer französischen Partnerbehörde ANSSI. Der baden-württembergische Innenminister Thomas Strobl hat es bei der Eröffnungsfeier mit den schönen Worten umschrieben, dass für ihn „ein sicherheitspolitischer Traum in Erfüllung gehe“. Besser hätten wir es nicht umschreiben können. Mittlerweile haben wir mit elf von 16 Ländern Absichtserklärungen geschlossen und zur Umsetzung gebracht.

MEHRWERT FÜR DIE LÄNDER

- **Fabienne Tegeler:**
  Die Frage nach dem Mehrwert für die Länder wurde bereits im Jahr 2017 in den Sitzungen der Bund-Länder-Gremien intensiv diskutiert. Das BSI verfügt als IT-Sicherheitsdienstleister für die Bundesverwaltung über ein umfassendes Produkt- und Dienstleistungsportfolio und ein breites Erfahrungswissen in der Umsetzung von IT-Sicherheitsstandards.

- **Horst Samsel:**
  Bilaterale Sondierungsgespräche mit nahezu allen Ländern waren ein wichtiger Ausgangspunkt für unsere Arbeit. Hier wurde deutlich, dass die Mehrzahl der

Länder von der Expertise des BSI stärker profitieren möchte. Als BSI verfolgen wir einen kooperativen und komplementären Ansatz. Das heißt konkret, wir arbeiten auf Augenhöhe zusammen und unterstützen mit unserer Fachexpertise in den Bereichen, in denen ein Land Unterstützung benötigt. Zugleich profitiert auch das BSI von den Erfahrungen und den Informationen aus der Zusammenarbeit mit den Ländern. Es war interessant zu sehen, wie unterschiedlich die Länder das Thema Informationssicherheit innerhalb der Verwaltungen adressieren.

■ **Stefanie Euler:**
Mit der Gründung der Sicherheitsberatung für Länder und Kommunen im Jahr 2019 erhielt das BSI die Möglichkeit, in erste Pilotprojekte mit den Bundesländern zur ISMS-Beratung einzusteigen, die Herausforderungen zur Umsetzung von Informationssicherheit in Kommunen kennenzulernen und aktiv unsere neu gewonnenen Erkenntnisse in die Beratung zu Sicherheitsanforderungen in ebenenübergreifende Verfahren einzubringen.

■ **Horst Samsel:**
Auf politischer Ebene zeigte sich der Wille zu einer engeren Bund-Länder-Zusammenarbeit im Bereich IT-Sicherheit unter anderem im Beschluss der 206. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder im Jahr 2017.

Das BSI wurde hier mit seiner anerkannten Kompetenz und seinen Ressourcen besonders herausgestellt. Es gilt nun, diesen Beschluss mit rechtlichen Grundlagen zu untermauern, um das BSI in die Lage zu versetzen, die Kooperation weiter zu vertiefen. Das BSI kann in diesem Zusammenhang auch eine stärkere Bündelungs- und Koordinierungsfunktion wahrnehmen.

KOOPERATIONSVEREINBARUNGEN MIT DEN LÄNDERN

■ **Fabienne Tegeler:**
Die Zusammenarbeit zwischen den Bundesländern und dem BSI wird in den kommenden Monaten in verbindlichen Kooperationsvereinbarungen fixiert. Wir haben hierfür gemeinsam ein Muster erarbeitet, das nun die Grundlage für die Weiterentwicklung der bilateralen Zusammenarbeit mit den Ländern bildet.

■ **Stefanie Euler:**
Zur Vertiefung der Zusammenarbeit auf operativer Ebene erarbeiten wir derzeit skalierbare und praxisorientierte Arbeitshilfen zur Unterstützung bei der Umsetzung von IT-Grundschutz, gerade für kleinere Behörden.

■ **Horst Samsel:**
Mit den neuen Standorten in Saarbrücken und in Freital geht das BSI jetzt weiter in die Fläche. Einen aktuellen Schwerpunkt nimmt die Stärkung und Intensivierung der Informationssicherheitsberatung bei der Digitalisierung von Verwaltungsleistungen der öffentlichen Verwaltung und der Justizverwaltung sowie im elektronischen Rechtsverkehr ein. Diese und weitere wichtige Aufgaben übernimmt neben anderen Beratungsaufgaben das neu eingerichtete Fachreferat BL13 „Informationssicherheitsberatung (Standort Sachsen)“.

■ **Stefanie Euler:**
Gemeinsam mit den Ländern und den Kommunalen Spitzenverbänden als Multiplikatoren für die Kommunen möchten wir das ganzheitliche Sicherheitsniveau in Deutschland auf allen Ebenen stärken.

■ **Fabienne Tegeler:**
Dazu müssen Bund und Länder auch gemeinsam an der Weiterentwicklung der Cyber-Sicherheitsarchitekturen arbeiten, um als föderaler Staat im Bereich der Cyber-Sicherheit handlungsfähig zu bleiben. Dass die Länder sich einen weiteren Ausbau des Verbindungswesens wünschen, zeigt, dass wir an einem Strang ziehen.

■ **Horst Samsel:**
Für mich ist klar, dass die Gestaltung von Cyber-Sicherheit in der Digitalisierung nur durch einen gemeinsamen Ansatz von Bund und Ländern zum Erfolg führen kann. Gefährdungen der Cyber-Sicherheit machen an Bund-Länder-Grenzen nicht halt. Wenn wir wirksam Cyber-Sicherheit in Deutschland gewährleisten wollen, müssen wir eng zusammenarbeiten und Fähigkeiten, Wissen und Ressourcen bündeln. ■

Weitere Informationen:

https://www.bsi.bund.de/DE/Das-BSI/BSI-Standorte/Nationales-Verbindungswesen/nationales-verbindungswesen_node.html

BSI vor Ort

Standorte / Stützpunkte

Verbindungsstellen

30 Jahre Krypto-kompetenz im BSI

Kryptographie und Kryptosysteme im Wandel der Zeit

Von Prof. Dr. Werner Schindler, Leiter des Referats Prüfung von Kryptoverfahren, Bernd Schweda, Leiter des Referats Sichere stationäre VS-IT – Technologiebereich I und Stephan Wenzel, Leiter des Referats Sichere stationäre VS-IT – Technologiebereich II

Kryptographie und Kryptotechnik gehörten von Anfang an zu den Kernkompetenzen des BSI. Begleiten Sie uns auf einer Zeitreise über 30 Jahre Kryptographie und Kryptotechnik.

WIE (IM BSI) ALLES BEGANN

Kryptographie und Kryptotechnik sind eng miteinander verbunden, da letztendlich nur eine Kombination aus starken kryptographischen Algorithmen und angriffsresistenten Sicherheitsarchitekturen IT-Sicherheit garantieren kann. Von Beginn an befanden sich die Aufgabenbereiche Kryptographie und Kryptotechnik gemeinsam in Bonn-Mehlem, wenngleich anfangs noch in zwei getrennten Abteilungen. Die Anfangsjahre waren von einem starken personellen Zuwachs an jungen Kolleginnen und Kollegen geprägt, vor allem aus den Bereichen Mathematik und Ingenieurwissenschaften. Seit fast 20 Jahren ist die Kryptokompetenz in einer Abteilung gebündelt.

KRYPTOGRAPHIE IM BSI: WANDEL DER AUFGABEN

Mehr als 2000 Jahre lang war Kryptographie vor allem eine Domäne des Militärs und der Nachrichtendienste. Als das BSI 1991 gegründet wurde, befand sich die Kryptographie im Übergang von einer geheimen zu einer öffentlichen Wissenschaft. 1981 hatte die erste große internationale Kryptographietagung stattgefunden, und einige Universitäten boten erste Vorlesungen an. Die Kryptographiereferate im BSI befassten sich anfangs fast ausschließlich mit mathematischer Kryptoanalyse. Ihre Aufgabe bestand im Wesentlichen darin, kryptographische Algorithmen zu entwickeln und zu evaluieren, die in VS-IT-Produkten (VS = Verschlusssache) eingesetzt wurden. Über den Standort Mehlem hinaus existierte kaum eine Vernetzung im BSI. Typische Angriffsszenarien gingen normalerweise davon aus, dass Verschlüsselungsgeräte von sicherheitsüberprüftem Personal in gesicherten Umgebungen bedient wurden (etwa im Auswärtigen Amt, in einem Botschaftsgebäude oder einem militärischen Sicherheitsbereich). Ziel des Angreifers war es, Chiffrate auf einer öffentlichen, ungesicherten Leitung abzufangen und zu entziffern. Es galt also sicherzustellen, dass die verwendeten kryptographischen Algorithmen dies nicht zuließen.

Die rasante Verbreitung von Internet und Chipkarten hat das Portfolio der kryptographischen Themengebiete deutlich erweitert. In der zweiten Hälfte der 90er Jahre wurden die sogenannten Seitenkanalangriffe entdeckt, die auch heute noch eine wichtige Rolle spielen. Die Grundidee besteht darin, z. B. Laufzeitunterschiede, den Stromverbrauch oder die elektromagnetische Abstrahlung auszunutzen, um daraus den kryptographischen Schlüssel zu bestimmen. Dies kann auch gegen kryptographisch starke Algorithmen gelingen, falls diese unsicher implementiert sind. Es können nicht nur Hardware-, sondern auch Softwareimplementierungen auf Rechnern oder mobilen Geräten Ziele von Seitenkanalangriffen werden; man denke etwa an Spectre und Meltdown.

Die derzeit größte Herausforderung stellt die Entwicklung von Quantencomputern dar, weil hinreichend große, universelle Quantencomputer die heute eingesetzte Public-Key-Kryptographie brechen würden. Die weltweite Forschung an Quantencomputern wird früher oder später zur Folge haben, dass die klassischen asymmetrischen Algorithmen durch Quantencomputer-resistente Algorithmen ersetzt werden müssen (Post-Quanten-Kryptographie), während die symmetrischen Verfahren im Wesentlichen erhalten bleiben. Auf diesem Gebiet wird derzeit weltweit intensiv geforscht, und NIST führt einen Standardisierungsprozess durch.

Die Aufgaben aus den 90er Jahren, insbesondere die kryptoanalytische Bewertung von Algorithmen und Protokollen, sind keineswegs verschwunden, aber wie bereits ausgeführt, hat sich das Aufgabenspektrum deutlich erweitert. Weitere inhaltliche Schwerpunkte liegen u. a. in der Sicherheitsbewertung von Zufallszahlengeneratoren, TLS-Implementierungen und Kryptobibliotheken, die in vielen kommerziellen und VS-IT-Produkten eingesetzt werden. Hinzu kommen die Bewertung von Sicherheitsvorfällen und kryptographische Fragestellungen, die sich aus aktuellen Trends und Entwicklungen in der Cyber-Sicherheit ergeben, etwa dem Cloud Computing oder der Blockchain-Technologie.

Kryptologinnen und Kryptologen unterstützen mit ihrer Expertise die Zertifizierungsreferate, soweit kryptographische Aspekte betroffen sind. Dies hat auch Einfluss auf VS-IT-Produkte, da zertifizierte Chipkarten häufig als Sicherheitsanker dienen. In Zulassungsverfahren spielen mobile Lösungen eine immer größere Rolle, und neuerdings sind auch Messengerdienste in den Fokus gerückt. Die Erweiterung des Aufgabenspektrums hat im Lauf der Zeit zu einer starken Vernetzung im BSI geführt, natürlich in erster Linie innerhalb der Abteilung, aber auch mit anderen Abteilungen.

KRYPTOTECHNIK IM BSI: ENTWICKLUNG DER KRYPTOSYSTEME

Die 1990er Jahre

Kryptogeräte existierten bereits seit längerem für den militärischen Einsatz und für ausgesuchte Verwendungen in der Bundesverwaltung. Anfang der 90er Jahre konzentrierte man sich im BSI im Wesentlichen noch

ED7 FN: IP-Kommunikationsplattform für vertrauliche Sprach- und Videokommunikation

auf die Entwicklung und Evaluierung von Kryptotechnik für den Schutz in Weitverkehrsnetzen, Funknetzen oder Liegenschaftsanbindungen. Die in Mehlem entwickelten Kryptoalgorithmen wurden im eigenen Labor in VHDL programmiert und später industriell als ASICs gefertigt. Diese Kryptochips bildeten den Kern neuer VS-IT-Produkte, die im Wesentlichen von Herstellern der IT-Sicherheitsindustrie im Auftrag und mit entwicklungsbegleitender Evaluierung des BSI gefertigt wurden. So entstand z. B. das ISDN-Kryptogerät ELCRODAT6-2, das für Verschlusssachen (VS) bis zum Geheimhaltungsgrad STRENG GEHEIM zugelassen und sowohl national wie auch international, z. B. im NATO Kontext, eingesetzt wurde.

Anfang der 90er hielten Arbeitsplatz-PCs als Schreibmaschinenersatz Einzug in die Bürolandschaft. Erste Verschlüsselungsprodukte schützten die Vertraulichkeit auf Datenträgern. Zu dieser Zeit dominierten Telefonie, Telefax und Briefpost die Bürokommunikation, doch sollte mit den ersten Internetanschlüssen die digitale Revolution auch hier ankommen. Während E-Mails für die übliche Briefpost immer mehr zur Konkurrenz wurden, brachte der Regierungsumzug von Bonn nach Berlin zum Ende der Dekade einen Impuls zur Entwicklung weiterer IT-Sicherheitsprodukte. Dies war u. a. der Startschuss für das vom BSI 1999 initiierte Projekt SINA (Sichere Inter-Netzwerk Architektur).

Die 2000er Jahre

Die neuen SINA Krypto-Boxen wurden für den Einsatz in IP-basierten Netzwerken entwickelt und 2002 erstmalig im damaligen Netzverbund des Bundesgrenzschutzes eingesetzt. Es folgten weitere SINA-Produkte, wie der SINA Thin Client und die SINA Workstation, die national wie international zum Schutz GEHEIM eingestufter VS-Daten zugelassen wurden. Das komplette Produktportfolio wurde mit Unterstützung des BSI permanent weiterentwickelt und an die Anforderungen der Kunden angepasst.

Die Bundeswehr startete mit Unterstützung des BSI im Rahmen der mobilen taktischen Kommunikation das Projekt SVFuA (Streitkräftegemeinsamen Verbundfähige Funkgeräteausstattung), wobei das BSI die entwicklungsbegleitende Evaluierung zum Zweck der VS-Zulassung übernahm. Der BOS-Funk (Behörden und Organisationen mit Sicherheitsaufgaben) wurde auf Digitalfunk umgestellt. Die Entwicklung der sogenannten BOS-Smartcard als Träger der kryptographischen Funktionen wurde vom BSI beauftragt und entwicklungsbegleitend evaluiert.

Zum Ende des Jahrzehnts zeichnete sich auch im Behördenbereich eine deutliche Zunahme bei der Nutzung mobiler IT ab. Das sogenannte Feature Phone wurde zunächst auf Leitungsebene zum regulären Arbeitsmittel. 2009 wurde zur kryptographischen Absicherung der mobilen Telefonie des Bundes der SNS-Standard des BSI entwickelt. Dieser bot für Telefonate bis zur Kategorie VS-NfD (Nur für den Dienstgebrauch) Schutz durch Ende-zu-Ende-Verschlüsselung.

Die 2010er Jahre

Das Smartphone erwies sich als die IT-Innovation des Jahrzehnts und avancierte auch im Behördenbereich innerhalb kürzester Zeit zum unverzichtbaren Arbeitsmittel, auch wenn die Sicherheitsstandards das Niveau der etablierten PC-Technologie anfänglich weit unterschritten. Das BSI vervielfachte in den folgenden Jahren seinen Einsatz für die sichere Mobilkommunikation der Behörden und lieferte entsprechende Lösungen. Mit der Integration von Bezahlsystemen verbesserten sich gegen Ende des Jahrzehnts zunehmend auch die Sicherheitseigenschaften der Smartphone-Technologie.

Auch bereits in den 2000er Jahren etablierte Systeme wurden weiterentwickelt. Auf Basis der SINA-Komponenten wurde ein neuartiges VS-Bearbeitungssystem inklusive elektronischer VS-Registratur geschaffen, die SWF (SINA Workflow). Und eine Ära ging zu Ende: Der Dienst ISDN wurde abgekündigt und verlangte nach neuen VS-IT-Produkten, wie etwa die in Kürze verfügbaren ELCRODAT7-FN und SINA Communicator zur GEHEIM-fähigen Sprach- und Videokommunikation.

KRYPTOKOMPETENZ MIT AUSSENWIRKUNG

Seit Ende der 90er Jahre bringt sich das BSI auch öffentlich in kryptographische Themen ein. So hat das BSI aktiv an

der Entwicklung und Verbreitung der Brainpool-Kurven (Elliptische Kurven) mitgearbeitet, hat die Verschlüsselungssoftware Chiasmus entwickelt und war in den Nullerjahren an zwei Faktorisierungsweltrekorden beteiligt.

In der jährlich erscheinenden technischen Richtlinie TR-02102 werden geeignete kryptographische Verfahren empfohlen. Die TR-02102 hat Auswirkungen auf andere TRs des BSI, auf den TLS-Mindeststandard, auf Zulassungs- und Zertifizierungsverfahren und auf die Auswahl von kryptographischen Mechanismen. Neben der frühzeitigen Empfehlung zweier Quantencomputer-resistenter Verfahren zur Schlüsseleinigung in der TR-02102 hat das BSI bereits 2020 erste Handlungsempfehlungen „Migration zu Post-Quanten-Kryptografie“ veröffentlicht. Große Bedeutung besitzen die Evaluierungsvorschriften AIS 20 für deterministische und AIS 31 für physikalische Zufallszahlengeneratoren, die im deutschen Zertifizierungsschema („Common Criteria“) verbindlich sind. Die AIS 31 wird auch im französischen Zertifizierungsschema angewendet, und ihre zentralen Ideen haben Eingang in einen internationalen ISO-Standard gefunden. Die AIS 31 hat außerdem das Design von physikalischen Zufallszahlengeneratoren spürbar beeinflusst. Das BSI gehört zu den Thought Leadern bei Anwendungen von KI-Methoden in der Kryptographie. Ein BSI-Team konnte im Rahmen der CHES 2018, der weltweit renommiertesten hardwarenahen Kryptokonferenz, zwei Challenges eines prestigeträchtigen Seitenkanalwettbewerbs gewinnen. Beim Nachfolgewettbewerb (CHES 2020) gelang es sogar, alle Preise zu gewinnen, die vergeben wurden. In beiden Fällen wurden KI-basierte Ansätze entwickelt. Die BSI-Broschüre „Blockchain sicher gestalten - Konzepte, Anforderungen, Bewertungen“ enthält eine Analyse der Blockchain-Technologie. Diese Aktivitäten und zahlreiche Publikationen in der einschlägigen Fachliteratur haben zu einer größeren Sichtbarkeit des BSI geführt und seinen Einfluss auf Entwicklungen deutlich erhöht.

Das BSI gestaltet auch Sicherheitsarchitekturen, die VS-IT-Produkten zu Grunde liegen, aktiv mit. Daher müssen Sicherheitsfunktionen stetig bewertet und für den Einsatz in Produkten empfohlen werden, die in Zusammenarbeit mit vertrauenswürdigen Partnern aus der Industrie für die Bedarfsträger bereitgestellt werden. Dem fachlichen Austausch mit Industrie und Wissenschaft kommt eine Schlüsselrolle zu, um neue Technologien bestmöglich für die Produktlandschaft verwerten zu können.

WIE GEHT ES WEITER?

Die aktuellen kryptographischen Themen werden auch im neuen Jahrzehnt von Bedeutung sein, vor allem die weitere Untersuchung und Entwicklung von KI-Ansätzen in der Kryptographie, die Auswahl geeigneter Quantencomputer-resistenter Algorithmen und die damit verbundene Anpassung von IT-Systemen. Post-Quanten-Kryptographie wird mittel- bis langfristig die klassische Public-Key-Kryptographie ersetzen.

In den vergangenen drei Jahrzehnten unterlag die VS-IT Systemlandschaft einem stetigen Wandel. Man kann davon ausgehen, dass sich dieser Trend fortsetzen wird, woraus sich neue Chancen, aber auch neue Herausforderungen ergeben. Immer kürzer werdende Innovationszyklen und neue Schlüsseltechnologien, wie z. B. Cloud-Szenarien, steigende Datenraten und der 5G/6G Mobilfunkstandard werden durch den kommerziellen Markt vorgegeben und von den Bedarfsträgern eingefordert werden. Der Erfolg zukünftiger VS-IT-Produkte hängt vom Zusammenspiel von Sicherheit, Innovation und Benutzerfreundlichkeit ab. Die starke Internationalisierung des IT-Komponenten- und Zuliefermarktes stellt dabei eine weitere Herausforderung dar.

Das BSI wird mit seiner Kryptokompetenz auch weiterhin kryptographische Entwicklungen und den technologischen Wandel in der IT-Sicherheit aktiv mitgestalten. ■

Danksagung

Wir danken zahlreichen Kolleginnen und Kollegen für wertvolle Anregungen und Beiträge zu diesem Artikel.

SINA Communicator H: IP-Kryptotelefon mit Videokonferenzoption

Viren-Suchprogramme
Als Schutz gegen Bedrohungen aus dem Internet hat das BSI Viren-Schutzprogramme und Viren-Suchprogramme herausgebracht. Zunächst als Diskette in verschiedenen Formen und Farben, dann als CD-Rom. Auch zu Papier wurden die Informationen gebracht, z. B. als Schriftenreihe im Bundesanzeiger.

Lang ist's her...

Artefakte aus 30 Jahren BSI

Seitdem das BSI vor 30 Jahren seine Arbeit aufgenommen hat, sind viele Dinge produziert worden, um den Auftrag der Behörde – die Gestaltung von Informationssicherheit in der Digitalisierung – zu erfüllen. Auch wenn einige Dinge heute vielleicht kurios und verstaubt wirken, waren sie doch zu ihrer Zeit ein probates Mittel und wurden lange erfolgreich eingesetzt, bevor sie durch (technische) Weiterentwicklungen abgelöst wurden. Diese Ausstellung ist eine Auswahl aus den vergangenen 30 Jahren BSI.

BSI für Bürger
Im Jahr 2002 wurde auf der Cebit das Angebot „Ins Internet – Mit Sicherheit" vorgestellt, vom damaligen Bundesinnenminister Otto Schily. Aus der CD-ROM, die dazu verteilt wurde, ist später das Internetangebot BSI für Bürger entstanden.

IT-Grundschutz
Der IT-Grundschutz ist eines der ältesten Themen des BSI. Die erste Ausgabe des IT-Grundschutz-Handbuchs erschien im Jahr 1994, damals noch als Loseblattsammlung, von den Mitarbeitern ausgedruckt und zusammengeheftet.

Spätere Ausgaben erschienen dann auf CD-ROM, genauso wie die erste IT-Grundschutz-Schulung.

Jahr-2000-Problem
Der Jahreswechsel 2000 und die Angst davor beschäftigte nicht nur viele Firmen, sondern natürlich auch das BSI. Informationen der Behörde zum Thema gab es damals noch als Diskette und auch als CD-ROM. Zum Glück war das Problem nicht so groß wie befürchtet.

*Diese **silberne Medaille** wurde im Rahmen der CC-Entwicklung gegen Ende des letzten Jahrtausends vom BSI bevorzugt an externe ausländische Teilnehmer ausgehändigt. Es sollte auch für Laien kein Problem sein, den Binärcode zu entschlüsseln.*

*Nach der Jahrtausendwende konnten die Inhalte des BSI online abgerufen werden. Für diejenigen mit schlechter Verbindung oder ohne Internetzugang gab es die Informationen der **Webseite auch offline als CD-ROM.***

*Mitarbeiter des BSI verrichten ihre Arbeit nicht nur im Büro, sondern gehen auch raus, um IT-Sicherheitsvorfälle zu untersuchen und vor Ort zu unterstützen. Der Zustand des **Polo-Shirts** zeugt von häufiger Nutzung.*

*Auch **CERT Bund** gibt es schon seit geraumer Zeit. Das 20-jährige Jubiläum der Einrichtung war Anlass genug, darauf anzustoßen.*

CERT-Bund

Von den Anfängen bis heute

CERT-Bund, das Computer Emergency Response Team für Bundesbehörden, ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen. Was 1994 mit einer Projektgruppe begann, ist heute gemeinsam mit dem Nationalen IT-Lagezentrum ein eigener Fachbereich im BSI mit über 60 Mitarbeiterinnen und Mitarbeitern. Günther Ennen, ehemaliger Leiter des CERT-Bund von 2001 bis 2007, und Stefan Ritter, Leiter des Fachbereichs IT-Sicherheitslage und CERT, berichten über die Anfänge des CERT und die heutigen Aufgaben.

■ **Wann wurde ein Computer Emergency Response Team erstmals zum Thema im BSI?**

Ennen: Das BSI stellte sich bereits kurz nach seiner Gründung 1991 im Bereich der Computer-Viren sehr kompetent auf. Als im März 1992 das Computer-Virus „Michelangelo“ weltweit großes Aufsehen erregte und Schäden herbeiführte, sah das BSI die Notwendigkeit, Fachwissen zur Gefährdung von Computern und Netzwerken durch Viren aufzubauen. Dies führte zur Gründung des behördeninternen BSI-CERT.

Ritter: Rückblickend betrachten wir die formale Aufnahme in die internationale CERT-Community mit der Mitgliedschaft im FIRST (Forum of Incident Response and Security Teams) 1994 als offizielles Gründungsjahr des CERT-Bund

■ **Wann fiel die Entscheidung, im BSI ein eigenes Referat CERT-Bund aufzubauen und welche Gründe gab es damals dafür?**

Ennen: Die Gründung eines eigenen Referats CERT-Bund resultierte unmittelbar aus dem Jahr 2000-Problem (Y2K). Dies hatte dafür gesorgt, dass verantwortliche Stellen auf Bundesebene sich bestehender Risiken – Computer- und Internetkriminalität, vorsätzliche Angriffe von außen – zunehmend bewusst wurden. Infolgedessen wurde im Februar 2000 unter Federführung des Bundesministeriums des Innern die Task Force „Sicheres Internet“ errichtet. Das BSI war Mitglied dieser Task Force.

Sie hatte die Aufgabe einen Katalog von notwendigen Sofortmaßnahmen gegen die neue Kriminalität zu erstellen. Durch frühzeitige Warnungen und präventive Maßnahmen sollte die Fähigkeit einer unmittelbaren Reaktion bei IT-Sicherheitsvorfällen sichergestellt werden. Der Aufbau von CERT-Bund als Dienstleister für die Bundesverwaltung war eine von der Task Force empfohlene Maßnahme. Als sich Anfang Mai 2000 der Computerwurm „Loveletter“ (Betreffzeile „ILOVEYOU“) weltweit explosionsartig verbreitete, wurde CERT-Bund zeitnah eine eigene Organisationseinheit im BSI.

■ **War allen Beteiligten gleich klar, welche Aufgaben ein CERT umfassen sollte?**

Ennen: Wir hatten zwar eine Vorstellung von der Aufgabe, es fehlte jedoch fundiertes Wissen über notwendige Dienstleistungen und die Erwartungen der Kunden in der Bundesverwaltung. CERT-Bund war deshalb zunächst gefordert, Kontakte zu existierenden CERTs zu suchen mit dem Ziel, die Ausprägung des eigenen CERT zu entscheiden. Unsere Mitarbeit bei der Erstellung eine Studie über die CERT-Struktur in Deutschland vernetzte uns in kurzer Zeit mit bekannten CERTs in Deutschland.

■ **Welche Dienstleistungen bot das CERT in seiner Gründungsphase an?**

Ennen: Wir entschieden uns für die typischen Dienstleistungen des nationalen CERT: ein Informations-, Warn- und Alarmierungsdienst, die Beantwortung von Anfragen sowie die Unterstützung bei der Bewältigung von Vorfällen. Ebenso wichtig war eine unmissverständliche Abgrenzung gegenüber Aufgaben, für die ein CERT nicht zuständig ist.

Eine ausgewogene Mischung aus Kompetenz in Technik und Organisation sowie die Festlegung von Aufgaben, Arbeitsbereichen, Rollen und eine klare Regelung von Verantwortung sind Voraussetzungen für effiziente und

erfolgreiche CERT-Arbeit. Damals häufig als „Internetfeuerwehr“ bezeichnet haben wir aus Erfahrungen und Informationen der Feuerwehr sehr nützlich Hinweise übernommen.

■ **Im ersten Schritt baute das CERT-Bund seine Kontakte zu Behörden auf. Wurden Sie dort mit offenen Armen empfangen?**

Ennen: Einen Empfang mit offenen Armen haben wir in sehr vielen Behörden gespürt, gleichwohl gab es auch Distanz und Berührungsängste. Offensichtlich war es die Sorge vor Regelungen und Kontrollen durch uns, eine nur nachgeordnete Behörde. In einer frühen Phase wurden wir daher auf das Ressortprinzip (Art. 65 Satz 2 GG) hingewiesen. Die Herausforderung für CERT-Bund beim Aufbau war eine wirkungsvolle Mischung aus Dienstleistungen zur Prävention und Reaktion zu finden, um die Behörden zur freiwilligen Zusammenarbeit mit CERT-Bund zu bringen.

■ **Wie hat sich nachfolgend die dauerhafte und erfolgreiche Zusammenarbeit mit den Behörden entwickelt?**

Ennen: Zunächst haben wir durch eine eigene Webseite und den Betrieb eines Mailservers Kommunikationskanäle etabliert. Mit Push und Pull wurden risikobewertete Informationen an Stellen in den Bundesbehörden verteilt, zunächst ohne Einschränkungen des Adressatenkreises. Da jede Information unmittelbar zu Nachfragen führte, waren wir nach kurzer Zeit mehr mit der Beantwortung von E-Mails als mit dem Aufbau von Dienstleistungen befasst. Wir musste also konsequent unsere Kundenseite organisieren, das heißt in jeder Behörde sollte nur eine personalisierte, verantwortliche Ansprechstelle für CERT-Bund existieren, über die die gesamte Kommunikation gesteuert wurde. Ein schwieriger Prozess, der nahezu zwei Jahre dauerte.

■ **Bald danach war das CERT diejenige Stelle im BSI, die erste Kontakte in die freie Wirtschaft, z.B. zu Telekommunikationsunternehmen knüpfte. Wie sah dort die Zusammenarbeit aus?**

Ennen: Nachdem CERT-Bund im BSI eine eigene Organisationseinheit war, galt es die Zusammenarbeit zwischen CERT-Bund und weiteren CERTs in der Wirtschaft und Industrie zu intensivieren. Brigitte Zypries, damals Staatssekretärin im BMI, forderte im ersten CERT-Bund Arbeitstreffen 2001: „Wenn wir wollen, dass die Wirtschaft sich engagiert, muss der Bund die Aufgabe besonders gut machen.“ Mit Stolz kann ich feststellen: Diesen Anspruch hat CERT-Bund erfüllt. Die Zusammenarbeit und der Austausch des Wissens mit nationalen CERTs war erfolgreich, nicht zuletzt wegen des gegenseitigen Vertrauens, das auch schriftlich festgehalten wurde: CERT-Bund vereinbarte bereits im August 2002 mit ausgewählten CERTs einen „Code of Conduct“.

Ritter: Dieses Engagement war nachhaltig. Der daraus entstandene Deutsche CERT-Verbund umfasst mittlerweile weit über vierzig deutsche CERTs aus Wirtschaft, Verwaltung und dem akademischen Raum mit Wissenschaft und Forschung.

■ **Seit vielen Jahren ist das CERT-Bund auch eng in den internationalen CERT-Verbund eingebunden. Warum kann ein Bundes-CERT nicht allein auf nationaler Ebene agieren?**

Ritter: Auch wenn die meisten CERTs für eine klare Zielgruppe zuständig sind – IT-Sicherheitsthemen sind behörden-, unternehmens- und grenzübergreifend. Und das erfordert gegenseitigen Austausch und übergreifende Zusammenarbeit, national und international!

Ennen: Die Arbeit im nationalen Rahmen wurde zunächst durch die Mitgliedschaft in den Gruppen TI (Trusted Introducer for CSIRTs in Europe) und FIRST erfolgreich erweitert. Der weltweite vertrauliche Austausch von Informationen, Hinweise auf Schwachstellen, Warnungen vor vermuteten oder tatsächlichen Angriffen ist heute Tagesgeschäft aller CERT-Strukturen. Alle Beteiligten haben davon unmittelbaren oder mittelbaren Nutzen. Durch frühe Warnungen betroffener IT-Systeme können Schäden bei noch nicht betroffenen IT-Systemen vermieden oder zumindest vermindert werden.

■ **Herr Ennen, gab es in Ihrer Zeit als Leiter von CERT-Bund ein Ereignis von besonderer Bedeutung?**

Ennen: Unvergessen sind die Auswirkungen der Fußball Weltmeisterschaft 2006 in Deutschland. Der Dienst im Lagezentrum „vor Ort“ wurde auf die Wochenenden und Feiertage erweitert – Arbeit an 365 Tagen. Mit der Personalstelle und dem Personalrat waren notwendige Dienstvereinbarungen abzustimmen, zudem galt es die Kolleginnen und Kollegen für einen „frei und willigen“ CERT-Dienst zu gewinnen. Diese Herausforderungen waren nicht einfach zu lösen, aber dies macht den Reiz der CERT-Arbeit aus.

■ **Herr Ritter, was sind die wesentlichen Unterschiede des heutigen CERT-Bund zum CERT-Bund bei seiner Gründung?**

Ritter: In den Anfangsjahren war CERT-Bund sehr stark auf den Warn- und Informationsdienst (WID) für Schwachstellen ausgerichtet. Da damals Updates und Patches noch verteilt auf den Webseiten der Hersteller „versteckt“ waren, hat CERT-Bund diese gesammelt, bewertet und priorisiert. Sie wurden dann formatiert und in der Tat oft aus dem Englischen übersetzt der Bundesverwaltung zur Verfügung gestellt. Dieser aufwändige Prozess wurde bald kundenfreundlich über der BSI-WID-Portal gelöst.

2015 hatten das BSI und CERT-Bund dann einen intensiven und medienwirksamen Einsatz beim Hackerangriff auf den Deutschen Bundestag. Infolgedessen nahmen – auch mit der Bereitstellung von Ressourcen für Mobile Incident Response Teams (MIRT) – die Aktivitäten bei der Vorfallsunterstützung deutlich zu. Mittlerweile ist die aufwändige Bearbeitung und Unterstützung bei schweren IT-Sicherheitsvorfällen die Schwerpunktaufgabe von CERT-Bund.

■ **Welches waren aus Ihrer Sicht die wichtigsten Entwicklungsschritte, seit Sie das CERT leiten?**

Ritter: Zum einen der Auf- und Ausbau des Nationalen IT-Lagezentrums mit seinen Dienstleistungen und Produkten im Referat CERT-Bund. Dazu gehören die nationale Meldestelle, die Lagebeobachtung von offenen und vertraulichen Quellen, die mittlerweile 24/7 erfolgt, sowie Tages- und Monatsberichte in verschiedenen Einstufungen und auch Berichterstattung zu Spezialthemen der Lage wie etwa Threat Intelligence. Mittlerweile ist das Nationale IT-Lagezentrum aus CERT-Bund herausgelöst und arbeitet mit den Bereichen „Grundsatz und Meldestelle", „Dauerdienst" sowie „Analyse und Prognose" über Referatsgrenzen hinweg zusammen.

Der zweite bedeutende Schritt ist das Wachstum von CERT-Bund selbst. Aufgaben, Nachfrage und damit auch der Personalbedarf haben sich so verändert, dass jetzt fünf Referate die ursprüngliche Aufgabe des ersten Teams 2001 übernehmen. Das Aufgabenspektrum reicht dabei vom Warn- und Informationsdienst mit Coordinated Vulnerability Disclosure über die nationale und internationale CERT-Netzwerkbetreuung, die Technische Analyse und Forensik, die Vorfallsunterstützung bis hin zum MIRT-Einsatz vor Ort.

■ **Sind die Zielgruppen des CERT heute noch mit denen der Anfangsjahre vergleichbar?**

Ritter: Zwar liegt der Fokus weiterhin auf der Bundesverwaltung. Über die Jahre hat sich aber mit den gesetzlichen Grundlagen des BSI auch die Zielgruppe des CERT-Bund erweitert. Dadurch sind wir befugt, die meisten unserer Unterstützungsdienstleistungen auch den Kritischen Infrastrukturen, den Bundesländern und der freien Wirtschaft anzubieten. CERT-Bund ist also heute eher ein nationales CERT als ein CERT der Bundesverwaltung, wie der Name noch vermuten lässt.

■ **Der letzte große IT-Sicherheitsvorfall – Kritische Schwachstellen in Microsoft Exchange-Servern – liegt erst wenige Monate zurück. Wie bereitet sich das CERT auf ein solches Szenario vor?**

Ritter: Mit dem Aufbau des Nationalen IT-Lagezentrum war ab 2007 auch die Vorbereitung und Einrichtung eines Nationalen IT-Krisenreaktionszentrums (IT-KRZ) verbunden. Mit dieser Besonderen Aufbau-Organisation ist es dem BSI möglich, organisatorisch und mit dem erforderlichen Personal in Zellen aufzuwachsen. Dies geschieht stufenweise und lageangepasst, um die jeweilige besondere Situation zu bewältigen. Als Hilfen für seine Zielgruppen gibt das IT-KRZ Lageberichte und technische Empfehlungen zur Problemlösung heraus. Es ist in das nationale Krisenmanagement des Bundesinnenministeriums eingebunden und unterstützt dieses. ■

CERT Bund

Kurzprofil Günther Ennen

Günther Ennen begann seine Tätigkeit im BSI bereits kurz nach dessen Gründung 1992. Ab2001 leitete er zunächst die Projektgruppe CERT-Bund und ab 2002 das Referat CERT-Bund. Von 2007 bis zu seinem Ruhestand 2017 leitetet er die IT-Sicherheitsberatung des BSI.

Kurzprofil Stefan Ritter

Stefan Ritter wechselte 2001 von der Bundeswehr ins BSI, wo er zunächst im Bereich Kritische Infrastrukturen weiter ausbaute. 2007 wurde er Leiter des Referats CERT-Bund. Seit 2020 leitet er den Fachbereich IT-Lagenzentrum und CERT.

30 Jahre BSI

Thought Leader mit stetig wachsenden Aufgaben

Wie hat sich das BSI seit 1991 von einer kleinen Fachbehörde zum Kompetenzzentrum für Cyber-Sicherheit entwickelt? BSI-Präsident Arne Schönbohm spricht im Interview über den bisherigen Erfolgsweg des BSI und künftige Herausforderungen.

■ 1991 wurde das BSI gegründet. 30 Jahre sind in der IT eine gefühlte Ewigkeit. Ist das BSI eine junge oder eine alte Behörde?

Es gibt natürlich viele Behörden, die älter sind als wir. Aber für eine Behörde, die sich mit dem Thema der IT-Sicherheit, der Cybersicherheit befasst, ist 30 Jahre ein bemerkenswertes Alter. Denken Sie zurück ins Jahr 1991: kein weit verbreitetes Internet, keine Mobiltelefonie, schon gar kein Internet der Dinge, Smart Factories oder Smart Cities. Viele Errungenschaften, die wir heute selbstverständlich nutzen, gehörten 1991 wohl eher in das Reich der Science Fiction, oder sogar der Fantasie.

■ Entsprechend sind auch die Anforderungen an die Cyber-Sicherheit heute und 1991 kaum miteinander vergleichbar...

Cyber-Sicherheit ist heute eine gesamtgesellschaftliche Aufgabe, die Staat, Wirtschaft sowie Bürgerinnen und Bürger gleichermaßen betrifft. Vor 30 Jahren sah das ganz anders aus. IT-Sicherheit war damals ein Nischenthema der Sicherheitspolitik, weit weg vom Alltag der Bürgerinnen und Bürger oder der Unternehmen. Heute gilt es, die fortschreitende Digitalisierung aller Lebensbereiche sicher zu gestalten, um allen Menschen in Deutschland die großen Potentiale der Digitalisierung möglichst risikofrei nutzbar zu machen.

■ Dass schon 1991 eine Behörde gegründet wurde, die sich mit dem Thema IT-Sicherheit beschäftigen sollte – war das nicht beinahe revolutionär?

Durchaus. Dem BSI-Errichtungsgesetz zugrunde lag ein damals neues Verständnis von Prävention, Information und Aufklärung – erstmals formuliert im „Zukunftskonzept Informationstechnik" der Bundesregierung im Juli 1989. Alle Betroffenen und Interessierten sollten über Risiken der Informationstechnik und mögliche Schutzmaßnahmen unterrichtet werden. Spätestens mit Beginn der breiten Nutzung des Internets ab 1993 wurde deutlich, wie zukunftsweisend dieser Ansatz damals schon war.

■ Das Aufgabenspektrum des BSI hat sich über die Jahre gewandelt und erweitert. Was waren die wichtigsten Meilensteine?

Von Beginn an umfasste der Arbeitsauftrag des BSI den Schutz der Regierungsnetze und der Bundesverwaltung vor Cyber-Angriffen. Mit der Novellierung des BSI-Gesetzes 2009 konnte das BSI für die Bundesbehörden verbindliche Sicherheitsstandards für die Beschaffung und den Einsatz von IT entwickeln. Das BSI wurde zudem zur zentralen Meldestelle für IT-Sicherheit innerhalb der Bundesverwaltung, um bei IT-Krisen nationaler Bedeutung durch Informationen und Analysen die Handlungsfähigkeit der Bundesregierung sicherzustellen.

Für die Bürgerinnen und Bürger haben wir ein umfangreiches Beratungs- und Informationsangebot aufgebaut, das sich immer größerer Beliebtheit erfreut, je weiter die Digitalisierung in unserem Alltag voranschreitet. Ähnliches gilt für Unternehmen, für die wir heute – unter anderem mit der Allianz für Cyber-Sicherheit – breite und maßgeschneiderte Angebote zur Verfügung stellen können. Wir konnten uns auch gegenüber den Ländern und Kommunen als verlässlicher Partner etablieren und pflegen mittlerweile durch das Nationale Verbindungswesen eine enge Zusammenarbeit.

Heute verfügt das BSI auf der Basis seiner technisch tiefgehenden Expertise als Thought Leader in Sachen Cyber-Sicherheit über eine integrierte Wertschöpfungskette von der Beratung über die Entwicklung sicherheitstechnischer Lösungen, der Abwehr von Angriffen auf die Cyber-Sicherheit bis hin zur Standardisierung und Zertifizierung.

■ **Inwiefern haben die IT-Sicherheitsgesetze die Aufgaben des BSI noch einmal ausgeweitet?**

Durch das erste IT-Sicherheitsgesetz erhielt das BSI 2015 Befugnisse und Aufgaben zum Schutz der Kritischen Infrastrukturen. Mit dem in diesem Jahr in Kraft getretenen IT-Sicherheitsgesetz 2.0 wurden diese noch einmal erweitert. Der Gesetzgeber hat hier ein solides rechtliches Fundament für die Arbeit des BSI geschaffen. Dieses Fundament und die damit verbundenen Aktions- und Durchgriffsmöglichkeiten des BSI – gerade auch in den Kritischen Infrastrukturen – helfen dabei, das Thema Cyber-Sicherheit in der Mitte der Gesellschaft zu verankern. Außerdem wurde der digitale Verbraucherschutz in das IT-Sicherheitsgesetz 2.0 aufgenommen. So können wir die Sensibilisierung der Verbraucherinnen und Verbraucher– was das BSI bereits mit vielfältigen Angeboten praktiziert – ausbauen.

■ **Welche Voraussetzungen muss das BSI schaffen, um seinen vielen Aufgaben gerecht zu werden?**

Es muss seine Vernetzung mit allen anderen Akteuren in der Sicherheitsarchitektur Deutschlands ausbauen, es muss internationale Kooperationen fördern und forcieren, es muss für die Bürgerinnen und Bürger als Ansprechpartner in Sachen Cyber-Sicherheit noch sichtbarer werden – und es muss sich selbst immer wieder herausfordern, damit es all diesen Aufgaben gerecht werden kann.

Dafür braucht es zum einem motivierte Mitarbeiterinnen und Mitarbeiter, die über den Tellerrand sehen und ihrem Beruf mit hoher fachlicher Kompetenz und Leidenschaft nachgehen.

Zum anderen braucht es eine agile Organisation, in der alle Beteiligten aktiv und anpassungsfähig sind, offen für Neues, bereit, bremsende Strukturen zu lösen und Kästchendenken aufzubrechen, auch und gerade um die anstehende räumliche Diversifizierung zu bewältigen.

■ **Wird das BSI heute von außen anders wahrgenommen als in den Anfängen?**

Das BSI hat sich in diesen 30 Jahren neben den Polizeien und den Nachrichtendiensten zu einer der drei tragenden Säulen der Sicherheitsarchitektur Deutschlands entwickelt. Wir, als die Cyber-Sicherheitsbehörde des Bundes, gestalten Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft in Deutschland. Der Aufbau und die Bündelung von Know-how im Bereich der Cyber-Sicherheit hat das BSI zu einer schlagkräftigen Institution gemacht, in der die Fäden der Cyber-Sicherheit zusammenlaufen.

■ **Ist Digitalisierung heute noch ohne Informationssicherheit denkbar?**

Deutschland digital sicher zu machen, das ist heute das Ziel des BSI. Informationssicherheit und Digitalisierung gehören heute untrennbar zusammen: Sie sind zwei Seiten derselben Medaille. Das BSI steht für beides. Der stetige Ausbau des Amtes erfolgt gezielt in zukunftsorientierten Bereichen, die für die positive Weiterentwicklung der Bundesrepublik Deutschland von elementarer Bedeutung sind: Dazu zählt zum Beispiel der Bereich Künstliche Intelligenz. Mit unserem Kriterienkatalog für KI-basierte Cloud-Dienste, den wir in diesem Jahr veröffentlicht haben, schaffen wir eine Grundlage für vertrauenswürdige KI und nehmen eine führende Rolle bei der Absicherung von KI-Anwendungen ein. Ein weiteres Zukunftsfeld ist die Cyber-Sicherheit im Gesundheitswesen – von der IT-Sicherheit von Medizinprodukten über die elektronische Patientenakte bis zur Corona-Warn-App gibt es hier zahlreiche Digitalisierungsprojekte, in die das BSI involviert ist. Autonomes Fahren oder der Ausbau des 5G-Netzes sind weitere Beispiele für die Bandbreite der heutigen BSI-Themen.

Durch diesen gezielten Ausbau des BSI und die engagierte Arbeit seiner Mitarbeiterinnen und Mitarbeiter wird Deutschland jeden Tag ein Stück cyber-sicherer. Gleichzeitig zeigt das BSI, wie Informationssicherheit zu einem neuen Qualitätsmerkmal einer Digitalisierung „Made in Germany“ wird, durch die Deutschland seine Position auf den internationalen Märkten stärken und ausbauen kann. ■

DAS BSI

Gekommen um zu bleiben

Personalentwicklung im BSI: Spannende Aufgaben zwischen Onboarding, Homeoffice und persönlicher Weiterentwicklung.

Ein Interview mit Anke Gaul, Leiterin des Referats Personalentwicklung

Im BSI arbeiten Expertinnen und Experten aus unterschiedlichsten Fachrichtungen zusammen an den wichtigsten Digitalthemen unserer Zeit wie zum Beispiel Künstliche Intelligenz, 5G, autonomes Fahren oder das sichere Smart Home. Somit gestaltet das BSI die sichere Digitalisierung für Deutschland. Angesichts dieser großen Aufgabe soll das Team auf rund 1550 Stellen wachsen. Über die Herausforderung, Mitarbeitende zu gewinnen, aber vor allem auch dauerhaft zu binden, sprechen wir mit Anke Gaul, Referatsleiterin Personalentwicklung.

■ **Welche Herausforderungen gibt es auf dem IT-Fachkräftemarkt und wie gehen Sie im BSI damit um?**

Der Markt für Fachkräfte – insbesondere im IT-Bereich – ist nach wie vor hart umkämpft und alle Prognosen sprechen von einem überproportional steigenden Bedarf. Arbeitgeber müssen sich verstärkt um Talente bemühen. Nah am Bewerbenden zu sein, digitalisierte Prozesse und kurze Reaktionszeiten sind hier sehr wichtig. Anders als früher ist auch der Arbeitgeber Gegenstand detaillierter Beobachtung und Bewertung, vor allem Online-Rezensionen sind eine wichtige Visitenkarte. Gleichzeitig heißt das, eine Organisation kann es nicht bei Marketing-Versprechen belassen: Versprechen, die nach außen gemacht werden, müssen nach innen gehalten werden.

■ **Wie gelingt das beim BSI?**

Glücklicherweise haben wir beim BSI eine gute Kombination aus spannenden Themen, der Möglichkeit diese aktiv mit zu gestalten und einem sicheren Arbeitsplatz. Aber es geht nicht nur darum, Mitarbeitende zu gewinnen, sondern diese auch dauerhaft zu binden und Entwicklungsperspektiven zu bieten. Ein eigens dafür zuständiges Team sorgt dafür, dass die Personalentwicklung „up-to-date“ ist. Es gilt - auch in Anbetracht der aktuellen Halbwertszeit von Wissen oder des demografischen Wandels - tragfähige Konzepte zu entwickeln, mit denen sowohl persönliche Weiterentwicklung, als auch die Erfüllung unserer ambitionierten Organisationsziele als führende Cyber-Sicherheitsbehörde gelingen kann.

■ **Welche Herausforderungen gab es durch Corona und wie wirkt sich die Situation auf die Entwicklung von Themen und Prozessen in der Personalarbeit des BSI aus?**

Als es 2020 zum deutschlandweiten Lockdown kam, hatten wir als IT-Behörde das Glück, dass wir bereits vor der Pandemie digitalisiert und unsere Mitarbeitenden mit sicherer mobiler Informationstechnik ausgestattet waren. In der Personalgewinnung und –entwicklung hat die Pandemie zusätzlich dazu geführt, dass wir von heute auf morgen unsere Prozesse komplett umstellen mussten. So führen wir unsere Auswahlverfahren überwiegend virtuell durch. Und auch in der Personalentwicklung setzen wir seitdem auf virtuelle Workshops, Vorträge und zum Beispiel Barcamps.

■ Auch Personalführung muss nun ganz anders gelebt werden. Wie geht das BSI damit um?

Ein wesentlicher Aspekt in der Personalentwicklung war die Fortführung unseres Prozesses „Führung@ BSI_2025“. Kern dieses Prozesses, der bereits 2019 startete, ist die Weiterentwicklung unserer Führungskultur. Durch Corona und der plötzlichen Notwendigkeit auf Distanz zu Führen bekam dies weitere Relevanz. So bieten wir den Führungskräften einen gezielten Kanon aus (Online-) Schulungsformaten, Workshops, Vernetzungsoptionen sowie Beratung und Coaching an. In einem durch Distanz geprägten neuen Führungsalltag zu guten Ergebnissen und Teamleistungen zu kommen und gleichzeitig aber auch nah an den Mitarbeitenden zu sein und deren jeweilige individuelle Situation im Blick zu haben, ist durchaus herausfordernd.

■ Rechnen Sie damit, dass die Veränderungen nachhaltig sind oder wird man doch wieder zu Gewohntem zurückkehren?

„Don’t waste a crisis!“ Unter Beteiligung unterschiedlichster Bereiche des Hauses haben wir definiert was das „New Normal“ für uns bedeutet und wie wir in Zukunft davon profitieren können. Was ich persönlich als besonders wertvoll erachte ist, dass die bisweilen – nicht nur bei uns – tief verwurzelte Haltung von „Anwesenheit als Leistungsmerkmal“ überdacht wurde bzw. wird und im ‚New Normal‘ keine Option ist. Das Ergebnis rückt in den Vordergrund.

Es wird aber – hoffentlich - bei einigen Themen auch wieder möglich sein, an Bewährtes anzuknüpfen. Insbesondere dort, wo der persönliche Kontakt eine wichtige Rolle spielt, wie z.B. bei der Einarbeitung neuer Kolleginnen und Kollegen. ■

Personalgewinnung

„Im Wettbewerb um die besten Köpfe bedarf es auch in Zukunft eines Mixes an zielgruppenspezifischen Recruiting-Kanälen. Daher weiten wir sukzessive unsere Hochschulkooperationen sowie unsere Präsenz auf (virtuellen) Karriereevents aus. Dabei setzen wir den regionalen Schwerpunkt auf unsere Standorte in Bonn und Freital sowie unseren zukünftigen Stützpunkt in Saarbrücken.“

Janine Koch, Referatsleiterin Personalgewinnung

Diversity

„Diversität spielt im BSI eine große Rolle. Unsere Mitarbeitendenbefragung hat gezeigt, dass genau darin unsere Stärke liegt und wir die Vielfältigkeit der Kolleginnen und Kollegen nutzen können, um voneinander zu lernen und innovative Ideen zu entwickeln.“

Bettina Jäkel-Schmidt, Personalentwicklung

Betriebliches Gesundheitsmanagement (BGM)

„BGM endet nicht an der Bürotür. Auch im Home Office sorgen wir mit unterschiedlichen Angeboten dafür, dass sich die Mitarbeitenden fit halten können. Zusätzlich bieten wir Unterstützungs- und Beratungsmöglichkeiten für den Umgang mit dem neuen Alltag an.“

Helena Marx, Personalentwicklung

Praktika und Abschlussarbeiten

„Im Rahmen eines Praktikums oder einer Abschlussarbeit können Studierende bereits während ihres Studiums erste Erfahrungen in einer Behörde sammeln. Mit den vielfältigen Arbeitsbereichen im BSI decken wir ein breites Themenspektrum ab, um die theoretischen Lerninhalte aus dem Studium praktisch anzuwenden.“

Sarah Spilles, Personalgewinnung

Führungskräfte-Nachwuchsprogramm (FKNP)

„Wir waren uns einig, dass wir unser FKNP trotz der Corona-bedingten Einschrän-kungen weiterführen wollen, um den Teilnehmenden wichtiges Rüstzeug für eine mögliche Führungsposition mitgeben zu können. Daher haben wir die Inhalte umstrukturiert sowie flexibel auf Remote umgemünzt und so einen Weg gefunden, das Programm auch in der aktuellen Situation stattfinden zu lassen. “

Mareike Mumm, Personalentwicklung

Ausbildung und Studium

„Um zukünftige IT-Fachkräfte bedarfsgerecht auszubilden, begleiten wir Absolventinnen und Absolventen sowie Studierende von Anfang an. Gemeinsam mit der Hochschule des Bundes bieten wir den Studiengang „Digital Administration and Cyber Security“ an. Eine IT- oder Verwaltungsausbildung ist bei uns ebenfalls möglich.“

Alessandra Krüger, Personalentwicklung

17. Deutscher IT-Sicherheitskongress 2021

Digitale Premiere mit Rekordkulisse

Mit über 8.000 Teilnehmerinnen und Teilnehmern verzeichnete das BSI eine Rekordkulisse beim 17. Deutschen IT-Sicherheitskongress, der am 2. und 3. Februar 2021 erstmals in digitaler Form stattfand.

Live-Vorträge und virtuelle Messestände machten IT-Sicherheit erlebbar. Die beiden Kongresstage konnten mit den vielen Vorträgen, Fachdiskussionen – beispielsweise der hochkarätig besetzten Podiumsdiskussion zum Thema „Faktor Mensch: Wie werden wir cyber-sicherer?“ – sowie den beiden Preisverleihungen CAST/GI Promotionspreis IT-Sicherheit 2021 und Best Student Award einen umfassenden fachlichen Einblick in aktuelle Themen der Cyber-Sicherheit ermöglichen.

In 30 Fachvorträgen standen beim Kongress Themen wie sichere digitale Identitäten, sichere Mobilkommunikation, Künstliche Intelligenz oder Post-Quanten-Kryptografie ebenso im Fokus wie neue Trends für mehr Sicherheit im Internet der Dinge, im Smart Home oder in Industriesteuerungssystemen.

INFORMATIONSSICHERHEIT IN DER DIGITALISIERUNG

BSI-Präsident Arne Schönbohm: „Mit über 8.000 Teilnehmenden hat das BSI den größten IT-Sicherheitskongress Deutschlands ausgerichtet. Das große Interesse am Kongress des BSI zeigt, dass Informationssicherheit ein Thema ist, das die Menschen beschäftigt. Cyber-Angriffe oder Datendiebstähle finden nicht in einer virtuellen Parallelwelt statt, sondern haben ganz reale Folgen für Bürgerinnen und Bürger ebenso wie für Unternehmen und Behörden. Bundeskanzlerin Angela Merkel hat in ihrem Grußwort zum Kongress daher zurecht betont, dass Digitalisierung und Informationssicherheit zusammen gehören. Für das BSI als Cyber-Sicherheitsbehörde des Bundes ist dies zusätzliche Motivation, auch zukünftig die Informationssicherheit in der Digitalisierung zu gestalten und damit einen wichtigen Beitrag zur Zukunft des Standorts Deutschlands zu leisten.“

DEUTSCHLAND. DIGITAL. SICHER. 30 JAHRE BSI

In diesem Jahr tagte der BSI-Kongress unter dem Motto „Deutschland. Digital. Sicher. 30 Jahre BSI“ und blickte auf drei bewegte Jahrzehnte IT-Sicherheit zurück. Denn seit seiner Gründung zum 1. Januar 1991 gestaltet das BSI als zentrales Kompetenzzentrum der Informationssicherheit die sichere Digitalisierung in Deutschland.

Die Grußworte und Geburtstagsglückwünsche, die das BSI während des Kongresses empfangen durfte, hoben die wichtige Bedeutung des BSI bei der sicheren Digitalisierung in Deutschland und darüber hinaus hervor und würdigten die Arbeit des BSI. „Digitalisierung und Informationssicherheit gehören zusammen. Wir müssen in beiden Bereichen stark sein. Das entscheidet wesentlich darüber, wie erfolgreich Deutschland in Zukunft sein wird. Vor diesem Hintergrund zeigt sich, welch wichtige Rolle das BSI spielt und auch in Zukunft spielen wird. […] Sie machen unser Land sicherer. Dafür danke ich Ihnen sehr“, so die Bundeskanzlerin Dr. Angela Merkel in ihrer Video-Grußbotschaft aus dem Kanzleramt.

„Das BSI hat eine 30-jährige Geschichte. Es ist eine 30-jährige Erfolgsgeschichte, in der das BSI über die Grenzen Deutschlands hinweg Maßstäbe in der Informationssicherheit gesetzt hat. Um diese Institution werden wir in weiten Teilen Europas beneidet“, äußerte Staatssekretär Dr. Markus Richter in seiner Grußbotschaft. Oberbürgermeisterin der Bundesstadt Bonn Katja Dörner, Ministerpräsident Tobias Hans sowie Parlamentarischer Staatssekretär Prof. Dr. Günter Krings hoben in ihren Grußworten ebenso die Untrennbarkeit von Digitalisierung und Informationssicherheit hervor und richteten damit lobende Worte an die erfolgreiche Arbeit des BSI: „30 Jahre BSI, das heißt 30 Jahre Kampf für mehr Sicherheit in IT und Telekommunikation und 30 Jahre Engagement für die Cyber-Sicherheit von Staat, Wirtschaft und Gesellschaft

Prof. Dr. Christoph Meinel, Prof. Dr. Claudia Eckert, Dirk Hoke, Claudia Nemat und Arne Schönbohm (v. l. n. r.) diskutieren mit der Moderatorin Claudia van Veen in der Podiumsdiskussion das Thema „Faktor Mensch: Wie werden wir cybersicherer?“

„Digitalisierung und Informationssicherheit gehören zusammen. Wir müssen in beiden Bereichen stark sein. Das entscheidet wesentlich darüber, wie erfolgreich Deutschland in Zukunft sein wird. Vor diesem Hintergrund zeigt sich, welch wichtige Rolle das BSI spielt und auch in Zukunft spielen wird. [...] Sie machen unser Land sicherer. Dafür danke ich Ihnen sehr.“

Bundeskanzlerin, Dr. Angela Merkel

in ganz Deutschland“, sagte Ministerpräsident Tobias Hans. Das BSI hat sich nach den Worten von Vizeadmiral und Inspekteur des Cyber- und Informationsraums (CIR) Dr. Thomas Daum zu dem „Gravitationszentrum der Informationssicherheit in Deutschland“ entwickelt und damit Deutschland sicherer gemacht: „Sie sind heute der Ansprechpartner für IT-Sicherheit in Deutschland. Sie sind der kompetente Partner im internationalen Raum für sämtliche IT-Sicherheitsfragen und Sie sind ein vertrauensvoller Kooperationspartner und eine geschätzte Beratungsautorität für die Bundeswehr“, so Dr. Thomas Daum. Die Botschaften zeigten sehr deutlich: Informationssicherheit und Digitalisierung gehören untrennbar zusammen: Sie sind zwei Seiten einer Medaille und des BSI.

Das große Interesse am Kongress des BSI zeigt, dass Informationssicherheit ein Thema ist, das die Menschen beschäftigt. Cyber-Angriffe oder Datendiebstähle finden nicht in einer virtuellen Parallelwelt statt, sondern haben ganz reale Folgen für Bürgerinnen und Bürger ebenso wie für Unternehmen und Behörden. Die positive Resonanz auf den erstmals digital ausgerichteten IT-Sicherheitskongress wird das BSI in die Planung des 18. Deutschen IT-Sicherheitskongresses miteinbeziehen, um den Teilnehmerinnen und Teilnehmern erneut eine Plattform für den Austausch zu den Themen der Digitalisierung zu geben. ■

Weitere Informationen:

https://www.bsi.bund.de/IT-Sicherheitskongress

https://www.bsi.bund.de/SharedDocs/Bilderstrecken/DE/Kongress-2021/bilderstrecke-kongress-2021_node.html

Informationssicherheit in der IT-Konsolidierung Bund

Gemeinsam sicher durch die Verzahnung der Informationssicherheitsmanagementsysteme

Von Christoph Lauffer und Sven Schneider, Informationssicherheitsbeauftragte IT-Konsolidierung Bund

Mit der Entscheidung der Bundesregierung und dem Kabinettsbeschluss, die IT des Bundes zu modernisieren und zu konsolidieren, wurde 2015 das bis dahin größte IT-Projekt der Bundesverwaltung gestartet. Bis zum Jahr 2025 soll die IT des Bundes gebündelt und standardisiert werden, um das Fundament für die digitale Zukunft zu schaffen. Dabei ist die Informationssicherheit eine wesentliche Voraussetzung für die erfolgreiche und umfassende Digitalisierung.

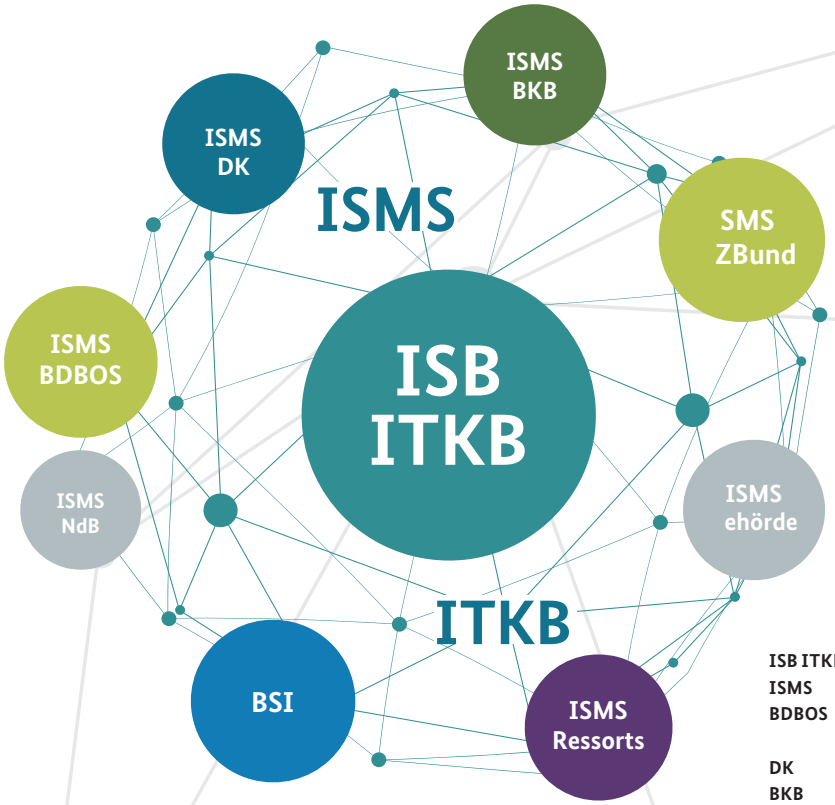
Großprojekte dieser Art haben in der Regel eine große Anzahl an verschiedenen internen und externen Abhängigkeiten, sind hochkomplex und stehen einer Vielzahl unterschiedlicher Herausforderungen gegenüber. Sich stetig ändernde Rahmenbedingungen machen dabei auch Änderungen an der Projektorganisation notwendig. So wurde im November 2019 vom Kabinett eine Reorganisation des Projektes IT-Konsolidierung beschlossen. Die wesentliche Bedeutung der Informationssicherheit für eine erfolgreiche Konsolidierung der IT wurde dabei nochmals verdeutlicht. Die IT-Konsolidierung Bund (ITKB) bietet hierbei Chancen und Risiken zugleich: Einerseits ermöglicht die gemeinsame Nutzung von IT-Ressourcen die flächendeckende Steigerung der Informationssicherheit durch Standardisierung und Fokussierung. Andererseits stellt die Konsolidierung auf wenige zentrale Dienste, Betriebsplattformen, Netze und Rechenzentren ein lohnenswertes Angriffsziel dar. Das Erreichen eines einheitlichen und angemessenen Sicherheitsniveaus und die Reduzierung von Risiken macht die Verzahnung der Institutionen der ITKB erforderlich. Dabei sind insbesondere das heterogene Umfeld mit vielen Beteiligten, die unterschiedlichen Reifegrade und Ausprägungen der jeweiligen Informationssicherheitsmanagementsysteme (Information Security Management Systems / ISMS) herausfordernd.

INFORMATIONSSICHERHEITSRICHTLINIE IT-KONSOLIDIERUNG BUND

Vor diesem Hintergrund wurde beschlossen, eine Richtlinie zur Informationssicherheit in der ITKB zu erstellen. Diese soll den „Umsetzungsplan Bund 2017 – Leitlinie für Informationssicherheit in der Bundesverwaltung (UP Bund)“ für die ITKB konkretisieren und sicherstellen, dass die ISMS der an ITKB beteiligten Behörden in geeigneter Weise kooperieren.

Die Richtlinie wurde unter Federführung des BSI entwickelt. Beteiligt waren darüber hinaus das Bundesministerium der Finanzen (BMF), das Bundesministerium des Innern, für Bau und Heimat (BMI), das Informationstechnikzentrum Bund (ITZBund) und die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS). Der Kick-off fand am 12.02.2020 im Stützpunkt des BSI in Berlin statt. Aufgrund der sich ausbreitenden Corona-Pandemie musste der damals geplante Arbeitsmodus geändert werden. Die geplanten Präsenztermine zur Erarbeitung und Abstimmung von Inhalten wurden in Telefon- und Videokonferenzen umgewandelt, was die gemeinsame Abstimmung zunächst erschwerte.

Gemäß dem Auftrag des UP Bund 2017 beschreibt die Informationssicherheitsrichtlinie IT Konsolidierung



ISB ITKB	Informationssicherheitsbeauftragter IT-Konsolidierung Bund
ISMS	Information Security Management Systems
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
DK	Dienstekonsolidierung
BKB	Betriebskonsolidierung Bund
ITZBund	Informationstechnikzentrum Bund
NdB	Netze des Bundes

Abbildung 1: Schematische Darstellung der Verzahnung der ISMS der ITKB Institutionen durch das ISMS ITKB und den ISB ITKB. Quelle: BSI

(ISR ITKB) den grundsätzlichen Aufbau des ISMS für die IT-Konsolidierung Bund zur Verzahnung der ISMS der an der IT-Konsolidierung Bund beteiligten Behörden, Dienstleister und Projektleitungen. Dabei erstreckt sich der Geltungsbereich auf die für die IT-Betriebskonsolidierung Bund bereitgestellten Betriebsplattformen sowie auf die Dienste für die IT Dienstekonsolidierung Bund sowie auf deren Betriebsplattformen. Darüber hinaus werden die zentralen Netze betrachtet, die für die Kommunikation zwischen den Kundeneinrichtungen und zu den Betriebsplattformen und Diensten benötigt werden sowie IT-Lösungen, die auf die Betriebsplattformen aufsetzen oder über Schnittstellen mit den oben genannten Bereichen verknüpft sind.

In der gemeinsamen Erstellung der Richtlinie wurden folgende Bereiche identifiziert, die bei der Verzahnung der ISMS vorrangig betrachtet werden müssen, um ein angemessenes Informationssicherheitsniveau in der IT-Konsolidierung Bund und der später konsolidierten IT des Bundes zu gewährleisten:

- Schnittstellen zwischen den ISMS
- Schutzbedarfsfeststellungen
- Nutzer-/Dienstleisterpflichten
- Verbundrisikomanagement
- Informationssicherheitscontrolling
- Prüfungen, Zertifizierungen und Abnahmen der Informationssicherheit in der ITKB

Dabei sind insbesondere die Bereiche Verbundrisikomanagement und Informationssicherheitscontrolling hinsichtlich des verzahnenden Charakters für die IT-Konsolidierung Bund neu zu etablieren. Die jeweiligen Details zu den genannten Themen werden in sechs der ISR ITKB untergeordneten Dokumente ausgearbeitet.

Die Richtlinie wurde am 10.12.2020 vom Lenkungsausschuss IT-Konsolidierung Bund des IT-Rates einstimmig beschlossen. Am 11.12.2020 wurden vom Präsidenten des BSI, Arne Schönbohm, Christoph Lauffer zum Informationssicherheitsbeauftragten ITKB (ISB ITKB) und Sven Schneider zu seinem ständigen Vertreter bestellt.

Bei seinen Aufgaben wird der ISB ITKB vom Informationssicherheitsmanagementteam ITKB (ISMTeam ITKB), bestehend aus Vertretern der Projektleitungen der Dienstekonsolidierung (BMI) und der Betriebskonsolidierung Bund (BMF), den Dienstleistern ITZBund und BDBOS sowie dem BSI unterstützt. ■

IT-SICHERHEIT IN DER PRAXIS

Der Landtag in Schleswig-Holstein und das BSI

Ein neues Kapitel der Zusammenarbeit

Von Prof. Dr. Utz Schliesky, Direktor des Schleswig-Holsteinischen Landtags

Im November 2019 trafen sich der Direktor des Schleswig-Holsteinischen Landtages und der Präsident des BSI zu einem ersten Interessen- und Erfahrungsaustausch. Vereinbart wurde eine Intensivierung der Zusammenarbeit zwischen BSI und dem Schleswig-Holsteinischen Landtag.

Noch vor einigen Jahren war das Referat für Informations- und Kommunikationsmanagement im Schleswig-Holsteinischen Landtag ein klassischer Einzelkämpfer. Zu seinen Aufgaben gehörte die Erbringung sämtlicher IT-Dienstleistungen in der Landtagsverwaltung und zur Sicherstellung des Parlamentsbetriebes. Dokumente wurden an andere Landesbehörden in Papierform über den Postweg verschickt. Ein elektronischer Austausch war durch unterschiedliche IT-Systeme der Landesregierung und des Landtages erschwert.

Wahrnehmbar änderte sich dies mit Etablierung einer neuen IT-Infrastruktur. Die Landesregierung führte gemeinsame zentrale Dienste unter Verantwortung des IT-Dienstleisters Dataport ein. Der Landtag schloss sich an. Als Ergebnis gab es standardisierte Systeme, bei denen Nutzerorientierung, IT-Sicherheit, Gruppenzusammenarbeit und Mobilität größere Beachtung fanden. Alles begann in kleinen Schritten.

FORTSCHREITENDE DIGITALISIERUNG

Heute sind solche Gegebenheiten nicht mehr vorstellbar. Die technische Entwicklung mündete in eine enge administrative und digitale Vernetzung zwischen Parlament und Landesregierung. Gemeinsam wurden elektronische Akte und E-Rechnung eingeführt. Das Schleswig-Holsteinische Transparenzportal, über das Informationen für

Bürgerinnen und Bürger veröffentlicht werden, startete. Für die Umsetzung des Onlinezugangsgesetzes werden bis zum Jahr 2022 umfassend Verwaltungsleistungen digitalisiert. Diese Entwicklungen wirken in den Landtag hinein. Er ist in den Digitalisierungsprozess eingebunden, indem z. B. Parlamentsdokumente künftig auf dem Transparenzportal zu finden sind. Mit dem Online-Petitionsverfahren und anderen Angeboten gibt es parlamentarische Dienstleistungen, die sich für die Anbindung an das OZG-Serviceportal eignen.

NEUE HERAUSFORDERUNGEN DURCH DIE CORONA-PANDEMIE

Einen weiteren Digitalisierungsschub löste die Corona-Pandemie aus. Plötzlich waren etablierte Veranstaltungen, wie z. B. Ausschusssitzungen mit Anhörung einer großen Anzahl an Sachverständigen, parlamentarische Abende und Informationsveranstaltungen für Bürgerinnen und Bürger, nicht mehr in Präsenz möglich. Die Einführung von Videokonferenzen wurde forciert. Für die Herstellung der Parlamentsöffentlichkeit bei digital tagenden Ausschüssen gab es neue Lösungen.

ZUSAMMENARBEIT MIT DEM BSI

Wie hängt dies alles mit einer Zusammenarbeit zwischen Landtag und BSI zusammen?

Als einer der ersten Parlamente setzte sich der Schleswig-Holsteinische Landtag für eine Stärkung der IT-Sicherheit ein. Bereits bei Durchführung der Landtagswahl im Jahr 2017 gab es eine Kooperation. Das BSI überwachte am Wahltag und während der gesamten Auszählung die technische Übermittlung der Wahlergebnisse der Landeswahlleiterin an den Landtag und die Medien.

Zusammen mit dem Baden-Württembergischen Landtag wurde der mittlerweile etablierte Erfahrungsaustausch der Informationssicherheitsbeauftragten der Landtage, des Bundestages und des Bundesrates initiiert. Ausgerichtet wurde außerdem die Veranstaltung „Die Hacker kommen“. Zahlreiche Abgeordnete und Landesbeschäftigte konnten so zu Cyber-Angriffen erfolgreich sensibilisiert werden.

Durch den Digitalisierungsschub sind die Herausforderungen an Sicherheit und Verfügbarkeit der IT-Systeme enorm gestiegen. Eine funktionierende IT-Sicherheitsorganisation in Zusammenarbeit mit Landes- und Bundesbehörden ist elementar, um den größer werdenden Herausforderungen durch Cyber-Angriffe wirksam begegnen zu können. Beispielhaft sei an dieser Stelle das Auftreten des Schadprogramms Emotet genannt, welches übergreifend und im Landtag Anlass zu verstärkten Sicherheits- und Sensibilisierungsmaßnahmen gab.

Dies hat der IT-Planungsrat längst erkannt und fordert in seiner aktuellen Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung einheitliche Sicherheitsstandards. Ein einzelner Landtag kann dies wegen der raschen Dynamik und notwendigen fortlaufenden Anpassung der Sicherheitsmaßnahmen kaum mehr alleine umsetzen. Hierfür bedarf es einer kompetenten Beratung und Unterstützung durch erfahrene Sicherheitsexpertinnen und -experten. Eine intensive Zusammenarbeit mit dem BSI liegt vor diesem Hintergrund nahe. Sie soll künftig in gemeinsame Informations- und Sensibilisierungsveranstaltungen für die Abgeordneten und Beschäftigten des Landtages münden. Perspektivisch sind weitergehende Projekte der Zusammenarbeit vorstellbar.

Der Schleswig-Holsteinische Landtag freut sich deshalb über die neu vereinbarte Zusammenarbeit und die Unterstützung des BSI im gemeinsamen Bestreben nach mehr IT-Sicherheit in der Parlamentsverwaltung. ■

Kurzprofil Prof. Dr. Utz Schliesky

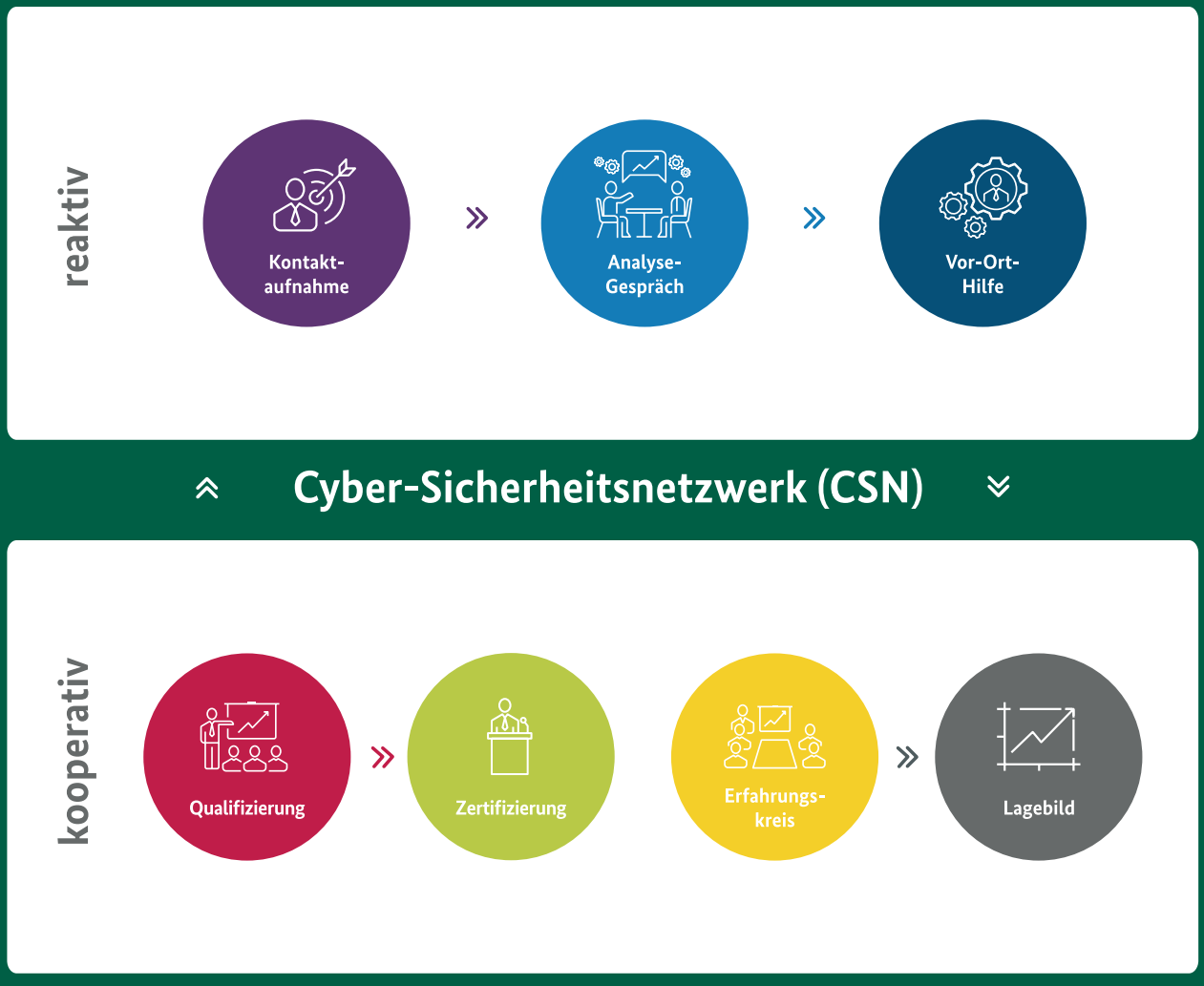
Nach Abschluss seines Studiums der Rechtswissenschaften an der Christian-Albrechts-Universität zu Kiel war Prof. Dr. Utz Schliesky in den Jahren 1993 bis 2003 zunächst als Wissenschaftlicher Mitarbeiter tätig, 1996 promovierte er zum Thema „Öffentliches Wettbewerbsrecht“ und legte anschließend sein Zweites Juristisches Staatsexamen vor dem Hanseatischen Oberlandesgericht ab. 2002 folgte die Habilitation bei Bundesminister a. D. Prof. Dr. Edzard Schmidt-Jortzig an der Christian-Albrechts-Universität zu Kiel. Seit 2003 war er Erster Beigeordneter und stellvertretender Hauptgeschäftsführer des Deutschen Landkreistages, Berlin. Von 2005 bis 2009 war er Leiter der Abteilung Verwaltungsmodernisierung im Finanzministerium des Landes Schleswig-Holstein im Range eines Ministerialdirigenten. 2009 übernahm Prof. Dr. Utz Schliesky das Amt des Direktors des Schleswig-Holsteinischen Landtages. Nebenamtlich ist er seit 2007 Vorstand des Lorenz-von-Stein-Instituts für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel, dort auch Leiter des Forschungsbereiches Staatliches Innovationsmanagement. Seit 2011 ist er Präsident der Schleswig-Holsteinischen Juristischen Gesellschaft e.V.

Cyber-Sicherheitsnetzwerk

Unterstützung bei IT-Sicherheitsvorfällen für KMU sowie Bürgerinnen und Bürger

Von Angelika Jaschob, Referat Kooperation mit Herstellern und Dienstleistern

Während Kritische Infrastrukturen und Konzerne nach einem IT-Sicherheitsvorfall auf interne Spezialisten sowie Forensik-Teams zurückgreifen können, stehen kleine und mittelständische Unternehmen (KMU) und Bürgerinnen und Bürger meist alleine da. Ohne die notwendige Expertise und Erfahrung fällt es ihnen schwer, einen IT-Sicherheitsvorfall zu bewerten und die richtigen Schritte zu ergreifen. Hier setzt das Cyber-Sicherheitsnetzwerk (CSN) an. Mit dem CSN wird eine flächendeckende, dezentrale Struktur aufgebaut, die KMU und Bürgerinnen und Bürgern bei IT-Vorfällen effizient und kostengünstig Unterstützung anbietet.



Das Qualifizierungsprogramm (Quelle: BSI)

CYBER-SICHERHEITSNETZWERK BIETET UNTERSTÜTZUNG

Das Cyber-Sicherheitsnetzwerk ist ein freiwilliger Zusammenschluss von qualifizierten Expertin-nen und Experten, die sich bereit erklären, ihre individuelle Expertise in der Vorfallbearbeitung zur Behebung von IT- Sicherheitsvorfällen zur Verfügung zu stellen. Sie helfen KMU oder Bürgerinnen und Bürgern IT-Sicherheitsvorfälle zu analysieren und zu beheben.
Ein Qualifizierungsprogramm stellt dabei die einheitliche Qualität der Vorfallbearbeitung durch Expertinnen und Experten sicher. Zusätzlich wird die Qualifizierung der „Digitalen Ersthelfer“ bzw. „Vorfall-Experten“ mittels eines Testats bzw. einer Personenzertifizierung bescheinigt.

Durch den Austausch von Erfahrungen bei der Vorfallbearbeitung werden der Zusammenhalt des Expertennetzwerks und der Aufbau einer einheitlichen Wissensbasis gefördert.

JETZT ZUM „DIGITALEN ERSTHELFER“ ODER „VORFALL-EXPERTE“ QUALIFIZIEREN LASSEN

Der Erfolg des Cyber-Sicherheitsnetzwerks steht und fällt mit den eingesetzten Expertinnen und Experten. Deshalb setzt das Cyber-Sicherheitsnetzwerk von Anfang an den Fokus auf deren Qualifikation und Zertifizierung. Das Programm bildet den Rahmen für die Qualifizierung der „Digitalen Ersthelfer“ und „Vorfall-Experten“. Für „Digitale Ersthelfer“ sollen in einem kostenlosen Online-Basiskurs Kenntnisse aus einem Erste-Hilfe-Programm vermittelt werden. Um aktiv das Cyber-Sicherheitsnetzwerk zu unterstützen, müssen sie sich anschließend noch beim Cyber-Sicherheitsnetzwerk registrieren lassen.

Für „Vorfall-Experten“ bieten spezielle Schulungsanbieter eine dreitägige Aufbauschulung an. In diesen Schulungen vermitteln qualifizierte Trainerinnen und Trainer zusätzliche und fachlich tiefergehende Inhalte in den Bereichen Vorfallanalyse und -behandlung. Die Schulung befasst sich mit Themenfeldern, die sowohl theoretisch als auch praktisch durch Übungen vermittelt werden. Mit diesem standardisierten Schulungsprogramm wird eine breite Basis geschaffen, um ein Qualifizierungsprogramm für die „Vorfall-Experten“ anzubieten.

Die Expertinnen und Experten des Cyber-Sicherheitsnetzwerks können zielgruppengerecht eine reaktive Unterstützung nach IT-Sicherheitsvorfällen anbieten, um KMU und Bürgerinnen und Bürger in geeigneter Art und Weise zu unterstützen.

„VORFALL-EXPERTE“ - EINE WICHTIGE ZUSATZ-QUALIFIKATION FÜR UNTERNEHMEN

Auch Unternehmen sollten - ähnlich dem IT- Sicherheitsbeauftragten - einen „Vorfall-Experten“ bereitstellen, um Kenntnisse über den Aufbau der „Digitalen Rettungskette“ zu erlangen und das Vorgehen bei der Vorfall-Behandlung kennenzulernen. Eine entsprechende Qualifikation durch den Besuch der o.a. Aufbauschulung wird für mindestens eine Mitarbeiterin oder einen Mitarbeiter des Unternehmens empfohlen.

Das Qualifizierungsprogramm (Quelle: BSI)

Um nach einem IT-Sicherheitsvorfall diesen möglichst schnell und effektiv behandeln zu können, würden diese internen „Vorfall-Experten“ des Unternehmens eine kompetente Schnittstelle zu den externen „Vorfall-Experten“ des Cyber-Sicherheitsnetzwerks bilden.

START DER PILOTPHASE DES CYBER-SICHERHEITSNETZWERKS IM HERBST 2021 IM RAUM BONN

Im Herbst dieses Jahrs beginnt ein sechsmonatiger Pilotbetrieb im Raum Bonn. Einige Herausforderungen werden sich erst während dieser Pilotphase zeigen und dann adäquat gelöst werden können. Die Pilotphase schließt mit einer Evaluierung ab, in der Empfehlungen für die nächsten Schritte zusammengefasst werden und die Planung für eine deutschlandweite Einführung der Unterstützungsdienstleistung durch das Cyber-Sicherheitsnetzwerk durchgeführt wird. ■

Cyber-Sicherheitsnetzwerk

https://www.bsi.bund.de/Cyber-Sicherheitsnetzwerk
info@cyber-sicherheitsnetzwerk.de

Weitere Informationen:

https://www.bsi.bund.de/Cyber-Sicherheitsnetzwerk

https://www.bsi.bund.de/SharedDocs/Videos/DE/BSI/Allgemein/210114_CSN_mp4.html

Maßgeschneiderte Angebote für KMU

Neues Referat betreut kleine und mittlere Unternehmen

von Manuel Bach, Leiter des Referats Cyber-Sicherheit für KMU

Ohne Cyber-Sicherheit wird es keine erfolgreiche Digitalisierung geben - doch welche Maßnahmen sollen Verantwortliche ergreifen, um den Risiken der fortschreitenden Digitalisierung zu begegnen? Insbesondere kleine und mittlere Unternehmen (KMU) verfügen bislang oftmals nicht über ausreichende eigene Ressourcen, um sich adäquat um das Thema IT-Sicherheit kümmern zu können. Und in Pandemiezeiten sind sie ohnehin mit einer Vielzahl von zusätzlichen Problemen konfrontiert. Sie brauchen also Hilfe. In der im vergangenen Jahr neu gegründeten Abteilung „Wirtschaft und Gesellschaft“ wurde daher im Herbst 2020 ein neues Referat eingerichtet, dass sich genau um diese Gruppe kümmern soll.

Dem BSI-Credo „IT-Sicherheit ist Chefsache!“ folgend, wendet sich das Referat mit seinen Angeboten direkt an die Führungsebene der Unternehmen. Erst, wenn dort ein ausreichendes IT-Sicherheitsbewusstsein vorhanden ist, werden die erforderlichen Maßnahmen der IT-Sicherheit umgesetzt.

Im Oktober 2020 hat das BSI daher ein Pilotprojekt gestartet, um kurzfristig Sicherheit bei KMUs erzeugen zu können. Anlass war eine Warnung von CERT-Bund im Januar 2020. Damals hatte das CERT öffentlich vor einer Schwachstelle in Citrix-Netscaler-VPN-Gateways gewarnt, die über das Internet automatisiert

kompromittierbar waren. Wie üblich hatte das CERT auch die deutschen Internet Service Provider über verwundbare Systeme ihrer Kundinnen und Kunden informiert. Neun Monate später waren zwar fast alle Systeme gepatcht, immerhin 160 verwundbare Systeme – fast alle stellten sich also solche von KMU heraus - waren jedoch noch sichtbar. Da die Erfahrung gezeigt hatte, dass eine große Zahl von Systemen bereits im Frühjahr 2020 automatisiert kompromittiert worden war und die Angreifer im Nachgang händisch erst Daten ausgeleitet und danach Ransomware auf die Systeme aufgebracht hatten, bestand für diese 160 Unternehmen höchste Gefahr. Das BSI entschied daher, die Geschäftsführungen dieser Unternehmen per Post persönlich anzuschreiben. Aus dem TLS-Zertifikat der verwundbaren Server konnte man den „Common Name“ entnehmen, die nötigen Daten für das Anschreiben wurden dann per Handarbeit aus dem Impressum der Unternehmen erhoben.

Das Pilotprojekt war erfolgreich. Innerhalb von zwei Wochen hatten 50 Prozent der Unternehmen ihre Systeme bereinigt. Warum aber hatten die anderen 50 Prozent nicht reagiert? Durch persönliche Nachfragen per Telefon stellte sich heraus, dass zwar ein großer Teil der KMUs der BSI-Empfehlung „Falls Sie selbst nicht das nötige Know-how besitzen, beauftragen Sie einen geeigneten IT-Dienstleister“ gefolgt war. Vielfach hatten die Dienstleister ihren Auftraggebern jedoch gemeldet, ihre Server seien jetzt sicher, obwohl diese tatsächlich weiterhin ungeschützt über das Internet erreichbar und damit kompromittierbar waren. Zwei der IT-Dienstleister hatten sogar die Schwachstelle auf ihren eigenen Systemen nicht gepatcht. Das BSI hält eine Liste von zertifizierten IT-Sicherheitsdienstleistern in den Geltungsbereichen IS-Revision und IS-Penetrationstest vor. Ergänzend arbeitet das BSI aktuell an einem „Cybersicherheitsnetzwerk“, das sich ausdrücklich an KMU und Bürgerinnen und Bürger richten wird – eine Pilotphase dieses Netzwerks wird in diesem Jahr starten.

Dem BSI wurden zwischenzeitlich weitere Fälle drohender Angriffe auf Unternehmen bekannt. Im Oktober 2020 hatte das CERT vor Sicherheitslücken im Produkt Microsoft Exchange Server gewarnt, im Februar 2021 waren immer noch 20.000 Server in Deutschland verwundbar, von denen dem BSI schließlich 9.000 Datensätze mit Kontaktdaten vorlagen. Auch hier wurden die Geschäftsführungen persönlich angeschrieben. Am Tag, an dem die Briefe gedruckt und versendet werden sollten, veröffentlichte Microsoft überraschend Informationen zu neuen Schwachstellen im Exchange Server. CERT-Bund rief sofort die IT-Bedrohungslage 4 (rot) aus. Die 9.000 Unternehmen waren sämtlich ebenfalls betroffen. Die Anschreiben wurden daher um die aktuellen Informationen ergänzt und konnten dann fast zeitgleich mit Bekanntwerden der Schwachstellen auf den Weg gebracht werden.

Der Rücklauf auf das Schreiben war erwartungsgemäß immens. Viele Fragen erreichten das BSI per E-Mail, eine ganze Reihe aber auch telefonisch über das Service Center. Schnell war klar, dass es einen weiteren Kanal für die Zielgruppe KMU geben muss. Nach einem vom BSI gemeinsam mit Microsoft durchgeführten Webinar, dessen 1.000 Teilnehmerplätze im Handumdrehen ausgebucht waren, fiel die Entscheidung, als BSI erstmalig live im Internet auf Sendung zu gehen. Mit nicht einmal einem Tag Vorbereitung wurde der Livestream gemeinsam mit anderen Referaten auf die Beine gestellt. Etwa 2.000 Zuschauer verfolgten den Stream live und einige Zeit später war er zusätzlich insgesamt noch über 35.000-mal angeschaut worden.

Die Rückmeldungen waren sehr erfreulich – das heißt: Das machen wir jetzt öfter! Die Einrichtung eines kleinen BSI-Studios ist gerade in Arbeit.

Aber auch außerhalb von akuten Bedrohungslagen steht das BSI KMU mit Warnungen und Informationen hilfreich zur Seite. ■

In Deutschland existieren nach EU-Klassifikation etwa 2,6 Millionen Unternehmen, die dem Bereich KMU zuzurechnen sind. Das sind 99,4 Prozent aller Unternehmen. Sie beschäftigen 57 Prozent (31 Millionen) der Arbeitnehmerinnen und Arbeitnehmer in Deutschland, stellen 82 Prozent der Ausbildungsplätze und generieren 43 Prozent der Bruttowertschöpfung der deutschen Wirtschaft. Das Bonner Institut für Mittelstandsforschung (IfM) verwendet eine leicht abweichende KMU-Definition, indem es die Grenze für mittlere Unternehmen nicht bei 249, sondern bei 499 Mitarbeiterinnen und Mitarbeitern zieht, da sich die deutsche Besonderheit der mittelständischen Familienunternehmen damit besser darstellen lässt. Viele dieser familien- bzw. eigentümergeführten Unternehmen zählen zur Gruppe der „Hidden Champions“, die in Deutschland etwa 1.500 Unternehmen umfasst - und damit etwa die Hälfte aller Hidden Champions weltweit ausmacht. Etwa 70 Prozent der deutschen Hidden Champions haben weniger als 250 Beschäftigte, 12 Prozent beschäftigen zwischen 250 und 499 Mitarbeiterinnen und Mitarbeiter.

Weitere Informationen:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/unternehmen-und-organisationen_node.html

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html

BSI INTERNATIONAL

Consumer IoT-Sicherheit

Europa als Vorreiter

von Thomas Gilles, Referat Cyber-Sicherheit in Smart Home und Smart Cities

Immer mehr Geräte, die wir zuhause oder unterwegs verwenden, verbinden sich über das Internet und bilden zusammen das Internet der Dinge (Internet of Things, kurz: IoT). Überdies vertrauen wir Webdiensten über die vernetzen Geräte eine Vielzahl von Daten an. Eine Person besitzt derzeit im weltweiten Durchschnitt sieben vernetzte Consumer IoT-Geräte, von Smartwatches, funkenden Thermostaten oder Smart TVs bis hin zu intelligenten Waschmaschinen. Die Weiterentwicklungen im Mobilfunk (5G-Technologie) beschleunigt das Wachstum des IoT zusätzlich.

Consumer IoT-Geräte sind häufig nicht oder nur unzureichend gegen Cyber-Angriffe geschützt. Nutzerinnen und Nutzer können ausspioniert und deren Smart Home manipuliert werden. Wird zum Beispiel die Smart Home-Zentrale übernommen, können Einbrecher smarte Türschlösser öffnen oder die Rollladen steuern. Außerdem werden immer wieder Fälle bekannt, in denen Nutzerinnen und Nutzer über ihre eigene smarte Kamera beobachtet werden. Wird eine Vielzahl von IoT-Geräten kompromittiert, können diese zusammen als Botnet genutzt werden, um Infrastrukturen anzugreifen. So können zum Beispiel Distributed Denial of Service-Angriffe (kurz DDoS) auf Webservices durchgeführt werden, wodurch diese überlastet werden oder durch massenhafte Ein-/Ausschaltvorgänge Schwankungen im Stromnetz erzeugt werden.

STANDARDISIERUNGSAKTIVITÄTEN IN EUROPA

Bisher existierten verschiedene Anleitungen bzw. Guides, die sich insbesondere an Entwicklerinnen und Entwickler richteten und beschrieben, wie IoT-Geräte sicherer implementiert werden können. Was bisher fehlte war eine international ankerkannte Messlatte, um zu beurteilen, ob die Geräte über ein Mindestmaß an Cyber-Sicherheit verfügen - also eine Art Urmeter für die Cyber-Sicherheit von Consumer IoT-Geräten. Die Veröffentlichung der europäischen Norm ETSI EN 303 645 schaffte hier Abhilfe.

EUROPÄISCHE NORM ETSI EN 303 645

Die EN 303 645 definiert Anforderungen für ein Mindestmaß an Cyber-Sicherheit aller Consumer IoT-Geräte mit Fokus auf den Schutz vor Angriffen über die Netzwerkschnittstellen der Geräte. Diese lassen sich häufig automatisieren, um eine Vielzahl von Geräten zu kompromittieren. Der Standard definiert generische Anforderungen an das Design der Geräte und die Herstellerprozesse wie die Entgegennahme von Schwachstellenmeldungen. Weitere Anforderungen sind u. a.: Passwörter müssen im Betrieb individuell sein, und die sicherheitsrelevante Konfiguration über ein Netzwerk muss authentisiert werden.

PRÜFSPEZIFIKATION ETSI TS 103 701

Selbst die beste Messlatte nützt aber nichts, wenn diese unterschiedlich angelegt wird. Deshalb legt die Prüfspezifikation ETSI TS 103 701 fest, wie eine Konformitätsbewertung von IoT-Produkten für Verbraucherinnen und Verbraucher anhand der Anforderungen von EN 303 645 durchgeführt werden kann, um die Vergleichbarkeit der Bewertungsergebnisse zu gewährleisten.

NUTZEN FÜR WIRTSCHAFT UND GESELLSCHAFT

Herstellerinnen und Hersteller können die erwähnten Spezifikationen in deren Entwicklungs- und Prüfprozesse für ihre Produkte zur Verbesserung der Cyber-Sicherheit integrieren. Prüflabore, Zertifizierungsstellen, Verbraucherschützerinnen und -schützer, Sicherheitsforscherinnen und -forscher bis hin zu Testzeitschriften können diese nutzen, um Anforderungen zu stellen und Geräte zu prüfen.

INTERNATIONALE VERBREITUNG

Die Eindämmung der Sicherheitsprobleme im Bereich Consumer IoT ist eine globale Herausforderung. Hierzu liefert der Sicherheitsstandard, der bereits von verschieden Nationen aufgegriffen wird, einen wichtigen Beitrag.

In Deutschland soll die EN 303 645 zunächst für das geplante IT-Sicherheitskennzeichen, an dem das BSI maßgeblich beteiligt ist, verwendet werden. Zukünftig können Herstellerinnen und Hersteller ihre Consumer IoT-Geräte mit einem IT-Sicherheitskennzeichen versehen, wenn diese über ein Mindestmaß an IT-Sicherheit verfügen. Basis hierfür bildet eine Herstellerselbsterklärung, deren Einhaltung durch eine Marktaufsicht überwacht wird. Analog wurde in Finnland und Singapur ein Security Label eingeführt, um sichere IoT Consumer-Produkte auf Basis der EN zu kennzeichnen. Das vereinigte Königreich plant überdies eine Regelung hinsichtlich der Mindestsicherheit von IoT-Geräten: Es dürfen nur Produkte in Verkehr gebracht werden, die einige der Kernanforderungen der EN erfüllen.

Aktuell wird diskutiert auf der Basis der Schlussfolgerungen des Rates der EU zur Cybersicherheit vernetzter Geräte, die unter deutscher Präsidentschaft angenommen wurden, im Cybersecurity Act ein europaweit harmonisiertes IoT-Zertifizierungsschema für Consumer-Geräte zu etablieren. Über die EN und die zugehörige Testspezifikation sollen vergleichbare Konformitätsprüfungen ermöglicht werden. Insgesamt leistet die unter Beteiligung des BSI entstandene neue europäische Norm einen wichtigen internationalen Beitrag für mehr Sicherheit im IoT. ■

Weitere Informationen:

Der aktuelle Entwurf der Prüfspezifikation ist hierüber abrufbar: https://docbox.etsi.org/CYBER/CYBER/Open/Latest_Drafts

https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/de/pdf

DIGITALE GESELLSCHAFT

Starke Kunden-authentifizierung bei Kreditkartenzahlungen

3D-Secure als neuer Standard

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

Spätestens seit dem 14.09.2019 ist für Online-zahlungen die Starke Kundenauthentifizierung (Strong Customer Authentication, SCA) verpflichtend im Einsatz. Mögliche Authentifizierungsverfahren, die den Ansprüchen der SCA gerecht werden, enthalten zwei Faktoren der Kategorien Wissen (z. B. Passwort), Biometrie (z. B. Fingerabdruck) oder Besitz (z. B. SMS-TAN oder bankeigene App). Zusätzlich darf die Authentifizierung nur für den konkreten Zahlungsvorgang Gültigkeit besitzen. Dazu müssen der Betrag und die IBAN des Zahlungsempfängers oder der Zahlungsempfängerin dynamisch miteinander verknüpft sein. Das bedeutet, dass die übermittelte TAN nur für diesen Zahlvorgang eingesetzt werden kann. Jedoch ist die SCA auch für Kreditkartenunternehmen und Online-Händler ein Thema, da die zweite Zahlungsdienstrichtlinie (Payment Services Directive 2, PSD2) grundsätzlich auch im E-Commerce bei Kartenzahlung die starke Kundenauthentifizierung vorsieht. Probleme bei der Implementierung des Verfahrens zur Absicherung von Kreditkartenzahlungen führten zu einem offiziellen Aufschub durch die EBA (European Banking Authority). Bis Ende 2020 konnten Kreditkartenzahlungen ohne den Einsatz der starken Kundenauthentifizierung vorgenommen werden und wurden auch nicht durch die Regulierungsbehörde BaFin (Bundesanstalt für Finanz-

dienstleistungsaufsicht) beanstandet. Seit Anfang 2021 muss jedoch zusätzlich zur Eingabe der Kreditkartendaten ein weiterer Schritt zur Ausführung der Zahlung durchgeführt werden.

3D-SECURE

3D-Secure ist der technische Name des Sicherheitsstandards, der in früheren Versionen bei Zahlungen mit Kreditkarten im Internet schon seit einiger Zeit eingesetzt wird. Dieser wurde für die Anforderungen der PSD2 jedoch komplett überarbeitet. Die einzelnen Kreditkartenunternehmen betreiben das Verfahren jeweils unter ihrem eigenen Label: Mastercard® Identity Check (ehemals Mastercard SecureCode), Visa Secure (ehemals Verified by Visa), Safe Key von American Express und J/Secure™ von JBC (Japan Credit Bureau).

WIE FUNKTIONIERT ES?

Bei einem Einkauf im Internet, einer sogenannten Card-Not-Present-Transaktion, musste die Kundin oder der Kunde bisher lediglich die auf der Karte aufgedruckten Daten - die Kartennummer, den Namen des Karteninhabers, das Gültigkeitsdatum und die Kartenprüfnummer (CVC) - eingeben. In Verbindung mit 3D-Secure sind diese Angaben nicht mehr ausreichend, so dass eine zusätzliche Authentifizierung erforderlich ist.

Zur Nutzung von 3D-Secure muss sich die Karteninhaberin oder der Karteninhaber bei der Bank registrieren, die die Kreditkarte ausgestellt hat. Dies kann auch einmalig während des Bezahlprozesses erfolgen. In der Regel nutzt die Kundin oder der Kunde dann die gleichen Authentisierungsmittel, die sie oder er auch beim Online-Banking verwendet. Insgesamt ähnelt der Vorgang dem Freigeben einer Zahlung beim Online-Banking.

Die Kundin oder der Kunde selbst kann letztendlich nicht beeinflussen, ob Zahlungen mit oder ohne 3D-Secure authentifiziert werden. Die Entscheidung liegt in letzter Instanz bei der Bank, und so ist ein Einfluss der Kundin oder des Kunden nur mittelbar über den Transaktionsbetrag und weitere Risikoparameter möglich.

AUSNAHMEN

3D-Secure muss nicht zwingend für jede Zahlung mit Kreditkarte zum Einsatz kommen. In der PSD2 wurden dazu Ausnahmen festgelegt:

- Transaktionen mit Kleinbeträgen bis zu 50 EUR. Sobald jedoch der Gesamtbetrag der ohne SCA geleisteten Zahlungen 150 Euro überschreitet oder 5 Zahlungen geleistet wurden, wird die SCA angefordert.
- Abonnements oder wiederkehrende Transaktionen mit einem festen Betrag. Erst bei einer Betragsänderung ist 3D-Secure erforderlich.
- Whitelist-Händlerinnen und -Händler, die von Kunden als „Vertrauenswürdige Empfänger“ deklariert wurden. Damit vermeiden Kundinnen und Kunden, die regelmäßig bei einem bestimmten Unternehmen einkaufen, die Anwendung der SCA.
- Versandhandels- und Telefonbestellungen sind vollständig von 3D-Secure ausgenommen, da sie nicht als „elektronische“ Zahlungen gelten.

Die genauen Ausnahmen von 3D-Secure Zahlungen sind auf der Webseite der entsprechenden Bank zu finden.

WIE SICHER IST 3D-SECURE?

Wie beim Online-Banking hängt die Sicherheit von 3D-Secure vom verwendeten Authentifizierungsverfahren ab. Grundsätzlich ist ein statisches Verfahren, wie die Nutzung eines Passworts, unsicherer als ein dynamisches Verfahren, wie eine Transaktion via Chip-TAN. Generell bietet die Starke Kundenauthentifizierung mit ihren zusätzlichen Faktoren jedoch eine deutlich erhöhte Sicherheit im Vergleich zu den bisher üblichen Card-Not-Present-Transaktionen. Zusätzlich kommt es darauf an, dass die Kundin und der Kunde sorgfältig mit ihren bzw. seinen Daten umgehen. Passwörter, PINs oder TANs sollten nie weitergegeben, versendet oder gemeinsam mit den Karten aufbewahrt werden.

Das 3D-Secure-Verfahren ist sowohl für den Einsatz im Web als auch in Apps geeignet. Somit können die biometrischen Schnittstellen, wie Fingerabdruckscanner oder Gesichtserkennung, zur Authentifizierung verwendet werden. Dies kann ebenfalls die Sicherheit erhöhen.

FAZIT

Zur Nutzung von 3D-Secure ist eine Registrierung bei der Bank erforderlich. Es entstehen jedoch keine zusätzlichen Kosten für die Nutzerin oder den Nutzer. Da Informationen benötigt werden, die über die auf der Karte ablesbaren hinausgehen, ist das Verfahren sicherer als die alleinige Eingabe der Kreditkartendaten. Ein Betrug wird erschwert, da eine wirkliche Authentifizierung der Kundin oder des Kunden stattfindet. ■

Weitere Informationen zu der Broschüre „Sicher Zahlen im E-Commerce“ unter:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sicher_zahlen_im_E_Commerce.pdf

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/online-banking-online-shopping-und-mobil-bezahlen_node.html

Das Motto als Programm:

#einfachaBSIchern

Bundesweite Kampagne des BMI und BSI gestartet

Die Digitalisierung ist in unserem Alltag längst vielfältig präsent. Die Auswirkungen der Corona-Pandemie haben diese Entwicklung weiter beschleunigt. Viele arbeiten im Home-Office, Schulkinder haben Fernunterricht über Video-Konferenzen und das Einkaufen geschieht vielfach online. Der „Kinoabend" findet auf dem heimischen Sofa über das Smart-TV statt, Erlebnisse werden virtuell über Soziale Netze geteilt und Reisen finden eher in virtuellen Welten beim Online-Gaming als in der realen Welt statt. Diese alltagsnahen Situationen greifen die ersten Motive der bundesweiten Kampagne des Bundesministerium des Innern, für Bau und Heimat (BMI) und des BSI zum Thema Informationssicherheit auf und zeigen die fast grenzenlosen Möglichkeiten der Digitalisierung.

Doch auch Cyberkriminelle und HackerInnen wissen um die gestiegene Nutzung digitaler Anwendungen: Sie versuchen jeden Tag viele tausend Male in Computernetze und Rechner einzudringen. Sie legen zum Beispiel digitale Geräte und Netzwerke lahm oder stehlen oder verschlüsseln die dort gespeicherten Daten, um Lösegeld zu erpressen. Die Bedrohungslage ist weiterhin angespannt, denn Cyberkriminelle nutzen die zunehmende digitale Vernetzung für ihre kriminellen Aktivitäten. Deshalb gilt mehr als jemals zuvor: Erfolgreiche Digitalisierung funktioniert nur mit Informationssicherheit – und Informationssicherheit braucht die aktive Mitwirkung von Verbraucherinnen und Verbrauchern.

DIE KAMPAGNE

Unter dem Slogan „einfachaBSIchern" starten das BMI und das BSI deshalb eine gemeinsame bundesweite Informations- und Sensibilisierungskampagne zum Thema Informationssicherheit.

Der Entschluss für eine gemeinsame Kampagne geht auf den Doxing-Vorfall Ende 2018/Anfang 2019 zurück, bei dem persönliche Daten zahlreicher Personen des öffentlichen Lebens im Internet veröffentlicht wurden. Daraufhin hat das BSI eine Online-Umfrage durchgeführt, um zu erfahren, zu welchen Gefahren in der Cyber-Welt Internetnutzerinnen und -nutzer informiert werden möchten. Das Ergebnis insgesamt: Mehr als 70 Prozent der Befragten wünschen sich mehr Informationen über Risiken im Netz und eine größere Unterstützung im Bereich der digitalen Sicherheit. Mit der Kampagne wird diesem Wunsch nach Unterstützung, dem gestiegenen Informationsbedürfnis und der zunehmenden Bedeutung digitaler Anwendungen im Alltag der Verbraucherinnen und Verbraucher Rechnung getragen.

ZIEL DER KAMPAGNE

Mit der Informationskampagne „einfachaBSIchern" sollen das Risikobewusstsein und die Kompetenzen der Verbraucherinnen und Verbraucher gestärkt werden. Damit sie sich sicher im Netz bewegen und die Chancen der Digitalisierung sicher nutzen können. Das BSI als die Cyber-Sicherheitsbehörde des Bundes bietet hierzu ein breites Informationsangebot, das durch die Kampagne noch bekannter gemacht werden soll.

AUSRICHTUNG DER KAMPAGNE

Die übergeordnete Kernbotschaft „einfachaBSIchern" der deutschlandweiten Kampagne ist positiv, motivierend und aktivierend. Sie soll breite Teile der Bevölkerung ansprechen und deutlich machen, dass sich jede und jeder – unabhängig vom eigenen Wissenstand – vor den Gefahren im digitalen Raum besser schützen kann. Hierfür zeigen die Motive der Kampagne typische digitale Nutzungsszenarien aus der alltäglichen Lebenswelt der Verbraucherinnen und Verbraucher.

UMSETZUNG DER KAMPAGNE

Die Kampagne ist zunächst für zwei Jahre Laufzeit und mehrstufig angelegt. Die Hauptkampagne richtet sich an eine breite Zielgruppe und greift fünf digitale Lebenswelten auf, zu denen Verbraucherinnen und Verbraucher über die Kampagnenwebseite konkrete Tipps des BSI finden. In Themenkampagnen werden einzelne IT-Sicherheitsthemen vertieft und gezielt für die unterschiedlichen Zielgruppen aufbereitet. Ziel ist es, konkrete

„DIGITALER VERBRAUCHERSCHUTZ IM BSI“
Als unabhängige und neutrale Anlaufstelle bietet das BSI umfangreiche Informationen und Hilfestellungen zu Fragen der Informations- und Cyber-Sicherheit. Denn Verbraucherinnen und Verbraucher leisten einen wichtigen Beitrag zu mehr digitaler Sicherheit in der Gesellschaft, indem sie die wichtigsten Sicherheitsvorkehrungen auch in der privaten Internetnutzung beachten und umsetzen. Die nebenstehende visuelle Darstellung steht für alle Angebote, die das BSI im Rahmen des digitalen Verbraucherschutzes für die Gesellschaft zur Verfügung stellt. Es soll verdeutlichen, dass jeder Internetnutzer und jede Internetnutzerin mit einem entsprechenden Sicherheitsverhalten im digitalen Raum einen Beitrag zur Cyber-Sicherheit in ganz Deutschland leistet.

Bislang stellte das BSI auf seiner Webseite „BSI für Bürger“ digitale Risiken und Empfehlungen für Privatanwenderinnen und Privatanwender zusammen. Von nun an finden Sie auf der Webseite des BSI im Bereich „Verbraucherinnen und Verbraucher“ wichtige Sicherheitsempfehlungen, Informationen zu Sicherheitsrisiken bzw. Angriffsmethoden sowie Kontakt- und Beteiligungsmöglichkeiten.
Denn digitale Sicherheit wird im Sinne eines digitalen Verbraucherschutzes immer wichtiger – für einzelne Anwenderinnen und Anwender ebenso wie für die Gesellschaft. Die Etablierung grundlegender Sicherheitsstandards und die Information sowie Sensibilisierung der Verbraucherinnen und Verbraucher ist daher eine Aufgabe, der sich das BSI als die Cyber-Sicherheitsbehörde des Bundes mit dem digitalen Verbraucherschutz stellt.

Handlungskompetenzen jedes Einzelnen zu stärken. Insgesamt wird die Kommunikation der Kampagne einen starken digitalen Fokus haben und mit Aktionen wie Veranstaltungen für Verbraucherinnen und Verbraucher in die Breite der Gesellschaft wirken. So sollen möglichst viele Menschen erreicht und befähigt werden, sich selbst angemessen zu schützen. Damit das Motto „einfachaBSIchern“ zum (Standard-) Programm wird und wir alle die Vorzüge der Digitalisierung sicher nutzen können. ■

Weitere Informationen:

https://www.bsi.bund.de/DE/Themen/Kampagne-einfach-absichern/kampagne_node.html

Digital leben: frei, individuell und sicher

Neuer Videospot zum 30-jährigen Bestehen des BSI

Der offizielle Auftakt in das BSI-Jubiläumsjahr war der 17. Deutsche IT-Sicherheitskongress am 2. und 3. Februar 2021 unter dem Motto „Deutschland. Digital. Sicher. 30 Jahre BSI“. Die Veranstaltung fand in diesem Jahr erstmals in digitaler Form statt – und mit über 8.000 Teilnehmerinnen und Teilnehmern verzeichnete das BSI eine Rekordkulisse. Auf dem Kongress feierte der neue Videospot des BSI Premiere.

VON DER IDEE ZUM FILM

Zu seinem 30-jährigen Jubiläum hat sich das BSI anstelle einer klassischen Festschrift für ein Video-Format entschieden, das die Bedeutung der Digitalisierung im Alltag deutlich macht: Der Spot „Digital leben“ greift die Chancen der Digitalisierung auf und zeigt, in welchen Anwendungsfeldern das BSI als kompetenter Berater für Wirtschaft, Wissenschaft, Staat und Gesellschaft eine sichere Digitalisierung in Deutschland voranbringen kann. Ob für Jung oder Alt, für Freizeit oder Arbeit, für Einzelpersonen oder Gruppen: Informationssicherheit und Digitalisierung gehören untrennbar zusammen. Sie sind zwei Seiten einer Medaille und des BSI. Wie die Digitalisierung für alle sicher nutzbar gemacht werden kann - ganz egal, wie die individuelle Lebenswelt aussieht – will das BSI in dem prägnanten und emotionalen Videospot verdeutlichen. Das Ziel war ein maximal 90 Sekunden langer Film, der in einzelnen Kurzepisoden jeweils eine kleine Alltagsgeschichte mit digitalen Anwendungen zeigt. Jede einzelne Szene sollte zudem allein funktionieren – und so als Kurzspot in den sozialen Medien verwendbar sein, um auf die Informationsangebote des BSI aufmerksam zu machen.

BEHIND THE SCENES: FILMDREH IN CORONA-ZEITEN

Die Idee stand, ein Drehbuch, das vielfältige Lebenssituationen, Menschen und digitale Anwendungen zeigt, war geschrieben. Doch wie dreht man einen Film mit unterschiedlichen Locations und Protagonisten unter den besonderen Umständen der Corona-Pandemie? Der Anspruch war so klar wie anspruchsvoll: Wir drehen nur dann, wenn die größtmögliche Sicherheit für Darsteller und Filmcrew gegeben ist. So entstand ein ausgeklügeltes Hygienekonzept und ein ständig am Set befindlicher Hygienebeauftragter sorgte für dessen strenge Einhaltung. Im Ergebnis gelang durch den besonderen Einsatz aller Beteiligten ein ungewöhnlicher, aber sicherer Dreh in besonderen Zeiten.

Der Link zum neuen BSI-Videospot:

http://www.bsi.bund.de/videospot

BSI Basis-Tipp

Level Up statt Game Over!

Quizzen mit dem Handy während der Zugfahrt, Autorennen auf der Konsole oder das Bauen futuristischer Städte am PC? So abwechslungsreich die digitale Spielwelt mittlerweile ist, so vielseitig ist auch der Nutzerkreis. Ob Schülerin oder Rentner – die Hälfte der Deutschen spielt regelmäßig.

Doch auch Cyber-Kriminelle nutzen das Spieleuniversum für ihre Machenschaften. Umfassende Games-Bibliotheken und in Profilen hinterlegte Kontodaten sind wahre Goldgruben für die Angreifer. Schnell kann das Spielvergnügen ruiniert sein: Nur kurz den Spiele-Einladungslink eines Freundes angeklickt und Benutzerdaten eingegeben – schon kann man Opfer eines Phishing-Angriffes sein. Hacker nutzen so erbeutete Anmeldedaten, um diese beim sogenannten „Credential Stuffing“ für eine Vielzahl anderer Accounts auszuprobieren. Damit erhalten sie nicht nur Zugriff auf die jeweiligen Spiele, sondern möglicherweise auch auf das hinterlegte E-Mail-Postfach.

Weitere Informationen und ein spannendes Interview mit einem BSI-Experten zum sicheren Gamen:

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

Spielregeln für die digitale Sicherheit beim Gamen

- **Aus sicheren Quellen herunterladen:**
  Beziehen Sie Spiele-Software oder Apps nur aus vertrauenswürdigen Quellen wie der offiziellen Herstellerseite oder dem offiziellen App-Store. Damit vermeiden Sie die Installation von versteckter Schadsoftware auf Ihrem Endgerät.
- **Sichere Passwörter und Zwei-Faktor-Authentisierung nutzen:**
  Bilden Sie Passwörter, die nicht von anderen erraten werden können, und nutzen Sie Möglichkeiten der Zwei-Faktor-Authentisierung, damit Ihre Spiele-Accounts nicht leicht gehackt werden können. Passwortmanager merken sich auch Ihr schwierigstes Passwort.
- **Sicherheitseinstellungen von Benutzerkonten prüfen:**
  Für Spiele auf Konsolen und Spieleplattformen werden oft Benutzerkonten benötigt. Wägen Sie bei der Nutzung von kritischen Funktionen – wie automatischen Bezahlvorgängen – zwischen Risiken und Komfort ab. Automatisierte Vorgänge könnten bei Diebstahl des Endgerätes zu hohen finanziellen Schäden führen.
- **Wenige persönliche Infos preisgeben:**
  Hinterlegen Sie nur notwendige Daten und verknüpfen Sie Ihre Spiele-Accounts nicht mit Ihren sozialen Netzwerken. Persönliche Informationen können für die Kopie Ihrer Online-Identität missbraucht werden.
- **Regelmäßig Updates installieren:**
  Aktualisieren Sie Software und Hardware regelmäßig, um Schadprogrammen kein Einfallstor auf Ihr Endgerät zu bieten.

Bestellen Sie Ihr BSI-Magazin!

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Referat Cyber-Sicherheit für den
Bürger und Öffentlichkeitsarbeit

Postfach 20063
53133 Bonn
Telefon: +49 (0) 228 99 9582 0
Telefax: 0228 99 9582-5455
E-Mail: bsi-magazin@bsi.bund.de

Zweimal im Jahr gibt das BSI-Magazin „Mit Sicherheit“ Einblick in nationale und internationale Cyber-Sicherheitsthemen, die digitale Gesellschaft sowie IT-Sicherheit in der Praxis. Lassen Sie sich jetzt direkt nach Erscheinen zur Hannover Messe im April und zur it-sa im Oktober die aktuellste Ausgabe bequem per Post zusenden, indem Sie sich mit unten stehendem Formular für den Abo-Verteiler anmelden.

Ich möchte die folgende BSI-Publikation im Abo erhalten:

☐ BSI-Magazin „Mit Sicherheit“ (2 x im Jahr, Print)
☐ Die Lage der IT-Sicherheit in Deutschland (1 x im Jahr, Print)

Name, Vorname

Organisation

Straße

PLZ, Ort

E-Mail

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

Datum/Unterschrift:

Verantwortliche Stelle für die Verarbeitung Ihrer oben genannten personenbezogenen Daten ist das Bundesamt für Sicherheit in der Informationstechnik, Postfach 200363, 53133 Bonn. Die von Ihnen angegebenen Daten werden ausschließlich für die Verwaltung des Versands bzw. die Übermittlung der Informationen verwendet, zu denen Sie oben zugestimmt haben. Sie können diese Einwilligung jederzeit widerrufen. Hierzu genügt eine E-Mail an bsi-magazin@bsi.bund.de. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Weitere Informationen darüber, wie wir Ihre personenbezogenen Daten bei uns verarbeiten und welche Rechte Ihnen diesbezüglich zustehen, können Sie den beigefügten „Datenschutzrechtlichen Hinweisen“ zur Bestellung von BSI-Publikationen entnehmen. Einfach das Formular per Fax oder E-Mail einsenden:
Telefax: 0228 99 9582-5455 | E-Mail: bsi-magazin@bsi.bund.de

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

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

Folgen Sie dem BSI auch auf Facebook und Twitter!
www.facebook.com/bsi.fuer.buerger | www.twitter.com/bsi_presse
Weitere Informationen sowie Checklisten und Tipps rund um Cyber-Sicherheit finden Sie unter:
www.bsi.bund.de | www.bsi-fuer-buerger.de | www.allianz-fuer-cybersicherheit.de
Datenschutzrechtliche Hinweise: https://www.bsi.bund.de/datenschutzrechtliche-hinweise

IMPRESSUM

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI) 53175 Bonn
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Referat WG24 – Öffentlichkeitsarbeit Godesberger Allee 185–189 53175 Bonn Telefon: +49 (0) 228 999582-0 E-Mail: bsi-magazin@bsi.bund.de Internet: www.bsi.bund.de
Stand:	Juni 2021
Texte und Redaktion:	Nora Basting und Mark Schulz, Bundesamt für Sicherheit in der Informationstechnik (BSI); FAKTOR 3 AG
Konzept und Gestaltung:	FAKTOR 3 AG Kattunbleiche 35 22041 Hamburg www.faktor3.de
Druck:	Appel und Klinger Druck & Medien GmbH Bahnhofstraße 3 96277 Schneckenlohe Internet: www.ak-druck-medien.de
Artikelnummer:	BSI-Mag 21/713-1
Bildnachweise:	Titel: Composing FAKTOR 3 AG - GettyImages © Matt Nolan_EyeEm, GettyImages © Westend61; S. 4-5: Mockup FAKTOR 3 AG, BSI; S. 6: GettyImages © Paper Boat Creative; S. 11: GettyImages © BlackJack3D, Illustration: US Verteidigungsministerium, 2013; S. 15: © Freepik.com, BSI; S. 18-19: GettyImages © smartboy10; S. 20-21: © Freepik.com; S. 22-23: © Bundesregierung/Kühler, Bernd; S. 26: © BSI; S. 30-31: GettyImages © DrAfter123, Freepik.com, BSI; S. 32-34: © Freepik.com; S. 36-39: © Freepik.com, BSI; S. 40-41: © BSI; S. 43-45: GettyImages © D3Damon, BSI; S. 46: © BSI; S. 48: © BSI; S.51: © BSI; S. 53: © BSI; S. 54-55: © Schleswig-Holsteinischer Landtag; S. 56-57: © BSI; S. 58-59: GettyImages © VENTRIS / SCIENCE PHOTO LIBRARY; S. 61: GettyImages © Image Source; S. 62: GettyImages © Westend61; S. 65: BSI/BMI; S. 66-67: BSI/BMI; S. 68: GettyImages © ilbusca;

Das BSI-Magazin erscheint zweimal im Jahr. Es ist Teil der Öffentlichkeitsarbeit des BSI.

Es wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

Für die digitale Version des BSI-Magazins scannen Sie den QR-Code

https://www.bsi.bund.de/BSI-Magazin

www.bsi.bund.de