BSI-Magazin 2022/02

Mit Sicherheit

Im Blickpunkt:

Digitale Erpressung mit Ransomware

Cyber-Sicherheit

Automotive Security:
Von der Produktion bis ins Fahrzeug

BSI International

BSI und NATO:
Cloud-Sicherheit im Bündnis gestalten

Digitale Gesellschaft

Sicherheit statt Risiko:
Digitaler Verbraucherschutz im BSI

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Editorial

Sehr geehrte Leserinnen und Leser,

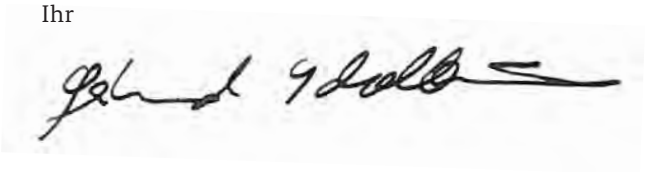
Berichte über Cyber-Sicherheitsvorfälle und Cyber-Angriffe auf Unternehmen und Institutionen sind inzwischen fester Bestandteil der Nachrichtenlage. Die weiter voranschreitende Digitalisierung unseres Alltags und vieler Geschäftsprozesse bietet – neben den vielfältigen Vorteilen – auch mehr Angriffsfläche für Cyber-Kriminelle. Deshalb sind Cyber-Sicherheit und solide Schutzmaßnahmen gegen digitale Bedrohungen für Staat, Wirtschaft und Gesellschaft heute wichtiger denn je. Dazu kommt: Die Bedrohung im Cyber-Raum ist angespannt, dynamisch und vielfältig und damit so hoch wie nie. Diese Entwicklung belegt der im Oktober veröffentlichte BSI-Bericht „Die Lage der IT-Sicherheit in Deutschland 2022".

Eine zentrale Erkenntnis des Lageberichts ist, dass Erpressung mit Ransomware weiterhin die Hauptbedrohung im Cyber-Raum ist. Hier standen besonders umsatzstarke Unternehmen im Fokus der Angreifer. Diese Angriffe können mit verschlüsselten Daten Druck auf die Betroffenen ausüben und damit ganze Geschäftsprozesse lahmlegen. Die betroffene Verwaltung eines Landkreises hatte 207 Tage mit den Folgen eines Ransomware-Angriffs zu tun. Aber auch Verbraucherinnen und Verbraucher sind Ziele von Cyber-Erpressung. Diese Erkenntnis bestätigt auch das Digitalbarometer 2022, das im November vorgestellt wurde. Neben Detektion und Reaktion ist Prävention eine zentrale Säule unserer Arbeit. Für die Gefahr durch Ransomware möchten wir Sie in der aktuellen Ausgabe des BSI-Magazins sensibilisieren: Unsere Fachkolleginnen und -kollegen haben dazu einen Schwerpunkt zu den unterschiedlichen Aspekten der digitalen Erpressung zusammengestellt.

Doch wir als Gesellschaft sind der Bedrohung im Cyber-Raum nicht schutzlos ausgeliefert. In vielzähligen Projekten haben wir – auch gemeinsam mit externen Partnern – Lösungsansätze erarbeitet, die das verdeutlichen. Spannende Einblicke erhalten Sie in der aktuellen Ausgabe beispielsweise in die Datensicherheit von Verbraucherinnen und Verbrauchern, die Cyber-Sicherheit in der Automobilbranche, die internationale Arbeit des BSI im NATO-Bündnis sowie in das noch recht neue Angebot für Kommunen, die BSI-Roadshow. Als Cyber-Sicherheitsbehörde des Bundes leistet das BSI täglich einen ganzheitlichen Beitrag für die digitale Sicherheit in Deutschland. Denn Informationssicherheit ist die Voraussetzung für eine nachhaltige Digitalisierung.

Ich wünsche Ihnen eine interessante Lektüre.

Ihr



Dr. Gerhard Schabhüser,
Vizepräsident des Bundesamts für Sicherheit
in der Informationstechnik

Inhalt

Cyber-Sicherheit

Im Blickpunkt:

Das BSI

IT-Sicherheit in der Praxis

BSI International

Digitale Gesellschaft

Anerkannt: Cyber-Sicherheits-kennzeichen

BSI-Vizepräsident Dr. Gerhard Schabhüser und CEO der Cyber Security Agency Singapore (CSA), David Koh, unterzeichnen bilaterale Vereinbarung.

BSI UND SINGAPUR ERKENNEN CYBER-SICHERHEITSKENNZEICHEN GEGENSEITIG AN

BSI-Vizepräsident Dr. Gerhard Schabhüser und der Chief Executive der Cyber Security Agency Singapore (CSA), David Koh, haben auf der diesjährigen Singapore International Cyber Week (SICW) eine bilaterale Vereinbarung zur gegenseitigen Anerkennung des Cybersecurity Labelling Scheme (CLS) und des deutschen IT-Sicherheitskennzeichens unterzeichnet.

Produkte mit dem deutschen IT-Sicherheitskennzeichen des BSI können in Singapur nun ein Cybersecurity Label der Stufe 2 erhalten. Kennzeichen aus Singapur der Stufe 2 oder höher ermöglichen es Herstellern, ein vereinfachtes Antragsverfahren zur Erteilung des deutschen IT-Sicherheitskennzeichens zu durchlaufen. Durch die gemeinsame Vereinbarung mit der CSA baut das BSI die Kooperation mit internationalen Cyber-Sicherheitsbehörden weiter aus. Die gemeinsame Vereinbarung bestätigt die Bedeutung des IT-Sicherheitskennzeichens als Blaupause für die Gestaltung europäischer und internationaler Kennzeichen.

Mit Hilfe des IT-Sicherheitskennzeichens können sich Verbraucherinnen und Verbraucher über die von Herstellern und Anbietern zugesicherten Sicherheitseigenschaften vernetzter, internetfähiger Produkte und Dienste ganz einfach per Kurzlink oder QR-Code informieren.

Videoreihe Cyber-Sicherheit²: 3. Staffel erschienen

APP-SICHERHEIT – IM GESPRÄCH MIT EXPERTINNEN UND EXPERTEN

Apps sind ständige Begleiter unseres digitalen Alltags. Ob Schrittzähler, Kalender oder Messenger – ihre Nutzung hat viele unserer Lebensbereiche durchdrungen.

Dabei können sie auch ein Sicherheitsrisiko bedeuten. Viele Sicherheitseinstellungen werden von Apps, wenn überhaupt, nur bei der Installation abgefragt und geraten danach bei vielen Nutzerinnen und Nutzern schnell wieder in Vergessenheit. Dabei gibt es viele Einstellungen, die für mehr Sicherheit bei der Nutzung von Apps sorgen können. In den sieben Folgen zum Thema App-Sicherheit sprechen Michaela Hansert (BSI-Referat Informationssicherheitsberatung für Länder und Kommunen) und Martin Bregenzer (EU-Initiative klicksafe) über Risiken, die wichtigsten Sicherheitseinstellungen, Datensicherheit und Datenschutz, Geräte- und Jugendschutz sowie Messenger-Apps.

Jetzt reinschauen und app-sichern:

Playlist auf YouTube:
https://www.youtube.com/playlist?list=PLUE-Po9QCkRA5RXHrbWsZdv8xPXIWSwPCu

Das BSI im Exekutivrat von ENISA

Horst Samsel – für das BSI und ENISA aktiv

Im Juni 2022 wurde Horst Samsel, Leiter der Abteilung Beratung für Bund, Länder und Kommunen im BSI, als Vertreter für Deutschland in den Exekutivrat der Agentur der Europäischen Union für Cybersicherheit (ENISA) gewählt. Das BSI vertritt Deutschland bereits langjährig im ENISA-Verwaltungsrat und engagiert sich in zahlreichen Facharbeitsgruppen.

Mit der Wahl von Horst Samsel in den Exekutivrat kann das BSI die ENISA noch stärker und gezielter bei der Erfüllung ihrer Mandatsaufgaben unterstützen. Es möchte in diesem Zusammenhang darauf hinwirken, dass die Agentur verstärkt als Multiplikator für Expertise zu Fragen der Cyber-Sicherheit auf EU-Ebene und als Austauschplattform für die Zusammenarbeit zwischen den Mitgliedstaaten und anderen Interessenträgern wirken kann.

Die momentanen Schwerpunkte der ENISA-Arbeit sind das Voranbringen von Zertifizierungsschemata gemäß Cybersecurity Act (CSA) und die Unterstützung operativer Zusammenarbeit in der EU. Zukünftig wird die Unterstützung der Mitgliedstaaten bei der Umsetzung der zweiten europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS2-Richtlinie) im Fokus stehen.

ENISA hat seit 2019 ein dauerhaftes Mandat durch den CSA erhalten. Das übergeordnete Ziel ist es, ein hohes gemeinsames Maß an Cyber-Sicherheit in der gesamten Union zu erreichen.

Neues deutsch-französisches Lagebild veröffentlicht

Das BSI hat gemeinsam mit der französischen Behörde für Informationssicherheit, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), ein Lagebild veröffentlicht. In der fünften gemeinsamen Veröffentlichung von BSI und ANSSI geht es um das Thema Zertifizierung. Mit besonderem Augenmerk auf das im Sommer geschlossene Abkommen zur gegenseitigen Anerkennung von BSZ (Beschleunigte Sicherheitszertifizierung und CSPN (Certification de Sécurité de Premier Niveau) Zertifikaten gelegt.

Neue Broschüren zur Cyber-Sicherheit für KMU und ePayment-Lösungen

Die Broschüre „Cyber-Sicherheit für KMU" bietet kleinen und mittleren Unternehmen einen leicht verständlichen Einstieg, um ihr Cyber-Sicherheitsniveau zu verbessern. Anhand von 14 Fragen werden die wichtigsten Aspekte beleuchtet und praktikable Hinweise gegeben. Die neue Veröffentlichung „ePayment – Schlüssel der Digitalisierung" bietet eine Checkliste für Behörden, die Online-Bezahlverfahren einführen wollen. Zudem werden auch grundlegende Informationen, die bei elektronischen Zahlverfahren in Behörden wichtig sind, erläutert.

Alle BSI-Publikationen finden Sie hier:

BSI-Publikationen:
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/publikationen_node.html

Automotive Security: Cyber-Sicherheit von der Produktion bis ins Fahrzeug

von Marco Krambrich, Referat Nationales IT-Lagezentrum, Analysen und Prognosen

Nach wie vor sind die Auswirkungen der Corona-Pandemie in der Automobilbranche spürbar – überall, aber insbesondere in den Bereichen von Zulieferteilen, -produkten oder -dienstleistungen. Maßgeblich geprägt wird die Lage jedoch momentan durch den Angriffskrieg Russlands gegen die Ukraine und die damit verbundenen wirtschaftlichen und zunehmend auch Cyber-Sicherheitsrelevanten Auswirkungen auf die deutsche Automobilindustrie. Eine Zwischenbilanz.

Cyber-Angriffe werden qualitativ immer ausgereifter und zielgerichteter. Ransomware-Angriffe sind aus Sicht des BSI weiterhin die größte operative Bedrohung der Cyber-Sicherheit – insbesondere für die IT-Systeme der Automobilhersteller und ihrer Zulieferer. So hatte beispielsweise jüngst ein deutscher Autoteilezulieferer durch Ransomware mit massiven Produktionsausfällen in zahlreichen Werken zu kämpfen. Die Produktion konnte erst einen Monat später wieder weitgehend in den Normalbetrieb überführt werden.

Es kommt erschwerend hinzu, dass der russische Angriffskrieg gegen die Ukraine zunehmend durch Maßnahmen im Cyber-Raum begleitet wird, die auch Auswirkungen auf die deutsche Automobilindustrie haben und die Cyber-Sicherheit gefährden. Dazu gehören DDoS-Angriffe mit dem Ziel, ganze Webseiten lahmzulegen sowie intensive Aktivitäten sogenannter Hacktivisten.

In der kürzlich erschienenen zweiten Ausgabe des Branchenlagebildes „Automotive 2021/2022“ präsentiert das BSI einen branchenspezifischen Überblick zur Lage der Cyber-Sicherheit in diesem Bereich und stellt Informationen zu Vorfällen und Schwachstellen zur Verfügung.

Weitere Informationen:

Branchenlagebild Automotive:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2021_2022.html?nn=520690

CYBER-SICHERHEIT IM FAHRZEUG SOWIE IN DIGITALEN PRODUKTEN

Die Digitalisierung bleibt neben der Elektromobilität ein bestimmendes Thema für die Automobilbranche. Die Cyber-Sicherheit der Fahrzeugsysteme ist dabei eine Schlüsseleigenschaft für eine erfolgreiche Umsetzung der Digitalisierung. Neu eingeführte Regelungen verpflichten die Hersteller, Cyber-Sicherheit in der Produktentwicklung zu berücksichtigen und ein Cyber-Sicherheitsmanagement aufzubauen, das im Fall neu auftretender Schwachstellen entsprechende Gegenmaßnahmen schnell ermöglicht.

Verschiedene Forschungsarbeiten haben die Anfälligkeit von Fahrzeugsystemen für Cyber-Attacken, die über eine Funkverbindung verfügen oder mit Hintergrundsystemen vernetzt sind, verdeutlicht. Dazu gehören:

- der Ausfall von Infotainmentsystemen durch fehlerhafte Metadaten
- das Öffnen von Fahrzeugen durch ungesicherte API-Token
- Replay-Angriffe auf Schließsysteme
- die Unterbrechung von Schnellladevorgängen.

VERNETZTES FAHREN

Die Entwicklung des automatisierten und autonomen Fahrens schreitet weiterhin stark voran, weil immer mehr Rechenleistung und immer größere Datenmengen zur Verfügung stehen, um Verfahren und Systeme mit Künstlicher Intelligenz (KI) weiterzuentwickeln. Neben der Umsetzung neuer Funktionalitäten und steigender Performanz schafft die Nutzung von KI im automatisierten und autonomen Fahren jedoch auch neue Herausforderungen.

CYBER-SICHERHEIT IN PRODUKTIONSANLAGEN UND -PROZESSEN

Der Grad der IT-Vernetzung und Automatisierung wird in der Produktion besonders deutlich: In modernen Fertigungsstraßen ist eine Vielzahl von Komponenten miteinander verbunden – von Sensoren bis zu Fertigungsrobotern. Mit der zunehmenden IT-Vernetzung erhöht sich aber die Angriffsfläche, da diese Systeme auch mit dem Unternehmensnetzwerk sowie Dienstleister- und Partner-/Lieferantennetzwerken verbunden sein können und teilweise über das Internet erreichbar sein sollen.

Neben der allgemeinen Gefahr durch Ransomware-Angriffe tauchen immer wieder Beispiele für Schadsoftware auf, die speziell auf industrielle Steuerungsanlagen (ICS) ausgerichtet ist. Diese verfolgen das Ziel, Informationen zu sammeln oder Manipulationen vorzunehmen.

Die Automobilhersteller tragen eine aktive Verantwortung für den Schutz ihrer eigenen IT-Systeme und -Netze und benötigen dafür ein geeignetes Schwachstellenmanagement. Wer das nicht hat, geht enorme Risiken ein, denn Produktionsausfälle infolge eines Cyber-Angriffs können schnell existenzbedrohend werden. Gemäß dem Motto des diesjährigen 18. IT-Sicherheitskongresses muss Cyber-Sicherheit daher Chefinnen- und Chefsache sein und mit ausreichenden Ressourcen zum festen Bestandteil des eigenen Risiko-Managements gemacht werden.

Auch die Verbesserung der Softwarequalität ist ein wichtiger Beitrag zur Erhöhung der Cyber-Sicherheit. Eine besondere Herausforderung sind in dieser Hinsicht die komplexen Software-Lieferketten, die das Auffinden und Beheben von Schwachstellen erschweren können. Das BSI fordert daher eine zielgerichtete Umsetzung von Maßnahmen für eine bessere Softwarequalität in IT-Produkten. Dazu unterstützt das BSI aktiv Konzepte wie beispielsweise Software Bill of Materials (SBOM)[1] und das Common Security Advisory Framework (CSAF)[2], um Coordinated Vulnerability Disclosure-Prozesse (CVD-Prozesse) zu optimieren. CVD-Prozesse dienen dem Umgang mit Meldungen über Schwachstellen in IT-Produkten und ermöglichen es Sicherheitsforschenden, die Schwachstellen in IT-Produkten entdeckt haben, diese an eine zentrale Adresse zu melden und bei deren Behebung und der geeigneten Veröffentlichung von Patches zu unterstützen.

MASSNAHMEN UND AKTIVITÄTEN DES BSI

Um den für den Wirtschafts- und Automobilstandort Deutschland sehr wichtigen Bereich der Digitalisierung sicher zu gestalten und verlässliche Rahmenbedingungen für Investitionen und Innovationen zu schaffen, arbeiten das BSI und das Kraftfahrt-Bundesamt (KBA) in Fragen der Cyber-Sicherheit eng zusammen. Mit neuen Regeln für die Genehmigung von Fahrzeugen soll beispielsweise das Thema Cyber-Sicherheit über den gesamten Lebenszyklus eines Fahrzeuges fest verankert werden, um Risiken besser vorbeugen zu können. Der für den Transfer in die Anwendung erforderliche Austausch mit der Automobilindustrie wird dabei auch proaktiv durch das BSI und den Verband der deutschen Automobilindustrie (VDA) vorangetrieben.

Für mehr Sicherheit neuer Technologien wie Künstliche Intelligenz, 5G oder Smart Home/Smart Factory gestaltet das BSI unter anderem praxisgerechte Sicherheitsanforderungen, Standards und Handlungsempfehlungen.

Neuregelungen für Unternehmen im besonderen öffentlichen Interesse (UBI) sollen zukünftig dabei helfen, ein breiteres Verständnis über die Cyber-Sicherheit dieser Unternehmen zu gewinnen, indem diese Informationen zu einschlägigen Zertifizierungen, Audits, IT-Störungen oder sonstigen Maßnahmen an das BSI übermitteln.

Die ganzheitliche Umsetzung dieser Aufgaben im Bereich „Automotive“ ist eine komplexe und vielfältige Herausforderung. Die Industrie bleibt hier gefordert, die Cyber-Sicherheit in allen Phasen und unternehmensübergreifend durch geeignete Entwicklungsprozesse zu gewährleisten. ■

[1] In einer SBOM werden alle Komponenten und Abhängigkeiten einer Software aufgelistet, um eine effiziente Überprüfung zu ermöglichen, ob eine bekannte Schwachstelle ein Produkt betrifft. [2] Ein maschinell verarbeitbares Format für Security Advisories.

Cyber-Sicherheit im Weltraum

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

„Vom Weltraum abhängig“ – so lautet der Titel eines Artikels in Ausgabe 2021/01 des BSI-Magazins, in dem die wachsende Bedeutung und Bedrohungslage für Satellitensysteme diskutiert wurde. Der Text lieferte auch erste Antworten darüber, wie sich das BSI zu dem Thema positioniert und welche Maßnahmen die Cyber-Sicherheitsbehörde des Bundes ergreift, um den neuen Herausforderungen gerecht zu werden und die Cyber-Sicherheit von Infrastrukturen im All zu stärken.

Ohne die Arbeit von Satelliten sähe unser Alltag ganz anders aus: Wir könnten uns nicht über GPS orientieren, hätten weniger guten Fernseh- und zunehmend auch weniger Internetempfang, und der Wetterbericht wäre weniger detailliert und zuverlässig.

Wie sehr Satelliten unseren Alltag beeinflussen, merken wir erst, wenn ihre Dienste ausfallen, wenn also Schutzziele wie Integrität und Authentizität mitunter auch die Vertraulichkeit der Signale und Daten nicht sichergestellt werden können.

Kritische Infrastrukturen (KRITIS) sind noch mehr als unsere Gesellschaft auf satellitengestützte Anwendungen angewiesen. Sie werden zur Erfüllung von Aufgaben wie der Überwachung des Schienen- oder Flugverkehrs, die Synchronisation von Kommunikations- und Stromnetzen und sowie zuverlässigen Finanztransaktionen eingesetzt. Gleichzeitig spielen sie eine zentrale Rolle bei der Erdbeobachtung / Erdfernerkundung, z. B. Erforschung des Klimawandels, oder der Koordinierung von Einsatzkräften im Katastrophenschutzmanagement. Aber auch im Bereich der digitalen Kommunikation werden Satelliten immer wichtiger.

Als Cyber-Sicherheitsbehörde des Bundes steht das BSI in der Verantwortung, die Informationssicherheit solcher Systeme zu stärken und die Verfügbarkeit von Diensten über integre, authentische Kommunikation sicherzustellen. Dazu hat das BSI systematisch strategische Handlungsfelder und konkrete Handlungsziele identifiziert sowie verschiedene Maßnahmen abgeleitet, die in den nächsten Jahren umgesetzt werden sollen.

ÜBERBLICK ÜBER GEPLANTE MASSNAHMEN

Ab 2023 soll ein Schwerpunktreferat für Informationssicherheit in Weltrauminfrastrukturen als zentrale, koordinierende Stelle für Cyber-Sicherheit in zivilbehördlichen sowie militärischen Luft- und Raumfahrtanwendungen und -systemen folgende Maßnahmen ergreifen:

- Identifizierung von Mindestanforderungen für Cyber-Sicherheit im Weltraum
- Erarbeitung und Fortschreibung von Vorgaben und Empfehlungen sowie entwicklungsbegleitende Beratung schon in frühen Projektphasen
- Beratung und Dienstleistungen bezüglich der Cyber-Sicherheit in den Bereichen Mindestanforderungen und Zulassung
- aktive Teilnahme an oder Durchführung von Veranstaltungen sowie die Publikation von Beiträgen mit fachlichem Bezug zu Luft- und Raumfahrtsystemen
- Standardisierung der Mindestanforderungen in Zusammenarbeit mit Partnern im internationalen Umfeld

Erste Maßnahmen sind bereits umgesetzt. So wurden 2022 gemeinsam von BSI, den Unternehmen OHB und Airbus sowie der Raumfahrtagentur im DLR Empfehlungen für eine Mindestabsicherung für Satellitenmissionen erarbeitet, die in Form eines IT-Grundschutz-Profils für Weltrauminfrastrukturen interessierten Anwendern (Hersteller, Betreiber und Zulieferer von Satellitensystemen und -komponenten) zur Verfügung gestellt worden sind.

Strategische Handlungsfelder des BSI zur Gestaltung der Cyber-Sicherheit für Weltrauminfrastrukturen

- Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung
- Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur
- Gemeinsamer Auftrag Cyber-Sicherheit von Staat und Wirtschaft
- Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik

EMPFEHLUNGEN FÜR EINE MINDESTABSICHERUNG FÜR SATELLITENMISSIONEN

Das IT-Grundschutz-Profil enthält einerseits Anforderungen anhand der im IT-Grundschutz-Kompendium definierten Bausteine. Es ergänzt jedoch spezifische Anforderungen, die im IT-Grundschutz nicht erfasst sind und die sich auf unterschiedliche Aspekte der jeweiligen Lebensphasen des Satelliten beziehen (Design und Entwicklung, Test, Transport, Startkampagne, In-Orbit-Phase, Betrieb, Außerbetriebnahme). Soweit es für die Durchführung der einzelnen Phasen relevant ist, adressiert das IT-Grundschutz-Profil auch die entsprechenden Anteile des Bodensegments. Um Empfehlungen für ein einheitliches Mindestschutzniveau für sämtliche derzeit denkbaren Satellitenmissionen zu formulieren, muss dem IT-Grundschutz-Profil eine passende Schutzbedarfskategorie („Normal“) zugrunde liegen. Nur so umfasst der Geltungsbereich der identifizierten Anforderungen jeden Satelliten, der in den Orbit gebracht wird. So wird beispielsweise empfohlen, den Baustein Kryptokonzept (CON.1) zur Kontrolle eines jeden Satelliten anzuwenden, um einen adäquaten Schutz der Vertraulichkeit, Integrität und Authentizität der Daten und der Verbindungen zu ermöglichen. Abhängig von der Mission und deren Kritikalität sollte dieser Baustein individuell angepasst werden, etwa durch die Auswahl geeigneter Kryptoverfahren.

Das BSI wird über die Umsetzung der weiteren Maßnahmen berichten und steht in Fragestellungen zur Cyber-Sicherheit im Weltraum jederzeit als fachlicher Experte zur Verfügung. ■

IT-Grundschutz-Profil

Das IT-Grundschutz-Profil dient als Muster-Sicherheitskonzept, das Institutionen der Raumfahrtbranche die Implementierung des IT-Grundschutzes erleichtern soll.

Weitere Informationen:

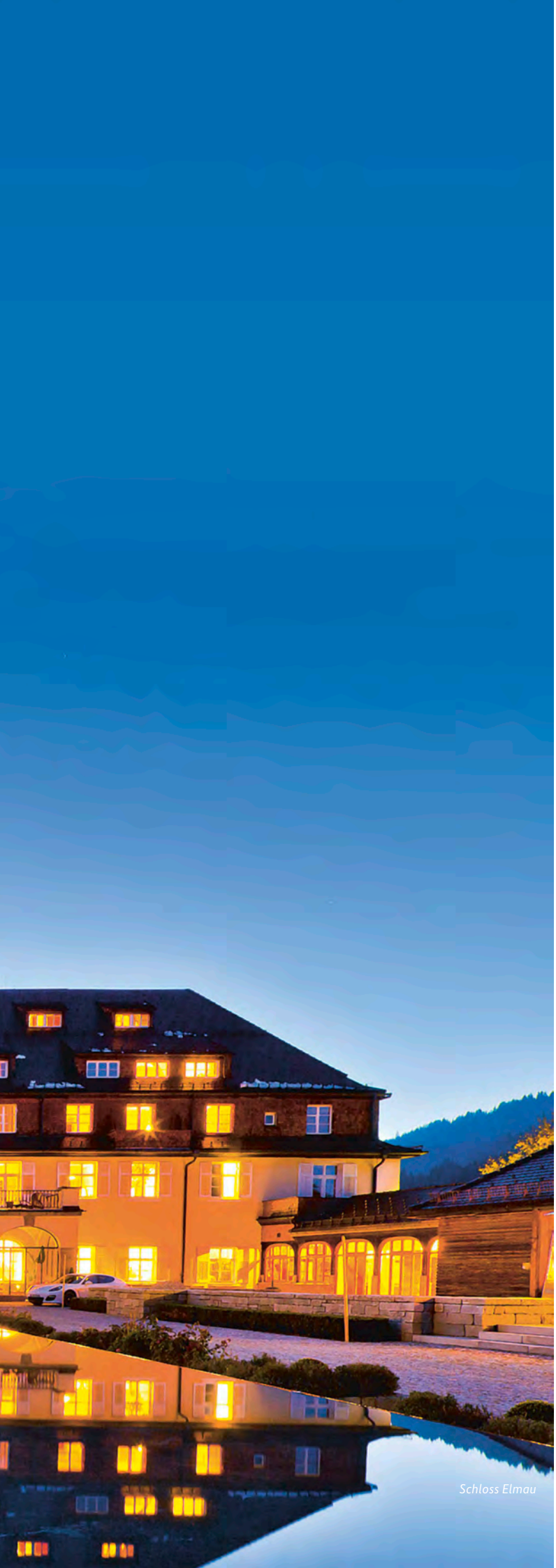
Cyber-Sicherheit für Weltrauminfrastruktur:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Weltrauminfrastrukturen/Cyber-Sicherheit_Weltrauminfrastrukturen.pdf?__blob=publicationFile&v=3

IT-Grundschutz-Profil für Weltrauminfrastruktur:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Weltrauminfrastrukturen.html

Die BSI-Lauschabwehr beim G7-Gipfel in Elmau 2022

von Dr. Astrid Schumacher, Leiterin des Fachbereichs Cyber-Sicherheit für elektronische Identitäten, und Uwe Beckert, Referatsleiter für Lauschabwehr

Im Rahmen des deutschen Vorsitzes fand im Juni dieses Jahres zum zweiten Mal das Treffen der Staats- und Regierungschefs der sieben wichtigsten Industriestaaten der Welt statt, der G7-Gipfel im bayrischen Schloss Elmau. Es gehört unbedingt zur vertrauensvollen Atmosphäre dieser Treffen, dass die Unterredungen dort vertraulich sind und Gesprächsinhalte nicht an die Öffentlichkeit oder unbefugte Dritte gelangen. Diese Vertraulichkeit der Gespräche zu gewährleisten, war in Elmau Aufgabe der Lauschabwehr des BSI.



Schloss Elmau

Die Vorbereitungen dafür begannen beim BSI bereits viele Wochen vor dem Treffen – mit Beratungen zwischen BSI und dem Auswärtigen Amt (AA), das das Gipfeltreffen formell ausrichtet. Dazu gehörten Fragen nach den notwendigen technischen und organisatorischen Maßnahmen für die Vertraulichkeit. Dabei wurde auch abgeklärt, welche Bereiche der Veranstaltung als besonders schützenswert gelten. Die Resultate dieser Konsultationen fließen als „Hierarchie der Räumlichkeiten“ in ein sogenanntes Raumbuch ein, das für alle Beteiligten anschließend als Referenz und Arbeitsgrundlage dient.

Einsatz eines Prüftools vor Ort

Einsatz des Peilfahrzeugs

Hinter den Kulissen: Dolmetscheranlagen

Einbauten im Konferenztisch

WO ANGRIFFE DROHEN

Es ist üblich, bei internationalen Veranstaltungen Dolmetscheranlagen zu installieren, um die Gespräche synchron in die Muttersprachen der Teilnehmenden zu übersetzen. Aus sicherheitstechnischer Sicht problematisch sind Anlagen, die Gesprächsinhalte über unsichtbares Infrarotlicht übertragen. Infrarotstrahlung durchdringt nahezu ungedämpft zum Beispiel Fenster. Das kann dazu führen, dass die Gespräche im Außenbereich selbst aus weiter Entfernung mit verhältnismäßig geringem Aufwand abgehört werden können. Das BSI hat sich daher dafür eingesetzt, beim G7-Gipfel ausschließlich kabelgebundene Dolmetschertechnik zu nutzen.

Eine weitere Schwachstelle können private mobile Geräte wie Smartphones, Tablets oder Smartwatches sein, die Teilnehmende in vertrauliche Besprechungen mitbringen. Wenn nicht sicher ausgeschlossen werden kann, dass eine Schadsoftware auf solchen Geräten Gesprächsinhalte aufzeichnet und an Unbefugte sendet, birgt dies ein hohes Risiko für die Vertraulichkeit der Gespräche.

Das BSI bietet den G7 dafür den Einsatz eines Mobilfunk-Detektionssystems an, mit dem unerwünscht eingebrachte Geräte nicht nur erkannt, sondern auch geortet werden können. Für die Veranstaltung selbst wurde zudem auf Empfehlung des BSI für vertrauenswürdige Besprechungen ein Mobilfunkverbot erlassen – und kontrolliert.

Erwähnt werden in diesem Zusammenhang muss auch der potenzielle Einsatz von IMSI-Catchern während der Veranstaltung. Um dieser Problematik vorzubeugen, wurden während der gesamten Veranstaltung IMSI-Catcher-Detektoren eingesetzt, die diese Bedrohung detektieren können.

BSI-LAUSCHABWEHR VOR ORT

Die Arbeit des Lauschabwehr-Teams während des G7-Gipfels bestand im Wesentlichen aus zwei Aufgaben: der Überprüfung gefährdeter Räume auf versteckte Abhöreinrichtungen und der kontinuierlichen Suche nach Anomalien im für die drahtlose Kommunikation genutzten Hochfrequenzspektrum, die auf aktive Abhörgeräte hinweisen.

Die Raumüberprüfungen wurden in Konferenzräumen sowie in den Bereichen durchgeführt, die für vertrauliche bilaterale Besprechungen vorgesehen waren. Sie begannen bereits bei der Konferenzmöblierung mit dem Verschließen von Hohlräumen, die als Versteck für Abhörtechnik geeignet sein könnten. Neben den visuellen Untersuchungen wurden die Räume inklusive der technischen Infrastruktur wie Beleuchtung und Verkabelung auch mit speziellen Lauschabwehr-Prüfgeräten inspiziert.

Zeitgleich mit der Möblierung der Räume wurden auch Hochfrequenzempfänger und Antennen installiert. Idealerweise geschieht das möglichst nahe am Konferenzgeschehen,

G7-Gipfel auf Schloss Elmau

Das Team der BSI-Lauschabwehr

um die Ortung verdächtiger Signale zu erleichtern. In Elmau wurden daher die Besprechungstische mit einem großen Hohlraum im Fuß aufgebaut, der Platz für die Technik bot. Die Steuerung der Empfänger erfolgte über ein ausreichend schnelles IP-Netzwerk, das die vorhandene Netzwerk-Infrastruktur nutzen konnte. Die Bedienung der Technik und die Auswertung der Messergebnisse konnte von einer zentralen Stelle aus durchgeführt werden, die in der Nähe der Dolmetscher-Hauptregie und der Dolmetscherkabinen lag.

Zusätzlich wurde im Außenbereich der Konferenz und ebenfalls in unmittelbarer Nähe zu den Tagungsräumen ein Messfahrzeug des BSI abgestellt. Auch dort installierte das BSI Hochfrequenzempfänger sowie ein leistungsfähiges Peilsystem. Damit war es möglich, im Vorfeld und während der Gespräche ungewöhnliche Hochfrequenzsignale, die auf einen illegalen Abhörangriff hindeuten könnten, mit den Messungen aus den Konferenzräumen zu vergleichen und eine Beurteilung vorzunehmen, ob der Ursprung der Signale im Konferenzgebäude oder außerhalb liegt.

FAZIT: ELMAU WURDE NICHT ABGEHÖRT

Der Einsatz des BSI zur Lauschabwehr, der für Dritte übrigens völlig unbemerkt ablief, ging mit dem Abschluss des G7-Gipfels zu Ende, ohne dass unsere Mitarbeitenden einen illegalen Abhörangriff feststellen konnten. Auch die Mobilfunküberwachung zeigte keine Auffälligkeiten, so dass der gesamte Gipfel ohne Zwischenfälle verlief. Die Vertraulichkeit der Gespräche konnte, auch mit Unterstützung des BSI, zu jedem Zeitpunkt gewährleistet werden. Die IMSI-Catcher-Detektion und die WLAN- und Bluetooth-Überwachung zeigten ebenfalls keine auffälligen Anzeichen von Einsätzen von IMSI-, WLAN- oder Bluetooth-Catchern.

Mit diesen Ergebnissen konnte die Lauschabwehr des BSI erneut zeigen, dass es auch bei derart sensiblen politischen Veranstaltungen möglich ist, das vertraulich gesprochene Wort vor unbefugtem Mithören zu schützen. ■

Das Cyber-Sicherheitsnetzwerk – ein Trainingsbericht

Das Cyber-Sicherheitsnetzwerk (CSN) ist ein freiwilliger Zusammenschluss von qualifizierten Helferinnen und Helfern, die ihre Expertise und ihr Know-how zur Behebung von IT-Sicherheitsvorfällen zur Verfügung zu stellen.

von Angelika Jaschob, Referat Kooperation mit IT-Herstellern und IT-Dienstleistern

Das CSN stellt einen digitalen Trainingskoffer mit einer kostenfreien Trainings- und Spielesammlung bereit. Mit diesem Material kann die Vorfallbearbeitung spielerisch trainiert werden.

Trainingseinheit Ransomware

Unterschiedliche Rollenspielkarten zum Üben

„Sowohl Unternehmen als auch Helferinnen und Helfern soll die Möglichkeit gegeben werden, in einer gesicherten Umgebung die Bewältigung von IT-Sicherheitsvorfällen zu trainieren“, kommentiert Matthias Mehrtens, Professor für Cyber Security Management an der Hochschule Niederrhein, dieses Angebot.

Doch wie läuft ein regionales Forum ab, in dem der Ernstfall trainiert wird?

IT-SICHERHEIT LÄSST SICH TRAINIEREN

„Es ist Dienstagnachmittag, 17:00 Uhr. Sechs digitale Ersthelfer, eine Jungunternehmerin und ein Vorfall-Experte des Cyber-Sicherheitsnetzwerks (CSN) treffen sich in der Hochschule Bonn/Rhein Sieg zu einem regionalen Forum – so, wie jeden ersten Dienstag im Monat. Hier diskutieren sie aktuelle IT-Sicherheitsvorfälle und neue Angriffsformen und tauschen sich über ihre Erfahrungen bei der Vorfallbehandlung aus. Heute steht ein besonderer Punkt auf der Agenda. Die Forenleiterin hat sich aus dem Trainingskoffer des CSN das Rollenspiel zu Ransomware heruntergeladen und mit Hilfe der Anleitung vorbereitet. Ziel ist es, in einer gesicherten Umgebung den Umgang mit einer digitalen Erpressung zu trainieren.

Trainingskoffer Rollenspiel

Trainingseinheit: Quer durch die Digitale Rettungskette des CSN

Normalerweise ist es üblich, zu Beginn eines Forentreffens eine „Tour de Table" zu machen, in der jede Teilnehmerin und jeder Teilnehmer aktuelle Erfahrungen oder Fragen einbringt. Aber heute freuen sich alle auf die Trainingseinheit, so dass dieser Erfahrungsaustausch eher kurz ausfällt.

Im Mittelpunkt des Nachmittags steht das (fiktive) Altenheim „Haus Weinstock" mit 30 Mitarbeiterinnen und Mitarbeitern sowie 75 Bewohnerinnen und Bewohnern. Am Wochenende hat ein Verschlüsselungstrojaner die IT-Systeme des Heims infiziert und verschlüsselt und so das Netzwerk komplett lahmgelegt. Für die Entschlüsselung der Systeme verlangen die Angreifer ein hohes Lösegeld.

Die Forenleiterin führt als Moderatorin in das Rollenspiel ein. Jeder Teilnehmende kann sich eine von acht Rollenspielkarten aussuchen, um sich anschließend in seine Rolle einzulesen. Neben der Rolle des Vorfallbearbeiters gibt es die einer nicht IT-affinen Geschäftsführerin, die eines jungen IT-Leiters, der eigentlich gerade im Urlaub ist, und die einer Mitarbeiterin des IT-Dienstleiters.

Der IT-Ausfall im Altenheim ist besonders brisant, weil die Medikation der Heimbewohnerinnen und -bewohner ohne die Daten auf den Tablets der Mitarbeitenden nicht nachvollzogen werden kann. Das führt nicht nur zu einem Versorgungsengpass mit den zum Teil lebenswichtigen Medikamenten, sondern sorgt schnell auch für Unmut bei besorgten Angehörigen. Zudem hat auch die Lokalzeitung schnell Wind von dem Vorfall bekommen und steht mit einer zu Recht neugierigen Journalistin vor der Tür. Schließlich wurde auch die Polizei eingeschaltet, die versucht, den Tathergang nachzuvollziehen.

Die folgenden Stunden vergehen damit, dass alle ihre Rolle spielen und dabei merken, an welche Grenzen sie stoßen. Da wird hektisch diskutiert, aber auch über die nächsten Schritte gefachsimpelt. Gut, dass es einen Vorfall-Experten gibt, der die Lage emotionslos analysieren kann, weil er die richtigen Fragen stellt und so das Krisenmanagement übernehmen kann.

Im Trainingszentrum der Hochschule Bonn/Rhein Sieg konnte so der IT-Sicherheitsvorfall schon nach 60 Minuten gelöst werden: Aus einem alten Backup konnte das Altenheim ein Ersatzsystem erstellen. Und aufgrund des professionellen Krisenmanagements konnte die Gesamtsituation schnell deeskaliert werden.

Nach dem Rollenspiel findet ein Debriefing statt, in dem die Forenleiterin ihre Sicht als neutrale Beobachterin schildert und das Vorgehen zusammenfasst. Zusätzlich stellt sie noch Empfehlungen des BSI zum Thema Ransomware vor. Anschließend diskutiert die Runde noch eine Weile, wie sie sich in ihren Rollen gefühlt haben. Am Ende sind sich alle einig, im Rahmen der Foren weitere Trainingseinheiten durchspielen zu wollen. „Ich wüsste nicht, wie ich in einer solchen Situation reagiert hätte", sagt einer der Teilnehmenden. „Aber ich weiß, dass ich nach der Trainingseinheit zuversichtlicher in die Zukunft sehe, da mich so ein Ransomware-Vorfall und dessen Folgen nicht mehr so unvorbereitet treffen wird."

VOM TRAINING ZUR WIRKLICHKEIT

Dass solche Szenarien nicht nur Theorie sind, zeigt ein IT-Sicherheitsvorfall aus dem Juni dieses Jahres, bei dem ein Vorfall-Experte des CSN ein mittelständisches Energieunternehmen unterstützt hat, das mit Ransomware angegriffen und teilweise lahmgelegt wurde. Dank eines Notfallplans ging es am Ende aber glimpflich aus.

Das CSN hat für Angriffe eine digitale Rettungskette entwickelt, in der festgelegt ist, wer an welcher Stelle des Prozesses welche Aufgabe übernimmt. Die Rettungskette reicht von der Unterstützung durch Checklisten über telefonischen Support durch das CSN bis hin zu einem Team von Vorfall-Experten, die vor Ort tätig werden können. So bringt das CSN qualifizierte Helferinnen und Helfer zusammen, die bei einem Vorfall koordiniert agieren können.

WIE GUT IST IHR UNTERNEHMEN AUF EINEN IT-SICHERHEITSVORFALL VORBEREITET?

Wenn Sie wissen möchten, wie gut Ihr Unternehmen auf einen IT-Sicherheitsvorfall vorbereitet ist, können Sie das mit dem Selbsteinschätzungstest des CSN herausfinden. Über den rund fünfminütigen Test können kleine und mittlere Unternehmen, aber auch Privatpersonen ihre Reaktionsfähigkeit auf IT-Sicherheitsvorfälle überprüfen. Der Test umfasst fünf Fragen zur IT-Infrastruktur und IT-Prozessen. Dazu kommen Fragen zu Zuständigkeiten von Mitarbeiterinnen und Mitarbeitern und dem Umgang mit Passwörtern im Unternehmen. Zusätzlich verweist der Test auf Dokumente und detaillierte Hinweise, die als Hilfestellung zur Verbesserung der eigenen Cyber-Resilienz verwendet werden können. ■

Nehmen Sie das kostenlose Angebot wahr und werden Sie Teilnehmer oder Teilnehmerin des Cyber-Sicherheitsnetzwerks.

Weitere Informationen:

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

E-Mail: info@cyber-sicherheitsnetzwerk.de

Im Blickpunkt

Digitale Erpressung mit Ransomware

Digitale Erpressung mit Ransomware

Angriffe mit einem hohen Schaden

von Korbinian Barthuber, Referat Vorfallsbearbeitung und Verbindungsstelle Nationales Cyber-Abwehrzentrum

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme vor allem über Datenverschlüsselungen einschränken oder verhindern. Eine Freigabe der Ressourcen erfolgt nur gegen Zahlung eines Lösegeldes (engl. „ransom“). Angriffe mit Ransomware stellen laut dem aktuellen BSI-Bericht „Die Lage der IT-Sicherheit in Deutschland 2022“ eine der größten Cyber-Bedrohungen für Staat, Wirtschaft und Gesellschaft dar.

Bei einem Ransomware-Angriff handelt es sich um eine Attacke auf das Sicherheitsziel der Verfügbarkeit und eine Form der digitalen Erpressung. Die Angreifenden nutzen Fehler wie falsche Bedienung, Fehlkonfigurationen, veraltete Software-Stände oder mangelhafte Datensicherungen aus. Die Zahlung des Lösegelds wird meist in elektronischen Währungen (üblicherweise Bitcoin oder Monero) gefordert.

Die Effektivität von Ransomware beruht auf ihrer unmittelbaren Wirkung. Im Unterschied zu klassischer Schadsoftware wie Banking-Trojanern, Botnetzen oder Phishing-Mails tritt der Schaden unmittelbar ein und hat konkrete Konsequenzen für die Betroffenen. Hier ersetzt kein Kreditinstitut den Schaden (Banking-Trojaner) und der PC funktioniert nicht nur etwas langsamer (Botnetz), sondern oft gar nicht mehr. Bei einem Ransomware-Angriff können zum Beispiel auch alle gespeicherten Dokumente verlorengehen, wichtige Unternehmensdaten sind nicht mehr zugreifbar oder kritische Dienstleistungen nicht mehr verfügbar.

Gegen solche Angriffe helfen am besten präventive Maßnahmen, speziell sogenannte Offline-Backups, die getrennt von den IT-Systemen und besonders geschützt aufbewahrt werden.

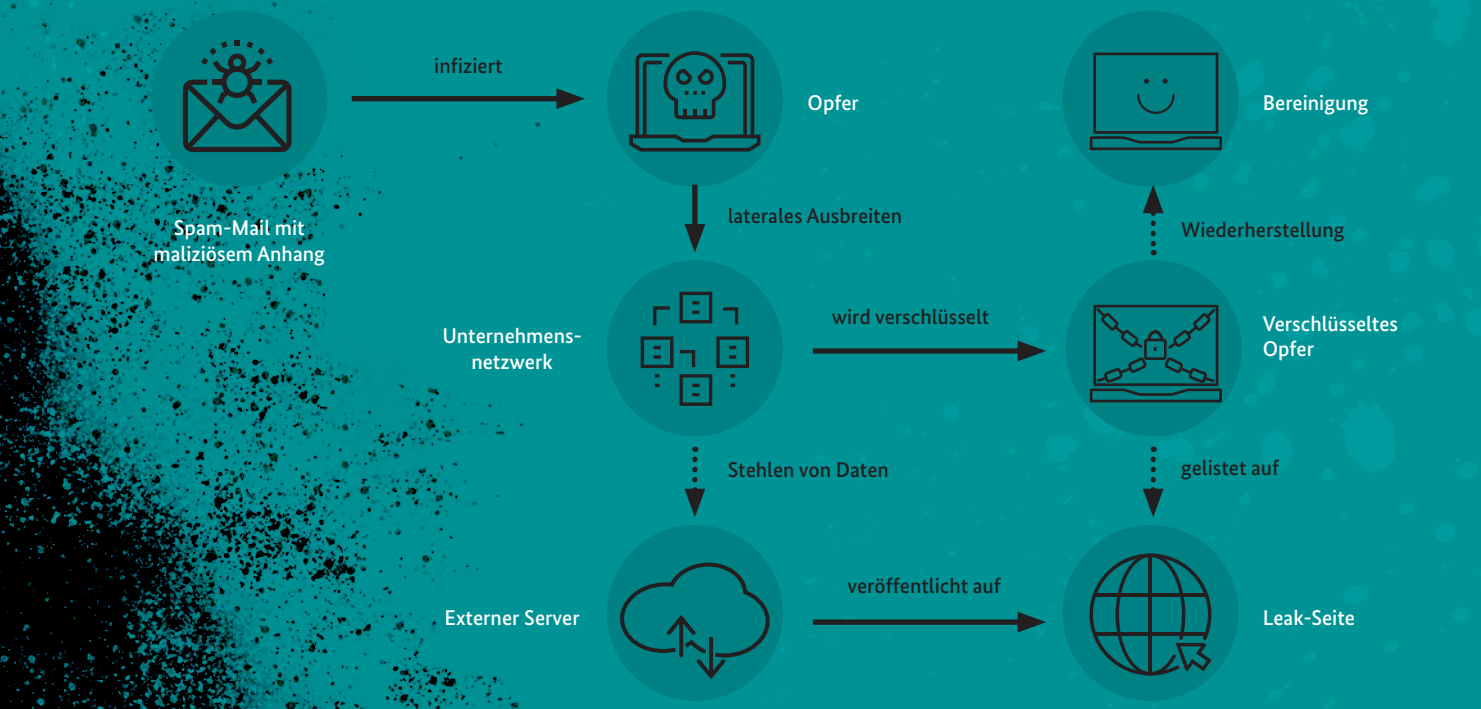
LÖSEGELD ODER DATENWIEDERHERSTELLUNG?

Weil der Leidensdruck der Betroffenen nach einem Ransomware-Angriff enorm hoch ist, zahlen viele Opfer das geforderte Lösegeld in der Hoffnung, schnell wieder arbeitsfähig zu sein. Abgesehen davon, dass es keine Garantie für eine Freigabe der Daten gibt, kann es je nach Qualität des Entschlüsselungstools des Erpressers aber auch möglich sein, dass die Wiederherstellung eines Systems über speziell gesicherte Backups schneller gehen würde.

Neben der Verschlüsselung von Daten drohen Cyber-Kriminelle neuerdings häufig auch damit, die entwendeten Daten zu veröffentlichen, um die Opfer zusätzlich unter Druck zu setzen. Potenzielle Opfer sind dabei Institutionen aller möglichen Größen – vom Kleinstunternehmen über Behörden und KRITIS-Unternehmen bis hin zu großen internationalen Konzernen.

Nicht jeder Ransomware-Angriff ist vorhersehbar, denn neue Ransomware kann auch neue, nicht ohne Weiteres abwehrbare Angriffswege nutzen. Für den Regelfall gilt aber, dass erfolgreiche Angriffe auf Unternehmen, Behörden und IT-Dienstleister oft durchaus verhindert werden können. Auch die Auswirkungen lassen sich mit Präventivmaßnahmen besser in den Griff bekommen.

Vereinfachte Darstellung eines Ransomware-Angriffs



TYPISCHER ABLAUF EINES RANSOMWARE-ANGRIFFS

Das häufigste Angriffsziel ist der Mensch. Ein Haupteinfallspunkt für Angriffe ist bei Client-Systemen in der Regel eine E-Mail mit schadhaftem Anhang. In Unternehmensnetzen öffnen auch verwundbare oder schlecht gesicherte und extern erreichbare Server Angreifenden die Tür.

Bei maliziösen Anhängen handelt es sich häufig um Office-Dateien mit VBA-Makros, .iso- und .lnk-Dateien oder (verschlüsselte) Zip-Dateien mit direkt mitgeliefertem Passwort. Bei Servern werden häufig Schwachstellen ausgenutzt. In der Vergangenheit waren das zum Beispiel CVE-2019-19781 („Shitrix“) für Citrix-ADC und -Gateway oder CVE-2021-34472 („ProxyShell“) für Microsoft Exchange.

Daneben können auch schlecht gesicherte Zugänge ohne zweiten Authentifizierungsfaktor eine Gefahr darstellen. Insbesondere bei Servern beginnt der eigentliche Angriff oft erst Monate nach der Infektion. Solche initialen Zugänge werden oft als Access-as-a-Service gehandelt und an andere Angreifergruppen verkauft.

Nach dem Öffnen der Tür laden Angreifende in der Regel Schadsoftware nach, um die erlangten Rechte zu erweitern sowie (teil-)automatisiert das Netzwerk des Betroffenen – bis hinein in die zentralen Komponenten der Rechteverwaltung (Active Directory) – komplett zu übernehmen. Passiert so etwas, ist das Unternehmensnetz vollständig kompromittiert und nicht mehr vertrauenswürdig.

Die Angreifenden besitzen dann alle Rechte, um beispielsweise Benutzerkonten mit Administrator-Rechten anzulegen, Daten einzusehen oder Hintertüren einzurichten. In diesem Status werden dann auch Daten entwendet („Datenexfiltration“), um mit deren Veröffentlichung zu drohen, falls ein Opfer nicht zu einer Lösegeldzahlung bereit ist (eine sogenannte doppelte Erpressung oder „Double-Extortion“).

Letztendlich werden Daten auf möglichst vielen Systemen verschlüsselt, insbesondere auf Backup-Systemen, in der Regel, ohne das Betriebssystem selbst zu beeinträchtigen. Stattdessen hinterlassen die Angreifenden Nachrichten mit Hinweisen, wie die Opfer Kontakt für Verhandlungen aufnehmen können.

Die Betroffenen selbst stehen vor der Herausforderung, ihre Systeme und Daten wiederherzustellen. Je nach Ausmaß der Betroffenheit muss dafür ein Übergangsbetrieb organisiert und der Vorfall an die Stakeholder, also an Eigentümer, Kunden und Partner, kommuniziert werden. ■

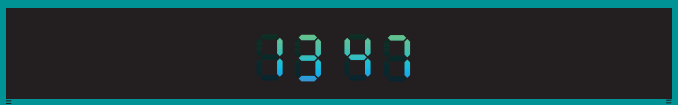
Ein Tag bei CERT-Bund

– und was passiert, wenn ein Ransomware-Vorfall gemeldet wird

von Veselina Hensel, Referat Mobile Incident Response Team, und Letitia Kernschmidt, Referat Vorfallsbearbeitung und Verbindungsstelle Nationales Cyber-Abwehrzentrum

Rund um die Uhr gehen Meldungen im Nationalen IT-Lagezentrum ein, die dort zentral aufgenommen, bewertet und je nach Kritikalität durch das „Computer Emergency Response Team“ (CERT-Bund) eskaliert werden. Betroffene können innerhalb des gesetzlichen Rahmens z. B. durch telefonische Beratung, die Übermittlung von Hilfsdokumenten oder die Durchführung von technischen Analysen bis hin zu einem Vor-Ort-Einsatz unterstützt werden.

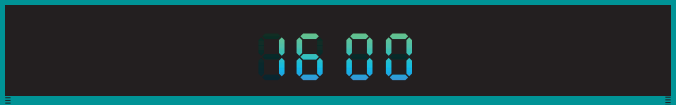
Ein Donnerstag im Jahr 2022, ...



Im Nationalen IT-Lagezentrum geht die Meldung einer Behörde ein, die angibt, von einem Ransomware-Vorfall betroffen zu sein, und um Unterstützung bittet.
Die Meldung wird gemäß dem Prozess an CERT-Bund ausgesteuert.

Der Duty Officer von CERT-Bund führt zunächst ein Telefonat mit dem Betroffenen, bei dem schnell klar wird, dass der Vorfall schwerwiegend ist. Da es sich bei dem Betroffenen um eine Stelle des Bundes handelt, kann das BSI im Rahmen seines gesetzlichen Auftrags weitreichende Unterstützungsleistungen anbieten. Eine Incident-Managerin übernimmt ab jetzt die weitere Fallbearbeitung.

In einer Videokonferenz berichtet der Betroffene, dass die Lage vor Ort angespannt und das Ausmaß der Betroffenheit unklar sei. Benötigte Steuerungstechnik sei komplett ausgefallen, so dass der Betrieb nur noch mit sehr hohem Aufwand kurzzeitig aufrechterhalten werden könne. Alle weiteren zentralen Dienste wurden sicherheitshalber heruntergefahren. Eine Strafanzeige wurde ebenfalls bereits gestellt.



Basierend auf den Schilderungen bietet das BSI der Behörde an, noch heute vor Ort zu unterstützen.
Der Betroffene nimmt das Angebot an. Da auch die Steuerungstechnik betroffen ist, wird das Team mit der Expertise für Industriesteuerungssysteme (ICS) mit herangezogen.
Bis zur Abfahrt werden noch organisatorische Tätigkeiten durchgeführt, wie das Überprüfen und Verladen des nötigen Equipments.

18:15

Alle Team-Mitglieder sind auf dem Weg zum Betroffenen, dem es zwischenzeitlich gelungen ist, Samples der eingesetzten Malware zu isolieren und an das BSI zu übermitteln. Diese werden noch von unterwegs an einen Kollegen aus dem Malware-Analyse-Team weitergeleitet.

20:30

Nach Eintreffen des BSI-Teams versammeln sich alle Beteiligten zu einem ersten Gespräch. Dabei ist es sehr wichtig, ein gemeinsames Verständnis zu schaffen, die Ziele des Unterstützungsauftrags zu definieren und offene Fragen zu klären. Darauf basierend wird das weitere Vorgehen geplant, Zuständigkeiten festgelegt und Aufgaben verteilt. Es gilt Struktur in einer außerordentlichen Situation zu schaffen, auf die der Betroffene meist nicht ausreichend vorbereitet ist.

Parallel dazu werden alle relevanten Systeme und Daten (z. B. Protokolldaten) forensisch gesichert. Da die virtuellen Maschinen für die Steuerungstechnik zum Großteil verschlüsselt sind, wird nach einer fachlichen Diskussion entschieden, dass das BSI die zwei Hosts für weitere Analysen mitnehmen darf. Zudem liegen eine erste Analyse der Malware sowie Regeln zur Detektion vor, die dem Betroffenen übergeben werden.

22:30

Die Incident-Managerin finalisiert noch den End-of-Day-Report und verschickt diesen an einen vordefinierten Verteiler. Dann ist vor Ort erstmal Feierabend!
Im Nationalen IT-Lagezentrum werden die Erkenntnisse des Vor-Ort-Teams über Nacht weiter verarbeitet und für die Übernahme in die Lageprodukte des BSI aufbereitet.

Am nächsten Tag

07:30

Im BSI werden die ersten Erkenntnisse aus dem Vorfall für eine Warnmeldung anonymisiert aufbereitet und später via E-Mail, der BSI-Webseite und dem CERT-Bund Twitter-Kanal veröffentlicht. Vor Ort laufen die Analyse- und Unterstützungsleistungen wieder an.

11:20

Der Vorfall wurde nun auch von den Medien aufgegriffen, so dass die Pressestelle erste Anfragen bearbeiten muss. Auch Anfragen von nationalen und internationalen Partnern sowie der Behörden im nationalen Cyber-Abwehrzentrum müssen koordiniert und beantwortet werden.
Im Rahmen der täglichen Lagebesprechung wird der Vorfall BSI-intern vorgestellt und diskutiert.

13:10

Das BSI-eigene Threat-Intelligence-Team reichert die Erkenntnisse mit weiteren Informationen an und teilt sie anonymisiert über das Malware Information Sharing Portal (MISP) mit den Zielgruppen des BSI. Auch das Bundes Security Operations Center (BSOC) im BSI verwendet diese Informationen, um so mögliche Angriffe auf die Netze des Bundes zu detektieren.
Der Vorfall wird anonymisiert mitsamt den weiteren Erkenntnissen des BSI in den Tageslagebericht des BSI aufgenommen und an die Zielgruppen des BSI verteilt.

16:00

Die ersten Analyseergebnisse und entwickelten Maßnahmen werden diskutiert. Darauf aufbauend muss die betroffene Behörde in den nächsten Tagen und Wochen die Bereinigung und den Wiederanlauf des Betriebs planen und umsetzen.

... und wie geht es dann weiter?
Die weitere Unterstützung kann sich je nach Fall auch über mehrere Wochen oder sogar Monate erstrecken. Es gibt hierzu kein einheitliches Vorgehen, da jeder Vorfall anders ist und somit eine andere, eventuell neue und zum Teil auch kreative Herangehensweise erfordert. Das Leben ist Veränderung, heißt es, und so unterliegt auch der Job im CERT-Bund einem ständigen Wandel. Doch genau das macht ihn so abwechslungsreich und interessant.

Schutz ist in jeder Phase möglich

Von Backup bis Notfallplan: Abwehrmaßnahmen identifizieren und umsetzen

von Maximilian Winkler, Mobile Incident Response Team (MIRT)

Ein Ransomware-Angriff besteht aus mehreren Schritten. Für jede Phase eines solchen Angriffs sind Gegenmaßnahmen möglich, um das Eindringen in Netzwerke oder das Verschlüsseln von Daten zu verhindern und möglichen Schaden zu begrenzen. Einige dieser Maßnahmen stellen wir im Folgenden vor.

Die Verschlüsselung von Daten über Ransomware und Erpressungen für ihre Freischaltung gehören zu den größten Bedrohungen für die Funktionsfähigkeit von IT-Infrastrukturen. Dies zeigt sich insbesondere dann, wenn durch die Verschlüsselung von IT-Systemen das wirtschaftliche Überleben von Unternehmen gefährdet oder der öffentlichen Verwaltung die Ausführung hoheitlicher Aufgaben und kritischer Dienstleistungen nicht mehr möglich ist.

Bei der Verschlüsselung handelt es sich tatsächlich aber nur um den letzten Schritt, den Angreifer ausführen, wenn sie zuvor bereits viel Zeit in einem kompromittierten Netzwerk verbracht haben. Für jede Phase eines Ransomware-Angriffs gibt es Maßnahmen, die erfolgreich Angriffe verhindern oder zumindest ihre Auswirkungen begrenzen können.

Angriffsphase 1 – Einbruch

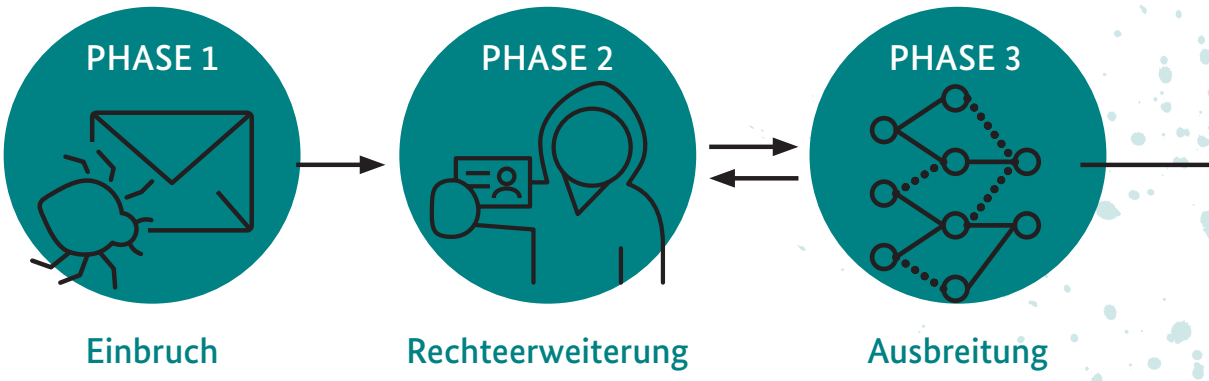
Die drei häufigsten Einfallsvektoren von Ransomware-Gruppen sind Phishing, die Ausnutzung von Schwachstellen sowie der Zugriff über schlecht abgesicherte externe Zugänge. Für jedes dieser Einfallstore existieren wirksame Maßnahmen.

Gegenmaßnahme Phishing: E-Mails und Sensibilisierung

Das BSI empfiehlt E-Mails, die als „Nur-Text“ oder „reiner Text“ codiert sind. Im Gegensatz zur Darstellung als „HTML-Mail“ können sie keine Makros oder versteckte Befehle enthalten. Zudem lassen sich hier Webadressen nicht mehr verschleiern. In einer HTML-codierten Mail könnte zum Beispiel ein Link mit der Bezeichnung „www.bsi.de“ in Wahrheit auf eine schadhafte Webseite verweisen. Ist eine Nur-Text-Codierung nicht möglich oder nicht erwünscht, sollte zumindest die Ausführung aktiver Inhalte in HTML-Mails unterdrückt werden, damit schadhafte Skripte nicht mehr ausgeführt werden können.

Mitarbeitende sollten im Rahmen von Sensibilisierungsmaßnahmen praxisnah über die Risiken im Umgang mit Mails geschult werden. Das gilt besonders für Mitarbeitende aus Unternehmensbereichen, die ein hohes Aufkommen an externer Mailkommunikation (etwa in der Personalabteilung oder im Marketing) zu bewältigen haben.

Vereinfachte Darstellung eines Ransomware-Angriffs



Gegenmaßnahme Schwachstellen: Patches und Updates

Um Infektionen zu vermeiden, die auf der Ausnutzung bereits behobener Sicherheitslücken beruhen, sollten Updates nach der Bereitstellung durch den Software-Anbieter unverzüglich in die IT-Systeme eingespielt werden – über die zentrale Softwareverteilung idealerweise auch in alle Desktop-Computer und Notebooks. Updates, die Schwachstellen von hoher Kritikalität schließen und/oder sich auf besonders exponierte Software wie Firewalls oder Webserver beziehen, sollten priorisiert behandelt werden.

Gegenmaßnahme Remote-Zugang: Mehr Faktor-Authentifizierung

Häufig versuchen Cyber-Kriminelle, Ransomware über kompromittierte Remote-Zugänge auf Systemen zu installieren. Daher sollte auch der Zugriff von außen abgesichert werden – normalerweise über VPNs in Kombination mit einer Mehr-Faktor-Authentifizierung.

Angriffsphase 2 – Rechteerweiterung Gegenmaßnahme: Administrator-Accounts absichern

Grundsätzlich sollten mit privilegierten Accounts nur Administratorentätigkeiten durchgeführt werden. Das Lesen von E-Mails oder das Surfen im Internet gehören nicht dazu. Administratorinnen und Administratoren sollten sich für solche „normalen Tätigkeiten" auch „normale" Nutzerkonten anlegen. Das lässt sich übrigens über technische Richtlinien auch erzwingen. Privilegierte Konten sollten immer über eine Mehr-Faktor-Authentifizierung geschützt sein. Zudem sollten für die Administration von Clients keine Domänen-Administrationskonten verwendet werden.

Angriffsphase 3 – Ausbreitung Gegenmaßnahme: Netzwerk segmentieren

Eine saubere Netzsegmentierung hilft, Schäden zu begrenzen, da das Einschleusen einer Ransomware nur die Systeme in unmittelbarer Nachbarschaft erreichen kann. Auch dafür ist die sichere Verwendung von Administrator-Accounts notwendig (siehe vorhergehende Maßnahme), weil ansonsten ein zentraler Bestandteil des Sicherheitskonzepts untergraben wird.

Angriffsphase 4 und 5 – Verschlüsselung mit/ohne vorherigen Datenabfluss Gegenmaßnahme: Backups und Datensicherung

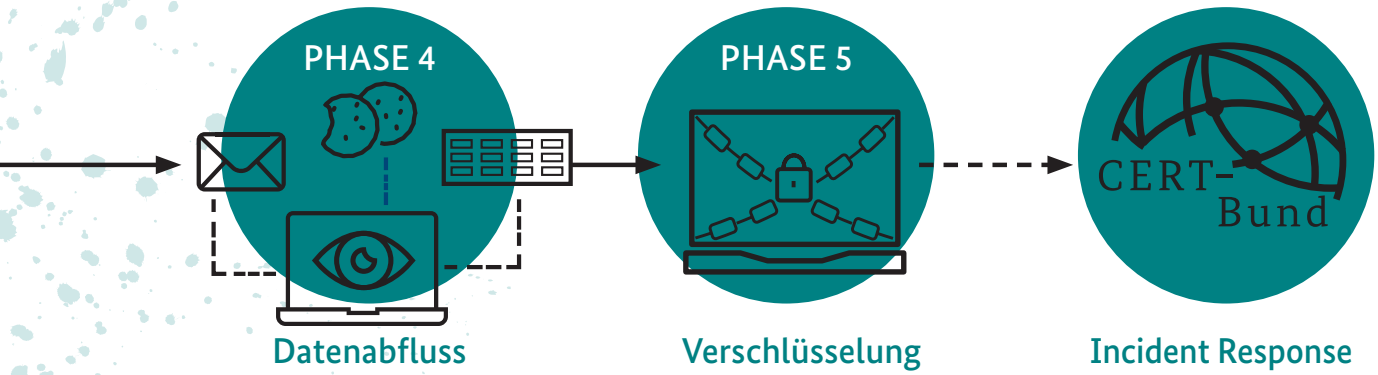
Backups sind der beste Schutz vor den Auswirkungen bei einer Verschlüsselung durch Ransomware, denn sie gewährleisten die unmittelbare Verfügbarkeit von Daten auch für diesen Fall. Dafür müssen die Daten aber in einem Offline-Backup gesichert werden, die zudem nach einem Backup von den übrigen Systemen des Netzwerkes getrennt werden. Erst dann sind sie vor Angriffen und Verschlüsselung geschützt. Zu einem Backup gehört auch immer die Planung und Vorbereitung des Wiederanlaufs und der Wiederherstellung der Daten. Dies sollte regelmäßig getestet werden, um Komplikationen und Herausforderungen bei der Wiederherstellung bereits vor einem Ernstfall zu erkennen.

Maßnahme: Notfallplan

Für das Worst-Case-Szenario eines erfolgreichen Angriffs, bei dem alle Systeme im Netzwerk verschlüsselt wurden, sollte eine Notfallplanung für Notbetrieb und Wiederaufbau existieren. Die Prozesse zur Reaktion und Wiederherstellung geschäftskritischer Systeme sollten in regelmäßigen Abständen geübt werden. Insbesondere müssen vorab die geschäftskritischen Systeme identifiziert werden und alternative Kommunikationsmöglichkeiten außerhalb des kompromittierten Netzwerks vorbereitet sein. Wichtige Telefonnummern von Kontaktpersonen sollten offline in Papierform vorgehalten werden.

Weitere Informationen:

Ransomware-Informationsportal des BSI: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html



Was Cybercrime und Wirtschaft gemeinsam haben

Arbeitsteilung, Outsourcing und Profit

von Alexander Härtel, Referat Nationales IT-Lagezentrum, Analysen und Prognosen

Ein genauer Blick auf die Praxis von Cyber-Kriminellen, die mit finanziellen Motiven Unternehmen mit Ransomware erpressen, ergibt überraschende Parallelen zur realen Wirtschaft.

In der IT, aber auch in traditionellen Wirtschaftszweigen werden verschiedene Dienstleistungen ausgelagert. In der IT ist das zum Beispiel ein „Software-as-a-Service", aber auch der Betrieb von Infrastruktur oder die Verarbeitung von Daten kann ausgelagert werden.

Solche ausgelagerten Dienstleistungen haben auch Cyber-Kriminelle immer häufiger im Angebot. So spezialisieren sich manche, etwa die Drahtzieher hinter Emotet oder QakBot, als Access Broker gezielt auf das Eindringen in IT-Netze. Andere „Dienstleister" verkaufen die dort gewonnenen Erkenntnisse und Zugangsdaten weiter. Und wieder andere wie die Gruppen hinter LockBit 3.0 oder Alphv bieten eine Art von „Ransomware-as-a-Service" (RaaS) an, mit denen dann sogenannte Affiliates aktiv werden, ohne selbst dafür Schadsoftware entwickeln zu müssen.

Solche und weitere Dienstleistungen decken mittlerweile nahezu jeden Aspekt eines Cyber-Angriffs ab und folgen den wirtschaftlichen Trends zum Outsourcing von Aufgaben – anders als in der realen Wirtschaft allerdings natürlich ohne gesetzliche Grundlagen und Aufsicht. Stattdessen vermitteln etablierte Untergrundforen wie XSS und Exploit Kontakte zu anderen Cyber-Kriminellen. Sie bieten ihnen Platz, damit sie für ihre Dienstleistungen werben können oder ermöglichen ihnen das Hinterlegen von Garantien in Form von Kryptowährungen. Im Konfliktfall vermitteln Moderatoren und treffen verbindliche Entscheidungen für die Community und sind damit einem Schiedsgericht nicht unähnlich. Die hinterlegten Garantien werden dann mitunter für Entschädigungen herangezogen. Auf dieser Basis können Cyber-Kriminelle selbst bei gegenseitigem Misstrauen zusammenarbeiten.

ALLES FÜR DEN MAXIMALEN PROFIT

Das Ziel der Gewinnmaximierung fördert auch in der Welt des Cybercrime Innovation, Effizienz und Expansion. Ein eindrückliches Beispiel dafür ist, dass Cyber-Kriminelle Daten, auf die sie widerrechtlich Zugriff erlangen, nicht nur verschlüsseln, sondern zusätzlich noch auf dedizierten Leak-Seiten veröffentlichen und damit eine sogenannte doppelte Erpressung („Double Extortion") durchführen. Erstmals intensiv beobachtet wurde dieses Verhalten bei den Angreiferinnen und Angreifern hinter der Ransomware Maze im November 2019. Mit Ende des Jahres 2021 ist Double Extortion zur Norm bei Ransomware-Angriffen geworden.

Ein anderes Beispiel ist die Modularisierung von Schadsoftware. Damit können Angreiferinnen und Angreifer effizient neue Schwachstellen in Anwendungen oder Systemen ausnutzen, verbesserte Detektionsmöglichkeiten in der Abwehr solcher Angriffe umgehen oder auf individuelle Bedürfnisse ihrer kriminellen Nutzerinnen und Nutzer („Affiliates") reagieren. Emotet und QakBot etwa wurden zunächst als Banking-Trojaner eingesetzt und später um Module zur Aufklärung infizierter Systeme, zum Diebstahl von E-Mail-Inhalten oder zum automatischen Verschicken der Malware an andere Opfer ergänzt. Durch Modularisierung können Teile einer Software ergänzt oder überarbeitet werden, ohne die gesamte Code-Basis ändern zu müssen.

RANSOMWARE-AS-A-SERVICE ALS MÖGLICHMACHER

Eine Malware wie eine Ransomware zu entwickeln, die mit modernen Abwehrmaßnahmen und Analysewerkzeugen mithält, erfordert einiges an Fachwissen in der Softwareentwicklung. Dieses Fachwissen bringen nicht alle Cyber-Kriminellen mit. An dieser Stelle setzt Ransomware-as-a-Service an. Mit Ransomware als Dienstleistung sinken die Anforderungen an einen Angreifer deutlich, weil durch diesen Service mittlerweile auch technisch unbedarfte Personen Ransomware-Angriffe durchführen können. Diese Expansion auf viele Angreifende bietet zudem den Vorteil, dass es für Betroffene schwerer wird, die Vorgehensweisen einzelner Affiliates zu unterscheiden oder zu detektieren.

DER EIGENE RUF ALS KRITISCHE RESSOURCE

Cyber-kriminelle Gruppen konkurrieren durchaus um ihre Affiliates, daher spielt in der Szene auch die Reputation der eigenen Marke eine wichtige Rolle. Diese Art des Wetteiferns führt zu einer zunehmenden Verschärfung der Bedrohungslage. Ein entscheidendes Argument für einen Affiliate ist beispielsweise, wie viel Druck auf einen Betroffenen ausgeübt werden kann. Daher bieten einige RaaS-Anbieter wie Alphv (auch als „BlackCat“ bekannt) DDoS-Angriffe als zusätzliche Dienstleistung an, die während der Verhandlung eines Lösegelds eingesetzt werden kann. So führt der Konkurrenzkampf zwischen cyber-kriminellen Gruppen zu einer Maximierung des Drucks auf Betroffene.

Andere Unterscheidungsmerkmale zwischen Ransomware-as-a-Service-Angeboten sind auch der Anteil am Lösegeld, der beim Affiliate verbleibt, oder die fortlaufende Verbesserung der Ransomware selbst. Eine andere Ransomware-as-a-Service, die auf solche „Premium-Services“ setzt, ist beispielsweise LockBit. Diese stellt u. a. die Malware StealBit zur Verfügung, die auf den Diebstahl von Daten für die Erpressung spezialisiert ist.

Und sogar der „War for Talents“, den sich die legale Ökonomie um die jeweils besten Köpfe liefert, findet auch im cyber-kriminellen Raum statt. Deshalb spielt dort auch der gute Ruf in den eigenen Kreisen eine wichtige Rolle. Einige Foren nehmen beispielsweise nur bereits bekannte oder erfolgreiche Cyber-Kriminelle auf – und bleiben so weitestgehend unter sich.

EINE FRAGE DER EHRE

Vertrauen, so seltsam das klingt, ist auch unter Cyber-Kriminellen eine Währung. Spricht sich zum Beispiel nach einem Ransomware-Angriff herum, dass ein Entschlüsselungstool nach einer Lösegeldzahlung nicht oder nicht „ordnungsgemäß“ funktioniert, führt dies in der Folge wahrscheinlich eher zu ausbleibenden Zahlungseingängen. Als Druckmittel bleibt dann nur noch die Drohung mit der Veröffentlichung der Daten, aber auch das geht nur selten als vertrauensbildende Maßnahme durch. So ist auch für Cyber-Kriminelle wichtig, bei ihren Opfern wenigstens ein Mindestmaß an gutem Benehmen zeigen zu können – hier vor allem in Form gehaltener Versprechen, Daten wieder freizuschalten und nicht zu veröffentlichen.

Das BSI weist darauf hin, dass eine Lösegeldzahlung keine Garantie für die Freigabe gesperrter Daten ist. Zudem tragen Lösegeldzahlungen dazu bei, dass sich kriminelle Ökosysteme und Organisationen professionalisieren und wachsen. Daher bleibt es bei der BSI-Empfehlung, auf Lösegeldzahlungen unbedingt zu verzichten. Wichtiger ist es, wirksame Vorkehrungen gegen Ransomware-Angriffe zu treffen.

„TOO BIG TO FAIL“ VS. „TOO BIG TO STAY AFLOAT“

Unternehmen und Institutionen, die zu groß oder zu wichtig sind, um zu scheitern, werden als „too big to fail“ bezeichnet. Dazu gehörten zum Beispiel in der weltweiten Finanzkrise 2008 zahlreiche Banken, die nur mit staatlichen Hilfen vor der Insolvenz gerettet werden konnten. „Too big to fail“ – gibt es das auch bei Cyber-Kriminellen?

Kurz gesagt: Nein. Hier ist Größe kein Rettungsgrund, sondern eher eine Ursache für das Ende. Ist eine Gruppe von Cyber-Kriminellen erfolgreich, steigt ihre öffentliche Bekanntheit und damit auch die Aufmerksamkeit, die sie bei Sicherheitsfachleuten und Strafverfolgungsbehörden genießt. Daher war es bisher nur eine Frage der Zeit, bis solche Gruppen unschädlich gemacht werden konnten oder sich gezwungen sahen unterzutauchen:

- Emotet wurde im Januar 2021 abgeschaltet
- RaaS DarkSide löste sich nach dem Cyber-Angriff gegen Colonial Pipeline auf
- RaaS REvil verschwand nach dem Cyber-Angriff über Kaseya VSA
- Das „Conti-Syndikat“ zersplitterte im Mai 2022

Während in der Wirtschaft Unternehmen durchaus den Status „too big to fail“ erreichen, werden cyber-kriminelle Gruppen also eher „too big to stay afloat“, also zu groß, um den Kopf über Wasser zu halten. Allerdings werden auch in Zukunft andere ihre Plätze einnehmen – getrieben von der Gier nach schnellen Profiten. ■

it-sa 2022 in Nürnberg

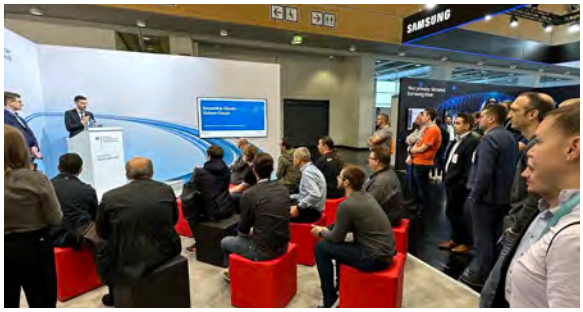
Cyber-Sicherheit endlich wieder live: Rückblick auf drei erfolgreiche Messetage

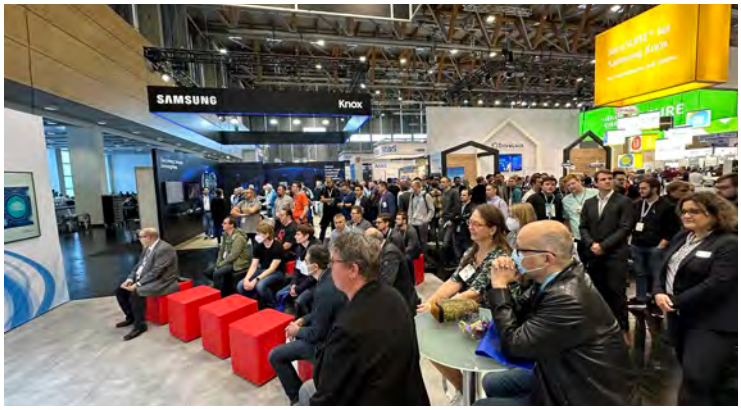
Vom 25.-27. Oktober 2022 fand die it-sa Expo & Congress, Europas größte Fachmesse zum Thema IT-Security, in Nürnberg statt. Als ein ideeller Träger der Messe war das BSI mit einem Stand, an dem sich Interessierte zu Fachthemen erkundigen und mit BSI-Expertinnen und -Experten austauschen konnten, vor Ort.

Viele Themen – rege Nachfrage

Diesjährige Fokusthemen des BSI am Messestand waren unter anderem die Angebote der Allianz für Cyber-Sicherheit, Lösungen zum Digitalen Verbraucherschutz, Zertifizierung sowie Mediale Identitäten und stießen auf großes Interesse bei den Messe-Besucherinnen und -Besuchern.

Zertifikatsübergabe für die Tachographkarte auf der it-sa: Dr. Hans Hanauer, Geschäftsführer der Firma MaskTech International GmbH und Sandro Amendola, BSI-Abteilungsleiter Standardisierung, Zertifizierung und Sicherheit von Telekommunikationsnetzen





Speakers' Corner

Die Speakers´ Corner feierte in diesem Jahr am BSI-Stand erfolgreich ihre Premiere. Unter dem Motto „Fachthemen kompakt präsentiert" gaben BSI-Expertinnen und -Experten Einblicke in unterschiedliche Aspekte der Cyber-Sicherheit.

„Bericht zur Lage der IT-Sicherheit in Deutschland 2022" vorgestellt

Im Rahmen der it-sa stellte BSI-Vizepräsident Dr. Gerhard Schabhüser am 25. Oktober den aktuellen BSI-Lagebericht vor. Der Bericht informiert über die IT-Sicherheitslage in Deutschland.
Interessierte hatten vor Ort die Gelegenheit, bei Vorträgen BSI-Erkenntnisse und Einblicke in die Cyber-Bedrohungslage zu bekommen.

Präsentieren die ersten Exemplare des BSI-Lageberichts: Prof. Dr. Roland Fleck, CEO Nürnberg-Messe GmbH; Roland Weigert, MdL, Staatssekretär im Bayerischen Staatsministerium für Wirtschaft, Landesentwicklung und Energie; BSI-Vizepräsident Dr. Gerhard Schabhüser; Peter Ottmann, CEO NürnbergMesse GmbH; Thomas Preutenborbeck, Mitglied der Geschäftsleitung NürnbergMesse GmbH

10 Jahre Allianz für Cyber-Sicherheit

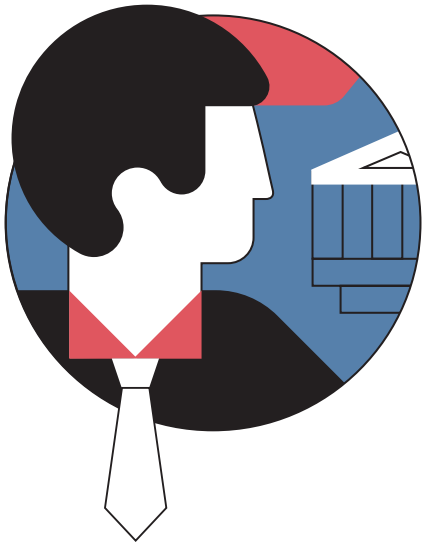
Das Jubiläum von Europas größtem Netzwerk für Cyber-Sicherheit wurde auf der Messe mit einem eigenen Bereich gewürdigt.

Jetzt schon vormerken!
Wir sehen uns bei der nächsten it-sa vom 10.-12. Oktober 2023.

Bedrohung so hoch wie nie

Die Lage der IT-Sicherheit in Deutschland 2022

Mit dem Bericht „Die Lage der IT-Sicherheit in Deutschland“ informiert das BSI einmal im Jahr über die Gefährdungslage der IT-Sicherheit im Berichtszeitraum. Der diesjährige Lagebericht zeigt klar auf, dass die Gefährdungslage zwar sehr hoch ist, wir den Gefahren jedoch nicht schutzlos ausgeliefert sind.



KRITISCHE LAGE SPITZT SICH WEITER ZU

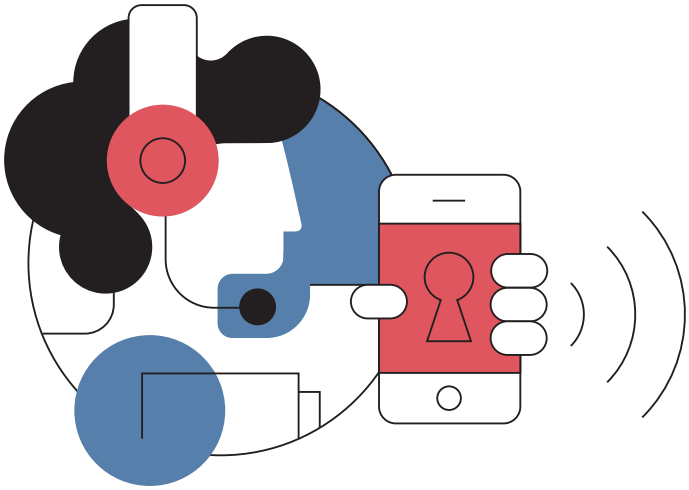
Die bereits angespannte IT-Sicherheitslage in Deutschland spitzt sich in diesem Berichtszeitraum weiter zu. Die Bedrohung im Cyber-Raum ist damit so hoch wie nie. Verantwortlich waren neben der anhaltenden Bedrohung durch Cybercrime, Gefahren durch den Angriffskrieg Russlands gegen die Ukraine. In Deutschland gab es eine Ansammlung kleinerer Vorfälle, die im Zusammenhang mit dem Angriffskrieg stehen, wie zum Beispiel Hacktivismus-Angriffe und Störungen der IT-Lieferketten sowie eine erhöhte Zahl an Charity-Scam-Mails. Eine übergreifende Angriffskampagne gegen deutsche Ziele war nicht ersichtlich, andere NATO-Partner haben im Cyber-Raum ernsthaftere Konsequenzen erfahren, die durch die erhöhte Vernetzung und Globalisierung auch über Ländergrenzen hinweg spürbar sind.

CYBER-ERPRESSUNG BLEIBT EINE DER GRÖSSTEN BEDROHUNGEN

Die aktuell größte Bedrohung im deutschen Cyber-Raum bleibt Ransomware, besonders für Unternehmen. Bei Ransomware handelt es sich um Schadsoftware, die den Zugriff auf Daten und Datenbanken über Verschlüsselung verhindert. Meist hinterlassen Angreifer eine Erpressernachricht, in der Regel eine Lösegeldforderung. Die Drohung: Sollte das Lösegeld nicht gezahlt werden, sind die Daten für das Unternehmen verloren. Außerdem wird mit der Veröffentlichung sensibler Informationen gedroht. Wird diese Art der Erpressung bei umsatzstarken Unternehmen angewandt, spricht man von Big Game Hunting. Aber auch für den Verwaltungsapparat stellen Ransomware-Angriffe eine reale Bedrohung dar, wie z. B. im letzten Jahr in Sachsen-Anhalt.

ERSTER DIGITALER KATASTROPHENFALL IN DEUTSCHLAND – DAS BSI HILFT VOR ORT

Im Juli 2021 wurde in einem Landkreis in Sachsen-Anhalt erstmals der Katastrophenfall nach einem Ransomware-Angriff auf eine Kreisverwaltung ausgerufen. Der Angriff hatte schwerwiegende Folgen: 207 Tage lang konnten keine bürgernahen Leistungen, z. B. das Zahlen von Eltern-, Sozial- oder Arbeitslosengeld, erbracht werden. Das BSI war mit einem mobilen Einsatzteam vor Ort, unterstützte jedoch auch von Bonn aus bei der weiteren Koordinierung des Krisenmanagements. In Zusammenarbeit mit der Bundeswehr analysierte das BSI den Angriff und die verwendete Software und beriet hinsichtlich des Wiederaufbaus und der Sicherheit der IT-Infrastruktur.

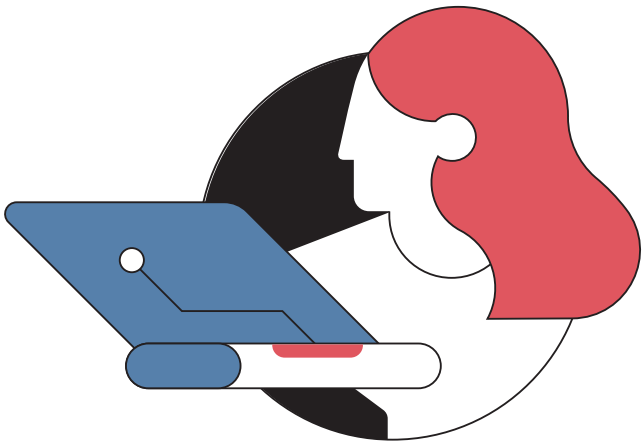


ZAHL DER SCHWACHSTELLEN STEIGT WEITER

Im Jahr 2021 wurden zehn Prozent mehr Schwachstellen in Software-Produkten bekannt als im Vorjahr. Mehr als die Hälfte von ihnen wiesen hohe oder kritische Scores nach dem Common Vulnerability Scoring System (CVSS) auf. Als kritisch wurden 13 Prozent der Schwachstellen bewertet. Zu ihnen zählt die Schwachstelle in Log4j, da sich diese in vielen frei verfügbaren Software-Bausteinen befand. IT-Sicherheitsverantwortliche konnten daher in der Regel nur schwer einschätzen, ob die von ihnen eingesetzte Software die Schwachstelle aufwies. Aufgrund der hohen Verbreitung von Log4j war von einer großen Angriffsfläche für Cyber-Angriffe auszugehen.

KRIMINALITÄT IM INTERNET

Die größten Bedrohungen für Verbraucherinnen und Verbraucher stellen Fake-Shops, Sextortion und Identitätsdiebstahl im Internet dar. Mehr als jeder Vierte ist im Berichtszeitraum Opfer von Internetkriminalität geworden. Hierbei fällt auf, dass die Zahlen der Fremdzugriffe auf Online-Konten und die Infektion mit Schadsoftware abgenommen haben, der Betrug beim Onlineshopping jedoch gestiegen ist. Zwei von fünf Befragten geben an, Sicherheitsempfehlungen zum Schutz vor Internetkriminalität



zu kennen, hiervon setzten allerdings nur etwas mehr als die Hälfte diese Empfehlungen (zum Teil) um. Dies spricht für die Notwendigkeit von mehr Informationen, besonders da sich Opfer von Internetkriminalität in der Regel selbst helfen.

SCHUTZ DURCH PRÄVENTIVE MASSNAHMEN

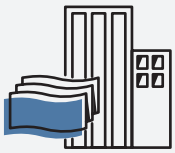
Globalisierung, Digitalisierung und Vernetzung gehen über Ländergrenzen hinaus, was viele Chancen ermöglicht, aber auch mit potenziellen Risiken verbunden ist, wie der Angriffskrieg Russlands gegen die Ukraine vor Augen führt. Das vergangene Jahr hat gezeigt, dass unvorhergesehene Ereignisse die Bedrohungslage auf ein neues Level heben können und Kollateralschäden durch Cyber-Angriffe in Nachbarländern auch unmittelbare Auswirkungen auf Deutschland haben können. Und der Bericht zeigt deutlich: Präventive Maßnahmen sind die wirkungsvollsten IT-Schutzmaßnahmen. Jedes Computersystem, das nicht gehackt werden kann, jede IT-basierte Dienstleistung, die nicht gestört werden kann, ist ein elementarer Beitrag zu einer funktionierenden digital vernetzten Gesellschaft. ■

Weitere Informationen und den BSI-Lagebericht abonnieren:

Die Lage der IT-Sicherheit in Deutschland: https://www.bsi.bund.de/lageberichte

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Fake-Shops im Internet	Ransomware Schwachstellen, offene oder falsch konfigurierte Online-Server IT-Supply-Chain: Abhängigkeiten und Sicherheit	Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online-Server

Erster digitaler Katastrophenfall in Deutschland.

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

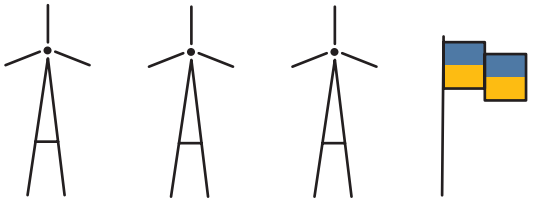
116,6 Millionen zugenommen

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken

Kollateralschaden

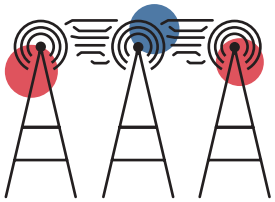
nach Angriff auf Satelliten-kommunikation



20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

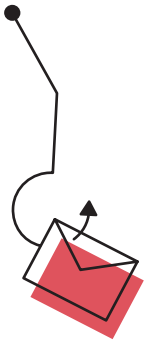
15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber



34.000
Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen

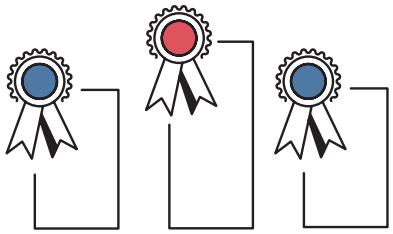
78.000
neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

69%
aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z. B. Phishing-Mails und Mail-Erpressung



90%
des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d. h., die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikaten



5.100
2021

4.400
2020

Zehn Jahre Allianz für Cyber-Sicherheit:
2022 sind wir bereits
6.220
Mitglieder

Deutschland Digital•Sicher•BSI•

Das #TeamBSI

Gestalterinnen und Gestalter von Cyber-Sicherheit

von Anna-Ris Kares, Referat Personalentwicklung

Motiv aus der Kampagne #TeamBSI – Jennifer Breuer

Von Informationssicherheitsberatung, digitalen Identitäten bis hin zu Kryptografie und Kritischen Infrastrukturen (KRITIS): Die Aufgaben des BSI sind vielfältig und wachsen durch die zunehmende Digitalisierung weiter. Mit der Umsetzung der Cybersicherheitsagenda des BMI soll das BSI künftig weitere Aufgaben übernehmen. Das #TeamBSI steht mit großer Fachkompetenz dafür zur Verfügung – und sucht gleichzeitig nach Verstärkung.

Beim #TeamBSI zählt vor allem eins: Teamgeist. Unsere Ziele können wir nur gemeinsam erreichen, um Deutschland auf seinem Weg in die sichere digitale Zukunft begleiten zu können. Jede und jeder Mitarbeitende leistet dafür ihren bzw. seinen Beitrag.

Um diese Aufgaben auch in Zukunft bewältigen zu können, muss das Team wachsen – und das in einem Markt, der speziell im IT-Bereich hart um Fachkräfte ringt. Dabei werden nicht nur die Kandidatinnen und Kandidaten für neue Jobs bewertet, sondern zunehmend auch die Arbeitgeber. Das Internet mit seinen Online-Kommentaren und -Rezensionen ist dafür ein wichtiger Ort. Für uns als Organisation bedeutet das: Versprechen, die wir nach außen machen, müssen wir nach innen auch halten. Es ist nicht nur wichtig, dass wir als BSI neue, zu uns passende Mitarbeitende gewinnen. Es ist genauso wichtig, diese neuen Mitarbeitenden auch zu binden.

GEKOMMEN, UM ZU BLEIBEN

Auch das BSI muss im Wettbewerb um die besten Köpfe als Arbeitgeber überzeugen. Die gute Nachricht ist: Bei uns arbeiten schon sehr viele der besten Köpfe. Das prägt nicht nur die Qualität unserer Arbeit, sondern gibt uns u. a. auch den Raum, motivierte und qualifizierte Absolventinnen und Absolventen mit wenig praktischer Berufserfahrung einzustellen. Die Praxislücken füllen wir durch ein vielfältiges Fort- und Weiterbildungsangebot – nicht nur im Bereich der Fachlichkeit, sondern auch in der Persönlichkeitsentwicklung. In der täglichen Arbeit können unsere neuen Kolleginnen und Kollegen von der Expertise der langjährigen BSI-Mitarbeiterinnen und -Mitarbeiter profitieren und werden „on the job" ganz praktisch zu Expertinnen und Experten weitergebildet.

#TEAMBSI: DIGITALKOMPETENZ UND INNOVATION

Im Fokus unserer Employer-Branding-Kampagne #TeamBSI stehen die Aspekte, die uns als Behörde und Arbeitgeber auszeichnen: Teamgeist und Digitalkompetenz. Mit der Kampagne stellen wir uns hinsichtlich unserer vielfältigen Fachbereiche, Aufgaben und Zielgruppen so breit wie möglich auf. Wir wollen sowohl Hochschul-Absolventinnen und -Absolventen als auch erfahrene Expertinnen und Experten ansprechen, die mit uns die Informationssicherheit in Deutschland und über die Grenzen hinaus gestalten wollen.

Das #TeamBSI leistet einen großen gesamtgesellschaftlichen Beitrag zu einer sicheren Digitalisierung. Mit der Kampagne möchten wir nicht nur das BSI als Arbeitgeber präsentieren, sondern auch zeigen, welche spannenden Aufgabenfelder der öffentliche Dienst bietet.

BINDUNG DER MITARBEITENDEN DURCH IDENTIFIKATION UND BETEILIGUNG STÄRKEN

Neben den spannenden Aufgaben und zukunftsweisenden Projekten ist vor allem das Mitgestalten eines gesellschaftlich relevanten Themas eine wichtige Motivation für unsere Mitarbeiterinnen und Mitarbeiter, die zu einer sehr hohen Identifikation mit dem BSI und seinen Aufgaben führt. Viele Kolleginnen und Kollegen aus den Fachabteilungen empfinden ihre Arbeit nicht als Job, sondern als Berufung. Klingt komisch, ist aber so: Die Begeisterung für den Job und die Aufgaben ist im BSI spürbar.

„Das BSI als die Cyber-Sicherheitsbehörde des Bundes soll mit der Umsetzung der Cybersicherheitsagenda des BMI weitere Aufgaben erhalten. Dafür braucht es ein stark aufgestelltes BSI mit den nötigen Befugnissen und einer ausreichenden Zahl von Fachkräften, um das erforderliche Know-how bereitstellen zu können."

Dr. Gerhard Schabhüser, Vizepräsident des BSI

Diese Stimmung hat uns dazu bewogen, unsere Mitarbeitenden von Anfang an in die Konzeption unserer Arbeitgeber-Kampagne einzubinden. Ein Thema, das uns dabei besonders am Herzen liegt: Im #TeamBSI setzen wir auf Vielfalt. Unsere Mitarbeitenden sind keine Stereotypen, sondern ein buntes Team: Sie zeichnen sich durch unterschiedliche Perspektiven, Charaktere und Erfahrungen aus, die für den Zusammenhalt im #TeamBSI äußerst wichtig sind. Wir wollen daher mit der Kampagne auch das Bewusstsein für diese Diversität schärfen und mithelfen, dass alle neuen und alle gegenwärtigen Kolleginnen und Kollegen nicht einfach nur bei uns dabei sind, sondern sich zugehörig fühlen. Die große Bereitschaft der Mitarbeitenden, die Kampagne mit ihrem Gesicht aktiv mitzugestalten, bestätigt uns in diesem Ziel, das sich direkt in unserem neuen Arbeitgeberauftritt widerspiegelt: Wir haben zehn Kolleginnen und Kollegen ausgewählt, die Einblicke in ihre Arbeitswelt geben und zeigen, dass die Behörde BSI aus motivierten und qualifizierten Menschen besteht. Unsere Protagonistinnen und Protagonisten erzählen authentisch, ehrlich und spontan von ihren Erfahrungen und Erlebnissen und davon, wie sie ihre Arbeit beim BSI empfinden. ■

Weitere Informationen:

#TeamBSI Kampagnenseite:
https://www.bsi.bund.de/DE/Karriere/Team_BSI/team_bsi_node.html

Lust die digitale Welt mitzugestalten?

Bringt mit uns die sichere digitale Zukunft voran und verstärkt das #TeamBSI mit eurem Engagement und eurer Expertise rund um Cyber-Sicherheit.

Bundesamt
für Sicherheit in der
Informationstechnik

Mehr Infos auf:

www.team-bsi.de

Wir geben dem #TeamBSI ein Gesicht: Dr. Friederike Laus

Dr. Friederike Laus arbeitet seit September 2019 im BSI und ist aktuell als Referentin im Referat Prüfung von Kryptoverfahren im höheren Dienst tätig. Zu ihren Schwerpunkten gehören Seitenkanalanalysen, insbesondere Verfahren aus den Bereichen Machine Learning und Künstliche Intelligenz sowie die kryptografische Evaluierung von Messengern und Audio- und Videokonferenzlösungen. Wir haben uns mit Friederike über ihre Arbeit und ihre Teilnahme an der Kampagne #TeamBSI unterhalten.

Motiv aus der Kampagne #TeamBSI – Dr. Friederike Laus

Friederike, wie bist du Referentin für die Prüfung von Kryptoverfahren geworden?

Auf Umwegen: Ursprünglich hatte ich mich auf eine Stelle im Nationalen Cyber-Abwehrzentrum beworben. Dort wurde ich gefragt, ob ich mir auch eine Tätigkeit im Bereich Cyber-Sicherheit für intelligente Transportsysteme und Industrie 4.0 vorstellen könnte. Das klang für mich ebenfalls spannend, und so habe ich dann in diesem Referat angefangen. Allerdings habe ich schnell festgestellt, dass die Arbeit dort für mich als Mathematikerin zu angewandt ist. Als sich die Chance auf eine freie Stelle in einem der beiden Mathematik-Referate ergab, bin ich dann in der Prüfung von Kryptoverfahren gelandet, wo ich mich bestens aufgehoben fühle: Hier kann ich meine Fähigkeiten und meine Expertise voll einbringen.

Was macht für dich den Teamspirit im BSI aus?

Im BSI arbeiten viele Kolleginnen und Kollegen, die fachlich extrem fit sind und ihr Wissen gerne mit anderen teilen. Ich weiß, dass ich mich mit Fragen jederzeit an sie wenden kann, und unterstütze sie natürlich auch gerne selbst, wo immer ich kann – und das nicht nur referatsintern, sondern auch abteilungs- und behördenübergreifend. Dieser starke kollegiale Zusammenhalt in Kombination mit der hohen fachlichen Kompetenz macht für mich die Arbeit im BSI zu etwas ganz Besonderem.

Was motiviert dich bei deiner Arbeit im BSI?

Am besten gefällt mir, dass ich im BSI sehr forschungsnah arbeiten kann – ähnlich wie zuvor als Wissenschaftlerin an der Uni. Wir verfolgen Forschung und Entwicklungen in unseren Fachgebieten, um stets auf dem aktuellen Stand in der sehr schnelllebigen IT-Sicherheitsbranche zu bleiben, und forschen teilweise auch selbst. Während man sich jedoch an der Uni häufig mit eher theoretischen Themen beschäftigt, die vielleicht in ein paar Jahren mal zur Anwendung kommen, arbeiten wir hier an hochaktuellen Themen, die immer auch einen konkreten Anwendungsbezug haben.

Insgesamt bin ich sehr gerne für das BSI tätig und auch ein wenig stolz, Teil eines so kompetenten und engagierten Teams zu sein. Es erfüllt mich, dass ich meine Fähigkeiten hier gut einbringen und an etwas mitarbeiten kann, das dem Wohle der Allgemeinheit dient und nicht den Interessen einiger weniger. Das alles motiviert mich ungemein, jeden Tag aufs Neue alles zu geben und meinen Beitrag dazu zu leisten, Deutschland ein Stückchen digitaler und sicherer zu machen. ■

Cyber-Sicherheitsniveau in Kommunen erhöhen

BSI startet „Roadshow Kommunen“ für mehr Cyber-Resilienz im öffentlichen Sektor

von den Referaten Informationssicherheitsberatung für Länder und Kommunen und Referat Nationales Verbindungswesen

Es war das erste Mal, dass eine Kommune in Deutschland wegen eines Hackerangriffs den Katastrophenfall ausgerufen hat. Der Landkreis Anhalt-Bitterfeld sah sich im Juli 2021 dazu gezwungen, weil seine IT-Systeme durch einen Cyber-Angriff so nachhaltig lahmgelegt wurden, dass für mindestens eine Woche die Auszahlung von Elterngeld, Arbeitslosen- und Sozialgeld nicht möglich war. Um die Resilienz gegen solche und ähnliche Cyber-Angriffe im kommunalen Umfeld zu erhöhen und das Cyber-Sicherheitsniveau insgesamt zu verbessern, hat das BSI die digitale Veranstaltungsreihe „Roadshow Kommunen“ ins Leben gerufen.

Folgenschwere Cyber-Vorfälle wie der in Anhalt-Bitterfeld erzeugen bei vielen Kommunen Unsicherheit darüber, ob die eigenen IT-Infrastrukturen ausreichend vor Cyber-Angriffen geschützt sind. Die Häufung der Fälle zeigt, dass gerade im kommunalen Bereich kein einheitliches und oft auch ein zu niedriges Cyber-Sicherheitsniveau existiert.

Das Nationale Verbindungswesen – Anlaufstelle des BSI unter anderem für Bundesbehörden, Länder und Kommunen – und die Informationssicherheitsberatung für Länder und Kommunen des BSI haben diese Herausforderungen erkannt und deshalb das speziell an die Zielgruppe Kommunen gerichtete neue Format „Roadshow Kommunen“ erarbeitet.

KOMMUNEN FÜR IT-SICHERHEITSFRAGEN SENSIBILISIEREN

Die Grundidee der „Roadshow Kommunen“ ist die Durchführung einer gemeinsamen virtuellen Veranstaltung mit interessierten Bundesländern. Ziel hierbei ist es, Kommunen bezüglich der Bedrohungen im Cyber-Raum zu sensibilisieren und Handlungsoptionen zur Erhöhung des Cyber-Sicherheitsniveaus aufzuzeigen. Die Planung und Durchführung der Veranstaltung erfolgt unter Einbeziehung der Länder und der kommunalen Spitzenverbände. Das BSI bringt in das Format unter anderem Vorträge aus den Bereichen Informationssicherheitsberatung für Länder und Kommunen, Nationales Verbindungswesen, CERT-Bund, BSI-Standards und IT-Grundschutz ein. Die Länder ergänzen mit unterschiedlichen, individuell auf das Land zugeschnittenen Vorträgen, um den Kommunen Handlungsempfehlungen, Best Practices und Erfahrungsberichte zur Verfügung zu stellen, die ihnen für ihre Arbeit im Bereich der IT-Sicherheit Mehrwerte bieten.

ORGANISATION UND ABLAUF DER ROADSHOW

Sofern ein Land Interesse an der Durchführung einer „Roadshow Kommunen“ bekundet, erfolgen ein oder mehrere Abstimmungstermine, um die Veranstaltung gemeinsam inhaltlich und terminlich auszugestalten. Hiernach wird eine gemeinsame Einladung erstellt, die etwa vier Wochen vor der Roadshow über die Landesverwaltungen an die Kommunen des jeweiligen Landes versandt wird.

Während der Online-Veranstaltung adressieren die Moderatorinnen und Moderatoren Fragen der Teilnehmenden über einen speziellen Chat. Ausgewählte Fragen werden im Anschluss an die einzelnen Fachvorträge von den Vortragenden

Im Kern steuert das BSI die folgenden Programmpunkte für die Roadshow bei:

Keynote der BSI-Amtsleitung
Die Amtsleitung unterstreicht mit einer Keynote die Bedeutung von Cyber-Sicherheit in Kommunen und skizziert hierbei die aktuellen Herausforderungen und Bedrohungen.

Vortrag: Bedrohungslage und Erfahrungen aus Ransomware-Angriffen
In einem Beitrag zur Bedrohungslage bei Kommunen bringt das BSI seine Erfahrung aus der Bearbeitung von Ransomware-Vorfällen in Wirtschaft und Verwaltung ein. Dazu gibt es eine Einschätzung der Bedrohungslage, aus der sich die Notwendigkeit ableitet, für einen angemessenen Schutz der kommunalen Verwaltungen zu sorgen. Dafür stellt das BSI präventive Maßnahmen vor, die über den IT-Basisschutz hinausgehen. Und für den Fall, dass ein Angriff nicht verhindert werden konnte, stellt das BSI reaktive Maßnahmen vor, die präventiv, also vor einem Angriff, vorgedacht und vorbereitet werden sollten.

Vortrag: Informationssicherheit für Kommunen
Informationssicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung und sollte nach einem ganzheitlichen Ansatz umgesetzt werden. In diesem Vortrag stellt das BSI dar, über welche Schritte und Hilfsmittel sich ein Managementsystem für Informationssicherheit erfolgreich aufbauen lässt. Dabei geht das BSI auch auf den IT-Grundschutz, das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ und die Unterstützungsmöglichkeiten der Cyber-Sicherheitsbehörde des Bundes ein.

Präsentation: Onlinezugangsgesetz (OZG)
Das OZG schreibt vor, Verwaltungsleistungen über alle Länder und administrativen Ebenen hinweg über den Portalverbund zu verknüpfen. Damit betreffen Sicherheitsrisiken innerhalb des Verbunds potenziell natürlich eine große Anzahl an Personen, Institutionen und Anwendungen. Zum Schutz des Verbunds hat das Bundesministerium des Innern und für Heimat (BMI) im Januar 2022 die „IT-Sicherheitsverordnung Portalverbund“ erlassen, die auch Kommunen gewisse Sicherheitsstandards vorschreibt. In der Präsentation stellt das BSI die Anforderungen und Schutzmaßnahmen vor.

Sonstige Angebote des BSI
In diesem Vortrag zeigt das BSI eine Auswahl an Produkten und Angeboten der Behörde, die geeignet sind, das Cyber-Sicherheitsniveau in den Kommunen zu erhöhen. Dazu gehört auch die Teilnahme an der Allianz für Cyber-Sicherheit.

beantwortet. Fragen, die während der Veranstaltung nicht beantwortet werden können, werden in den FAQ im Nachgang beantwortet und gemeinsam mit den Vortragsfolien an die Teilnehmenden verteilt.

ERSTE ROADSHOWS IN SACHSEN, NIEDERSACHSEN, SACHSEN-ANHALT UND THÜRINGEN

Die erste Roadshow fand Anfang Mai im Freistaat Sachsen statt, wo Führungskräfte, Ansprechpartnerinnen und -partner für Informationssicherheit aus den Kommunen an der virtuellen Veranstaltung von BSI und Sächsischer Staatskanzlei teilnahmen. Die Bedeutung von Kommunen in der Cyber-Sicherheitsarchitektur in Deutschland wurde auch durch die Teilnahme von hochkarätigen Entscheiderinnen und Entscheidern aus Politik und Wirtschaft unterstrichen. Dem Auftakt folgten Roadshows in Niedersachsen, Sachsen-Anhalt und Thüringen mit stetig steigenden Teilnehmerzahlen, die das große Interesse und den Bedarf der Kommunen für das Themenfeld belegen. Allein für die erste Roadshow in Sachsen wurden rund 180 Anmeldungen registriert. Darüber hinaus fanden Ende November „Roadshows Kommunen“ mit den Ländern Nordrhein-Westfalen und Mecklenburg-Vorpommern statt, weitere sind für 2023 geplant. ■

Ein perfektes Paar: Informationssicherheit und digitale Verwaltung

von Prof. Thomas Popp, Staatssekretär für Digitale Verwaltung und Verwaltungsmodernisierung sowie CIO des Freistaates Sachsen

Bürgerinnen und Bürger sowie Unternehmen erwarten zu Recht von einer modernen Verwaltung, dass sie digitale Leistungen zuverlässig und sicher bereitstellt. Je vernetzter und digitaler gearbeitet wird, desto wichtiger ist jedoch die Informationssicherheit. Wie macht es der Freistaat Sachsen?

Kurzvita Prof. Thomas Popp
Staatssekretär für Digitale Verwaltung und Verwaltungsmodernisierung und CIO des Freistaates Sachsen

Thomas Popp wurde am 8. November 1961 in Schweinfurt geboren. Seit Anfang 2015 ist er in der Sächsischen Staatskanzlei tätig, der er seit April 2018 als Amtschef vorsteht. Mit Wirkung zum 1. August 2018 erfolgte darüber hinaus die Ernennung zum Beauftragten für Informationstechnologie (Chief Information Officer – CIO) des Freistaates Sachsen. Am 20. Dezember 2019 wurde Thomas Popp zum Staatssekretär und Mitglied der Sächsischen Staatsregierung ernannt.

Mehr digitale Verwaltung ist eine legitime Forderung. Allerdings geht dies nur, wenn wir die Sicherheit der Daten und der IT-Infrastruktur gewährleisten. Prävention, Notfallvorsorge und Hilfe im Ernstfall sind bei der Informationssicherheit unser tägliches Handwerk. Das gilt für die staatliche Verwaltung und besonders für die Kommunen. Dort, wo ein Großteil der Leistungen für die Bürgerinnen und Bürger und für Unternehmen erbracht wird, muss Informationssicherheit wirklich großgeschrieben werden.

MEHR INFORMATIONSSICHERHEIT GEHT IMMER

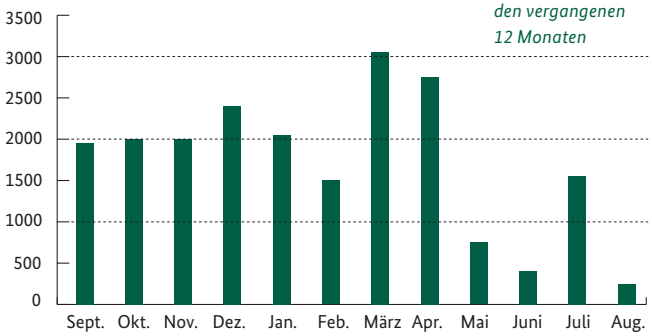
Selbstverständlich gibt es keine hundertprozentige Informationssicherheit. Aber es besorgt mich, dass die Informationssicherheit nicht überall mit dem nötigen Nachdruck verfolgt wird. Dabei ist mit dem 2019 verabschiedeten Informationssicherheitsgesetz der rechtliche Rahmen gesetzt.

Auch den sächsischen Kommunen sind damit diverse Pflichten auferlegt. Das beinhaltet zum Beispiel die Benennung eines Beauftragten für Informationssicherheit. Kommunen werden zunehmend zum Ziel von Cyber-Angriffen, teilweise mit gravierenden Folgen. Je mehr digitale Angebote bereitgestellt werden, desto größer wird auch das mögliche Schadensszenario. Deshalb müssen wir jetzt umdenken. Informationssicherheit ist die Pflichtversicherung für Kritische Infrastrukturen, zu denen nach unserem Verständnis auch die Kommunen gehören. Genau darum muss sich der Beauftragte für Informationssicherheit aktiv in Behörden und Kommunen kümmern.

INFORMATIONSSICHERHEIT ALS DIENSTLEISTUNG

Um die staatlichen Stellen und Kommunen im täglichen Kampf gegen Cyber-Kriminelle zu unterstützen, nimmt das sächsische Sicherheitsnotfallteam SAX.CERT eine zentrale Rolle ein. Es analysiert die Lage der Informationssicherheit und gibt diese Informationen weiter. Es wertet eine Vielzahl von Quellen aus, insbesondere der zentralen Schutzsysteme des Sächsischen Verwaltungsnetzes und der monatlichen Sicherheitsscans von über 6.000 Webseiten der Landes- und Kommunalverwaltung. Daraus werden Schlüsse gezogen und Maßnahmen abgeleitet, um die Sicherheit weiter zu verbessern. Kommt es zu einem IT-Sicherheitsereignis oder gar zu einem IT-Sicherheitsvorfall, unterstützt und berät das SAX.CERT die Betroffenen. Besondere Dienstleistungen zur Cyber-Abwehr bietet das SAX.CERT kostenfrei allen sächsischen Staats- und Kommunalverwaltungen an. Dazu gehören zum Beispiel ein „Einbruchsmelder“ für unerwünschte Zugriffe oder ein individualisierter Schwachstellenwarndienst.

Schadsoftware im Internet-Verkehr in den vergangenen 12 Monaten

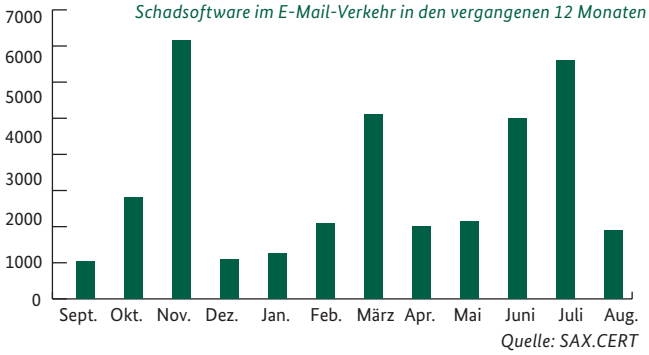


Quelle: SAX.CERT

DER FAKTOR MENSCH

Technische Schutzsysteme und Spezialisten sind zwei wichtige Pfeiler, auf denen Informationssicherheit ruht. Es entscheidet aber jeder Verwaltungsbedienstete und jede Führungskraft mit seinem oder ihrem Verhalten über das Informationssicherheitsniveau. Oft gelingt ein Angriff, weil der Faktor Mensch versagt. Wenn die technischen Schutzmechanismen die dicken Mauern und den unüberwindbaren Burggraben symbolisieren, dann ist der unbedachte Click auf einen per E-Mail versandten Link der Hebel, der die Zugbrücke herunterlässt und so dem Angreifer das sprichwörtliche Einfallstor bietet.

Schadsoftware im E-Mail-Verkehr in den vergangenen 12 Monaten



Quelle: SAX.CERT

Solche Dinge passieren, weil Cyber-Kriminelle sich darauf verstehen, menschliche Eigenschaften wie Neugier oder Mitgefühl auszunutzen und ihre potenziellen Opfer zu manipulieren. Über Risiken aufzuklären und Bedienstete für mehr Achtsamkeit im digitalen Alltag zu sensibilisieren, ist deshalb unerlässlich.

Für alle Bediensteten von sächsischen Landes- und Kommunalbehörden bieten wir dafür kostenfrei ein E-Learning-Programm an. Bislang wurde es über 17.000-mal absolviert. Besonderen Zuspruch erhalten wir für die Veranstaltung „Die Hacker kommen" – ein anschauliches Format, das wir regelmäßig für unsere Bediensteten anbieten. Dabei wird auf unterhaltsame Weise dargestellt, welche Gefahren im digitalen Arbeitsumfeld lauern, welchen Schaden sie anrichten können und wie man sie umgehen kann. Über 15.000 Bedienstete haben an diesem Event bereits teilgenommen.

Spezielle Veranstaltungsformate wie die „Roadshow Kommunen" des BSI am 2. Mai dieses Jahres tragen ebenfalls dazu bei, das Bewusstsein für Informationssicherheit besonders bei den sächsischen Kommunen zu schaffen und weiter zu stärken.

Der sächsische Staatssekretär für Digitale Verwaltung und Verwaltungsmodernisierung, Professor Thomas Popp (links), und der Leiter des sächsischen Sicherheitsnotfallteams SAX.CERT, Prof. Dr. Karol Kozak, präsentieren in der Innovationslounge auf dem ITOF ihre Dienstleistungen zur Cyber-Abwehr, die alle Behörden und Kommunen nutzen können.

ITOF – GEMEINSAM, DIGITAL, ERFOLGREICH

Informationssicherheit war auch ein Schwerpunktthema beim 10. IT- und Organisationsforum (ITOF), das im September im Dresdner Flughafen stattfand. Die rund 500 Teilnehmerinnen und Teilnehmer aus sächsischen Staats- und Kommunalbehörden konnten sich in Vorträgen, an Ausstellerständen und in der Innovationslounge darüber informieren, wie eine sichere digitale Verwaltung funktioniert. So präsentierte das Sicherheitsnotfallteam SAX.CERT seine Dienstleistungen zur Cyber-Abwehr, beispielsweise den Einbruchssensor HoneySense, einen Passwortchecker oder den Webseitenscan. Das ITOF ist die wichtigste verwaltungsinterne Veranstaltung des Freistaates Sachsen. Es bringt staatliche und kommunale Vertreter zum Erfahrungsaustausch zueinander.

FAZIT

Wir brauchen mehr digitale Verwaltung, um auch künftig unseren Auftrag erfüllen zu können. Eine komplexe technische Infrastruktur und mehr digitale Vernetzung im Arbeitsalltag helfen uns dabei. Allerdings müssen wir in der Architektur unserer Systeme und im Arbeitsalltag darauf achten, Informationssicherheitsstandards einzuhalten. Wir müssen das Thema überall zur höchsten Priorität bei Führungskräften machen und gemeinsam an Prävention und Notfallvorsorge arbeiten. ■

Weitere Informationen:

Startseite SAX.CERT:
https://www.cert.sachsen.de/

So kommen die Lichtbilder für Ihren Ausweis zukünftig in die Behörde

Sichere elektronische Übermittlung von Lichtbildern an Pass-, Personalausweis- und Ausländerbehörden

von Ann-Kristin Derst, Joschka Olbrück & Sebastian Palm, Referat eID-Lösungen für die digitale Verwaltung

Wie können biometrische Lichtbilder von einer Fotografin oder einem Fotografen sicher auf digitalem Weg an hoheitliche Stellen übertragen werden? Diese Frage beantwortet die Technische Richtlinie BSI TR-03170 „Sichere elektronische Übermittlung von Lichtbildern an Pass-, Personalausweis- und Ausländerbehörden“.

Das „Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen“ (PassAuswRÄndG) enthält eine Reihe von Neuregelungen, wie elektronisch erfasste Lichtbilder sicher an Pass-, Personalausweis- und Ausländerbehörden übermittelt werden können. Mit dem Gesetz wollen Bundestag und Bundesrat insbesondere Manipulationen von Lichtbildern auf hoheitlichen Dokumenten durch Morphing gezielt begegnen. Morphing bezeichnet eine Bildmanipulationstechnik, bei der die Gesichtsmerkmale von zwei oder mehr Personen zu einem einzigen Gesicht auf einem Foto gemorpht bzw. verschmolzen werden. Mit seiner Veröffentlichung im Bundesgesetzblatt ist das Gesetz seit dem 11. Dezember 2020 in Kraft.

Schon seit 2014 regelt die Technische Richtlinie TR-03146 („E-Bild hD“) die Übermittlung von Lichtbildern als Anhang einer De-Mail. Mit der Verabschiedung des PassAuswRÄndG wurde das BSI beauftragt, zwei weitere Prozesse zur sicheren Übermittlung zu entwerfen. Eine Variante sind Selbstbedienungsterminals („Live Enrolment Stations“) in den Pass-, Personalausweis- und Ausländerbehörden. Der Versand über diese Geräte wird in der Technischen Richtlinie TR-03121 geregelt. Des Weiteren wird es die Möglichkeit der Übermittlung nach TR-03170 geben, die im Folgenden dargestellt wird:

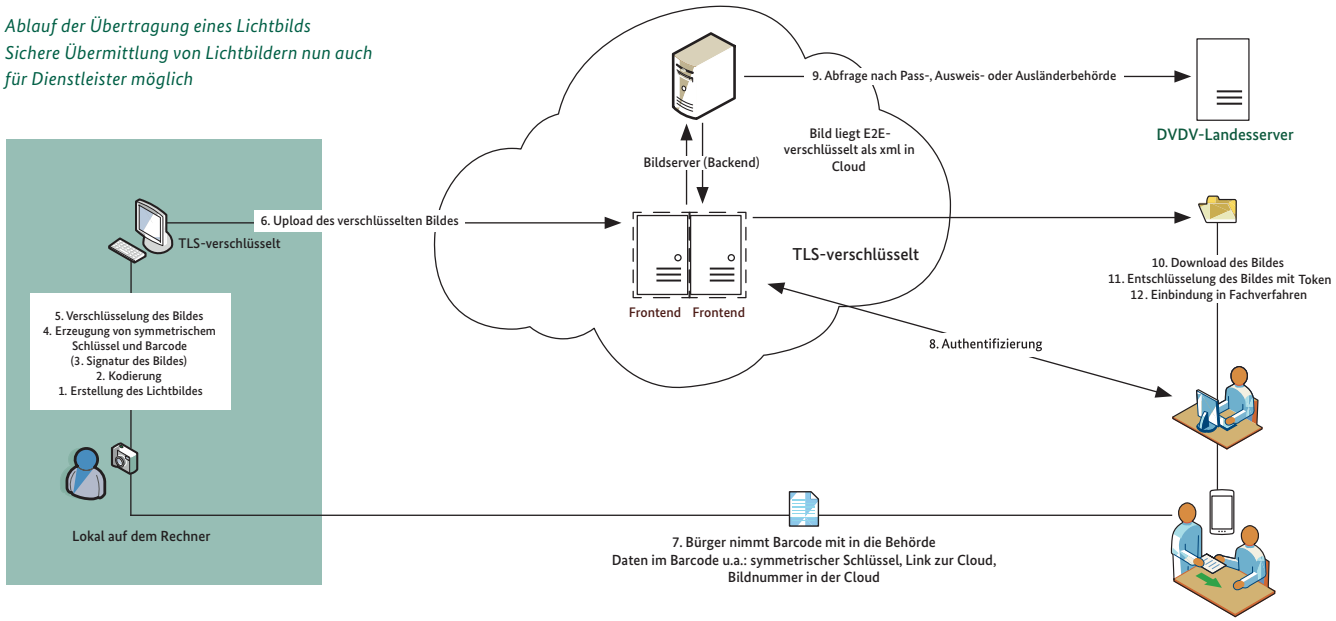
SICHERE ÜBERMITTLUNG DER LICHTBILDER VON DIENSTLEISTERN

Ausgangspunkt für den neuen Übermittlungsprozess sind Dienstleister wie Fotografinnen und Fotografen, die Lichtbilder an einen Cloud-Dienst übermitteln können sollen. Sie müssen sich dafür vorab bei dem Cloud-Anbieter registrieren, da nur registrierte und verifizierte Dienstleister Lichtbilder über diesen Weg übertragen dürfen. Zudem sind nur solche Cloud-Dienste für die Übermittlung zugelassen, die in das Deutsche Verwaltungsdiensteverzeichnis (DVDV) eingetragen sind.

Im Rahmen der sicheren digitalen Lichtbildübermittlung finden die folgenden Prozessschritte statt:

1. Die Bürgerin/Der Bürger lässt vom registrierten Dienstleister ein biometrisches Lichtbild erstellen.
2 Gegebenenfalls wird das Lichtbild durch den Dienstleister signiert.
3. Noch beim Dienstleister werden für das Lichtbild ein symmetrischer Schlüssel und ein Barcode erzeugt. Der Barcode beinhaltet neben dem symmetrischen Schlüssel auch eine eindeutige Kennung für das Lichtbild und die URL des Cloud-Anbieters.
4. Das Lichtbild wird mit dem symmetrischen Schlüssel verschlüsselt.
5. Der Dienstleister überträgt das verschlüsselte Lichtbild über die Upload-Schnittstelle an den Cloud-Dienst.
6. Die Bürgerin oder der Bürger bekommt vom Dienstleister einen Barcode, mit dem bei der Behörde das Ausweisdokument beantragt werden kann.
7. Die Pass-, Personalausweis- oder Ausländerbehörde ruft das elektronische Lichtbild beim Cloud-Dienst unter Verwendung der Kennung aus dem Barcode ab.
8. Dazu prüft der Cloud-Dienst über das DVDV anhand der Behördenkategorie, ob die Behörde zum Abruf berechtigt ist.
9. Damit kann sich die Behörde gegenüber dem Cloud-Dienst authentisieren.
10. Die Behörde lädt das Lichtbild herunter.
11. Anschließend wird die möglicherweise vorgenommene Signatur validiert und das Lichtbild entschlüsselt. Die Entschlüsselung ist nur möglich, wenn der Behörde der korrekte Schlüssel als Teil des Barcodes ausgehändigt wurde.
12. Das Lichtbild wird in das behördliche IT-Fachverfahren zur Ausstellung des Dokuments eingebunden.

Ablauf der Übertragung eines Lichtbilds
Sichere Übermittlung von Lichtbildern nun auch für Dienstleister möglich



Der Prozess ermöglicht die flexible Nutzung elektronisch erfasster Lichtbilder von Dienstleistern durch die Behörden. Dabei ist es wichtig zu wissen, dass die Bürgerinnen und Bürger nicht an eine bestimmte Behörde für den Abruf gebunden sind, sondern diese frei wählen können: Über die Richtlinie ist es möglich, dass jede berechtigte Behörde das Lichtbild vom autorisierten Cloud-Dienst abrufen kann. So kann dasselbe Lichtbild beispielsweise bei mehreren Antragsverfahren genutzt werden, solange die Löschfrist des Lichtbildes noch nicht erreicht ist.

Die Prüfung der Berechtigung einer Behörde über das DVDV stellt sicher, dass nur zuständige Behörden Lichtbilder abrufen und weiterverarbeiten können. Das Verfahren setzt zudem konsequent auf eine Ende-zu-Ende-Verschlüsselung. Das gewährleistet, dass nach dem Upload keine Veränderungen am Lichtbild vorgenommen werden können. Außerdem wären die Lichtbilder auf diese Weise selbst bei einer Kompromittierung des Cloud-Anbieters vor unberechtigtem Zugriff geschützt.

Es ist geplant, das neue Verfahren den Bürgerinnen und Bürgern zur sicheren Übertragung ihrer Lichtbilder bis spätestens 2025 zur Verfügung zu stellen. ■

Weitere Informationen:

Technische Richtlinie TR-03170:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03170/tr-03170.html

Mehr Sicherheit im Straßenverkehr

Kooperative intelligente Transportsysteme

von Dr. Katharina Bräunlich, Referat eID-Strukturen für die Digitalisierung, und Torsten Matzerath, Referat Cyber-Sicherheit für intelligente Transportsysteme und Industrie 4.0

Die Vernetzung von Verkehrsteilnehmerinnen und -teilnehmern und Straßeninfrastrukturen ermöglicht die Entwicklung neuer Dienstleistungen und Funktionen. Solche „kooperativen intelligenten Transportsysteme“ sollen dazu beitragen, den Straßenverkehr sicherer, komfortabler und effizienter zu gestalten. Mit der Technischen Richtlinie BSI TR-03164 gibt das BSI Handlungsempfehlungen für den sicheren Betrieb dieser Systeme.

In kooperativen intelligenten Transportsystemen (englisch „Cooperative Intelligent Transport Systems“, C-ITS) sind Verkehrsteilnehmende und Straßeninfrastrukturen miteinander vernetzt und tauschen Nachrichten untereinander aus. Die Nachrichten werden zum Beispiel dazu genutzt, um vor gefährlichen Verkehrssituationen oder Straßenbedingungen zu warnen und den Verkehrsfluss zu regulieren. So können etwa Rettungskräfte über C-ITS andere Verkehrsteilnehmende im Falle eines Einsatzes warnen, damit Fahrzeuge rechtzeitig eine Rettungsgasse bilden können. Es ist auch möglich, Ampeln für Einsatzfahrzeuge auf Grün zu schalten, um ihnen ein ungehindertes und sicheres Vorankommen zu ermöglichen.

Damit Fahrzeuge oder Infrastrukturkomponenten C-ITS nutzen können, müssen sie mit dedizierten Hardware- und Softwarekomponenten ausgerüstet sein, sogenannten C-ITS-Stationen. Da die Systeme einen großen Einfluss auf Verkehrssicherheit und Verkehrsfluss haben, darf es Angreifenden nicht möglich sein, C-ITS-Nachrichten zu manipulieren und so Einfluss auf das Verkehrsgeschehen zu erlangen. Andernfalls könnten sie zum Beispiel vor einer nicht vorhandenen Gefahrenstelle warnen oder sich als Einsatzfahrzeug ausgeben.

Um das zu verhindern, dürfen nur hinreichend sicher gestaltete und entsprechend zertifizierte C-ITS-Stationen genutzt werden. Zusätzlich werden Nachrichten in C-ITS digital signiert, denn digitale Signatur und eine Public-Key-Infrastruktur (PKI) gewährleisten die Integrität der C-ITS-Nachrichten und die Authentizität des Absenders einer C-ITS-Nachricht.

EU-KOMMISSION SORGT FÜR EINHEITLICHE VORGABEN

Mit Hilfe der Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems hat die Europäische Kommission einheitliche Vorgaben spezifiziert, um sowohl hersteller- und grenzübergreifende Interoperabilität als auch ein homogenes Sicherheitsniveau zu gewährleisten. Neben der European Certificate Policy gibt es auf europäischer Ebene weitere Spezifikationen, die die Umsetzung der Vorgaben konkretisieren und die durch das European Telecommunications Standards Institute (ETSI) erarbeitet wurden.

Die European Certificate Policy und die einschlägigen ETSI-Spezifikationen regeln einige Bereiche aber nicht hinreichend detailliert und vollständig, da beispielsweise Aspekte oder Prozesse nicht oder nicht ausreichend konkret betrachtet werden oder Interpretations- und Gestaltungsspielräume lassen. Dies birgt die Gefahr, dass die verschiedenen Stakeholder bei der Implementierung operativer C-ITS-Systeme Annahmen treffen, die unter Umständen nicht alle Sicherheitsaspekte zufriedenstellend berücksichtigen oder die die Interoperabilität gefährden.

TECHNISCHE RICHTLINIE BSI TR-03164 SORGT FÜR KLARHEIT

Um hier für mehr Klarheit und Sicherheit zu sorgen, hat das BSI Anfang 2022 die Technische Richtlinie BSI TR-03164 veröffentlicht. Sie ist als Ergänzung zu den europäischen Vorgaben zu sehen und verfolgt das Ziel, eine einheitliche Interpretationsbasis der einschlägigen Vorgaben zu schaffen und bei Gestaltungsspielräumen konkrete Empfehlungen für die Umsetzung zu geben. Damit sorgt die Technische Richtlinie für Klarheit und für Interoperabilität zwischen den Stakeholdern aus Industrie und öffentlicher Hand.
Die Richtlinie hilft zudem allen Beteiligten, Aspekte der IT-Sicherheit von vornherein zu berücksichtigen, so potenzielle Schwachstellen zu vermeiden und ein homogenes Sicherheitsniveau zu gewährleisten.

Die BSI-Richtlinie besteht aus zwei Teilen: Der erste Teil dient als Richtlinie für den sicheren Betrieb von Public-Key-Infrastrukturen für C-ITS. Der zweite Teil konkretisiert Konfiguration, Registrierung und den Betrieb von C-ITS-Stationen.

FAZIT

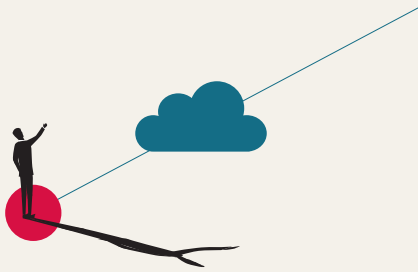
Kooperative intelligente Transportsysteme befinden sich aktuell noch im Aufbau. Derzeit starten erste Fahrzeughersteller und Straßeninfrastrukturbetreiber mit dem operativen Betrieb erster C-ITS-Dienste. Mit der Konkretisierung und Spezifikation von Anforderungen an C-ITS in dieser frühen Phase der Entwicklung und in Form einer Technischen Richtlinie will das BSI einen positiven Einfluss auf die Umsetzung operativer C-ITS-Systeme nehmen. Gemäß dem Paradigma „Security by Design“ werden Sicherheitsanforderungen somit schon vor der serienmäßigen Markteinführung hinreichend adressiert. Das macht die Systeme nicht nur sicherer, sondern soll sich auch positiv auf die rasche Verbreitung von C-ITS im Verkehr auswirken. ■

Weitere Informationen:

Technische Richtlinie TR-03164:
https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/TR_Transportsysteme_220117.html

BSI und NATO: Cloud-Sicherheit im Bündnis gestalten

von Sven Niedtfeld, Referat Internationale Beziehungen,
und Referat Technik-Kompetenzzentrum für Virtualisierung und Cloud-Sicherheit



Zur Erfüllung seiner gesetzlichen Aufgaben ist das BSI auch international tätig. Es agiert sowohl bilateral mit einer Vielzahl von Partnerbehörden in unterschiedlichen Ländern als auch eingebunden in internationale Organisationen. Die NATO ist eine der wichtigsten davon. Innerhalb des Verteidigungsbündnisses gestaltet das BSI derzeit aktiv die Cloud-Sicherheit mit.

Das BSI übernimmt für die Bundesrepublik Deutschland gegenüber der NATO die Rollen als nationale Kommunikationssicherheitsbehörde („National Communications Security Authority“) und als nationale Cyber-Sicherheitsbehörde („National Cyber Defence Authority“).

Es ist daher direkt in die Arbeit vieler NATO-Gremien und -Arbeitsgruppen mit technischem Schwerpunkt eingebunden und wirkt zudem beratend in Richtung Bundesministerium des Innern und für Heimat zu Cyber-Defence-Themen im Policy-Kontext. Durch sein Engagement im westlichen Verteidigungsbündnis festigt und steigert das BSI die Informationssicherheit für die Bundesrepublik Deutschland und für deren Verbündete. Der so gesicherte Informationsaustausch untereinander ist notwendige Voraussetzung dafür, dass die NATO sich auch in Zeiten von Krisen und Konflikten für Frieden und Stabilität im Nordatlantikraum einsetzen kann.

Die komplexe Struktur der Allianz ist eine echte Herausforderung für die handelnden Akteure. In der NATO gilt nämlich das Prinzip, dass Entscheidungen nur im Konsens der 30 (und nach Aufnahme von Finnland und Schweden 32) Mitgliedstaaten getroffen werden – obwohl sie eine Gemeinschaft ist, in der mitunter unterschiedliche Interessen vertreten werden. Seine Expertise sowie sein kontinuierliches Engagement ermöglichen es dem BSI, auch vor diesem Hintergrund eigene Akzente zu setzen und die Weiterentwicklung der Informationssicherheit mitzugestalten.
Ein gutes Beispiel für dieses erfolgreiche Engagement ist die Ausarbeitung und Verabschiedung der „Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-based Communication and Information Systems“ für „NATO UNCLASSIFIED“.

SICHERE PUBLIC CLOUDS FÜR DIE NATO

Die NATO misst der Digitalisierung ihrer eigenen Prozesse eine hohe Bedeutung bei. In der „NATO Cloud Computing Policy“ ist festgelegt, dass dafür innerhalb der Allianz geeignete Cloud-Technologien adaptiert werden sollen.

Grundsätzlich gelten in der NATO besondere Sicherheitsanforderungen – je nach Grad der Einstufung der verarbeiteten Informationen. Der unterste Grad ist „NATO UNCLASSIFIED“, gefolgt vom zweiten Einstufungsgrad „NATO RESTRICTED“. Für die Einstufung „NATO UNCLASSIFIED“ gibt es kein nationales Äquivalent in Deutschland. Informationen dieses Einstufungsgrades sind dennoch grundsätzlich nur zur NATO-internen Verwendung vorgesehen und entsprechend zu schützen. „NATO RESTRICTED“ wird äquivalent zum deutschen „VS-NUR FÜR DEN DIENSTGEBRAUCH“ gehandhabt. Also sind die Sicherheitsanforderungen dafür nochmals deutlich höher als für die erste Stufe.

Das NATO-Gremium „Information Assurance and Cyber Defence Capability Panel“, in dem das BSI direkt die Interessen der Bundesrepublik Deutschland vertritt, hat eine Projektgruppe, ein sogenanntes NATO Writing Team, eingerichtet. Dieses soll Sicherheitsmaßnahmen identifizieren

und zusammenzustellen, deren Erfüllung ein Public-Cloud-Angebot für die Verarbeitung von Informationen der Einstufungen „NATO UNCLASSIFIED“ und „NATO RESTRICTED“ qualifiziert. Das Writing Team setzt sich aus einer Reihe von NATO-Organisationseinheiten sowie aus einigen NATO-Staaten zusammen. Neben Deutschland gehören Frankreich, Großbritannien und Belgien dazu. Das BSI hat die Leitung des Writing Teams übernommen. Als Autor des international anerkannten „Cloud Computing Compliance Criteria Catalogue“ (C5) verfügt es dafür über die exakt passende Expertise.

Im Dezember 2021 reichte das Writing Team die ersten Ergebnisse fristgerecht ein; der vorgelegte Entwurf der Direktive für die Verarbeitung von „NATO-UNCLASSIFIED“-Informationen in Public Clouds wurde dann von den NATO-Nationen angenommen. Auf Grundlage dieser Direktive ist die NATO seitdem in der Lage, Public-Cloud-Angebote systematisch für die Verarbeitung von „NATO-UNCLASSIFIED“-Informationen freizugeben. Durch die Berücksichtigung des C5 und weiterer aktueller Cloud-Standards spiegelt die Direktive den aktuellen State of the Art der Cloud-Sicherheit wider und vereinheitlicht nach innen wie nach außen das Sicherheitsniveau der NATO bei der Nutzung von Public Clouds.

HARMONISIERTE SICHERHEITSNIVEAUS UND THOUGHT LEADERSHIP

Mit der Annahme dieser Cloud-Direktive für „NATO UNCLASSIFIED“ durch die NATO-Mitgliedstaaten ist es dem BSI gelungen, die Inhalte des in Deutschland etablierten C5-Standards erfolgreich in die NATO einzubringen und die Sicherheitsniveaus der beiden Anforderungskataloge zu harmonisieren. Damit nimmt das BSI auch im internationalen Rahmen seine Rolle als Thought Leader wahr und stärkt erfolgreich die Informationssicherheit national wie auch im Bündnis.

Diesem ersten Meilenstein soll ein weiterer folgen: Unter der Leitung des BSI arbeitet das Writing Team momentan an der Erweiterung der bestehenden Direktive, um künftig der NATO auch die Verarbeitung von „NATO RESTRICTED“-Informationen in Public Clouds zu ermöglichen. ■

Weitere Informationen:

Thema Cyber-Abwehr auf www.nato.int:
https://www.nato.int/cps/en/natohq/topics_78170.htm

Kriterienkatalog Cloud Computing C5:
https://www.bsi.bund.de/C5

Update für europäische Cyber-Sicherheit

von Joshua Breuer und Samuel Rothenpieler, Referat Internationale Beziehungen

Am 16. Dezember 2020 veröffentlichte die Europäische Kommission ihren Vorschlag für die NIS-2-Richtlinie (NIS2), mit welcher Mindestanforderungen an erfasste Einrichtungen und Mitgliedstaaten im Bereich Cyber-Sicherheit definiert werden. Seitdem liefen sowohl im Rat der Europäischen Union als auch im Europäischen Parlament intensive Verhandlungen. Am 12. Mai 2022 konnte im dritten politischen Trilog zwischen den Verhandlungsführern aus Kommission, Parlament und Rat eine Einigung erzielt werden. Damit steht in den kommenden Wochen nur noch die offizielle Verabschiedung der Richtlinie aus.

NIS2 soll die NIS-Richtlinie aus dem Jahr 2016 (NIS1) ersetzen, mit der erstmalig ein einheitlicher Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cyber-Sicherheit, eine stärkere Zusammenarbeit der EU-Mitgliedstaaten (MS) sowie Mindestsicherheitsanforderungen und Meldepflichten für Betreiber von Kritischen Infrastrukturen und für bestimmte Anbieter digitaler Dienste geschaffen wurde.

Schon früh deutete sich jedoch an, dass die Kommission im Rahmen des festgeschriebenen Reviews eine weitere Harmonisierung anstreben würde. Vor allem der unterschiedlich gehandhabte Identifizierungsprozess führte in den EU-Mitgliedstaaten zu Divergenzen bei der Anzahl erfasster Einrichtungen und damit auch des Meldeaufkommens. Zudem existierte ein ungleiches Niveau der Sicherheitsanforderungen.

INHALTE DER EINIGUNG

Mit NIS2 gehen folglich umfangreiche Änderungen einher: Der Anwendungsbereich wird qualitativ und quantitativ erweitert. So berücksichtigt die Richtlinie zusätzliche Sektoren, erstmals werden auch Einrichtungen der öffentlichen Verwaltung aufgenommen. Im Regelfall erfolgt die Erfassung der Einrichtungen innerhalb der Sektoren künftig anhand der Unternehmensgröße („size-cap rule“). Die Mitgliedstaaten haben in der nationalen Umsetzung aber gewisse Spielräume.

In der Richtlinie wird zwischen wichtigen und wesentlichen Einrichtungen unterschieden, wobei letztere einer strengeren Aufsicht unterliegen, und die Sicherheitsanforderungen national im Sinne einer Verhältnismäßigkeitseinschätzung abgestuft angewandt werden können. Die verpflichtenden Sicherheitsmaßnahmen werden in einem Katalog festgehalten, der im Vergleich zu NIS1 auch neue Anforderungen umfasst, etwa hinsichtlich Lieferkettensicherheit.

Auch die Meldepflichten wurden angepasst: Die bislang einstufige Meldepflicht bei Vorfällen wird durch ein dreistufiges Melderegime mit festen Fristen ersetzt.

Daneben werden auch neue Themen formell in europäische Kooperationsformate überführt, etwa die koordinierte Offenlegung von Schwachstellen sowie eine europäische Schwachstellendatenbank. Auch für das Cyber-Sicherheitskrisenmanagement gibt es Regelungen in NIS2. Neben den bereits etablierten Gruppen (CSIRTs Netzwerk und Kooperationsgruppe) wird speziell für diesen Bereich das „European cyber crises liaison organisation network (EU-CyCLONe)“ rechtlich verankert.

Quelle: DG CNECT

BSI UND NIS2

NIS2 wird zu einer deutlichen Erweiterung der erfassten Einrichtungen auch in Deutschland führen. Das BSI setzt sich dafür ein, dass dabei national weiterhin auch die BSI-Kritisverordnung berücksichtigt wird. Für das BSI spielt zudem der Bereich der Aufsicht und Durchsetzung eine wichtige Rolle. Hier werden die Befugnisse und Handlungsmöglichkeiten für die national zuständigen Behörden erweitert. Die Beratungs- und Unterstützungserwartungen an das BSI werden sich jedoch ebenfalls massiv erhöhen.

Als Cyber-Sicherheitsbehörde des Bundes hat das BSI im Laufe der Verhandlungen seine Expertise und die Erfahrungen aus NIS1 aktiv eingebracht und im Sinne der Cyber-Sicherheit zu einem positiven Ergebnis beigetragen.

UMSETZUNG & EINORDNUNG IM WEITEREN LEGISLATIVEN KONTEXT

Nach der offiziellen Verabschiedung der neuen Richtlinie folgt eine 21-monatige Umsetzungsfrist in nationales Recht. Bereits jetzt ist absehbar, dass dadurch in Deutschland Änderungen am BSI-Gesetz notwendig werden, da die Anforderungen der Richtlinie deutlich über die Bestimmungen des IT-SiG 2.0 hinausgehen oder sie teilweise ersetzen.

Als sogenannter horizontaler Rechtsakt schafft die NIS2 ein sektorübergreifendes Mindestsicherheitsniveau, allerdings ergeben sich angesichts weiterer sektoraler und horizontaler Rechtsakte deutliche Querbezüge zu anderen Regulierungsbereichen. So wurde parallel die Critical-Entities-Resilience-Richtlinie (CER) verhandelt, die ein überarbeitetes Konzept für die Widerstandsfähigkeit Kritischer Infrastruktur enthält und deren erfasste Einrichtungen automatisch als wesentliche Einrichtungen nach der NIS2 definiert werden sollen.

Auch der Digital Operational Resilience Act (DORA) für die Regulierung des Finanzsektors enthält Bestimmungen zur Identifizierung, Aufsicht und Durchsetzung im Bereich der IT-Sicherheit von Finanzunternehmen, die bei der nationalen Umsetzung der NIS2 ebenfalls berücksichtigt werden müssen. Ein weiterer wichtiger Baustein europäischer Cyber-Sicherheitsgesetzgebung, der aktuell verhandelt wird, adressiert die Cyber-Sicherheit von Einrichtungen der Europäischen Union selbst, die nicht in den Geltungsbereich von NIS2 fallen und bisher keiner einheitlichen Regulierung unterliegen. ■

Weitere Informationen:

Presseartikel zur NIS-2-Richtlinie:
https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985

Presseartikel zur NIS-2-Richtlinie:
https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/

Sicherheit statt Risiko

Wie der Digitale Verbraucherschutz im BSI die Sicherheit von Verbraucherdaten verbessert

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

Das BSI registriert regelmäßig Meldungen zu sogenannten Datenleak-Vorfällen, d. h. dem unbefugten Zugriff und der Offenlegung von Daten, die nicht für Dritte bestimmt sind. Darin zeigt sich die oft unzureichende Umsetzung von angemessenen Anforderungen an die Sicherheit der Informationstechnik.

Daten sind in aller Welt. Von der Verbreitung digitaler, datengetriebener Geschäftsmodelle und der zunehmenden Vernetzung informationstechnischer Systeme profitieren auch Verbraucherinnen und Verbraucher, wenn sie entsprechende digitale Produkte und Dienste nachfragen möchten. Was oft zu kurz kommt: der differenzierte Umgang mit Daten unter Berücksichtigung des Schadenpotenzials im Falle eines Missbrauchs. Für Verbraucherinnen und Verbraucher besteht grundsätzlich ein Risiko, dass ihre bei Online-Diensten hinterlegten persönlichen Daten von Unbefugten entwendet und für zukünftige Angriffe, wie z. B. Phishing oder Smishing, verwendet werden.

Datenleaks stehen häufig in Verbindung mit Ransomware-Angriffen. So gelang Cyber-Kriminellen im Oktober 2021 der Zugriff auf die IT-Infrastruktur eines deutschen Reiseunternehmens. Infolgedessen kam es zu einer Verschlüsselung sensibler Daten durch Ransomware, begleitet durch den Diebstahl und die Veröffentlichung eines Teils dieser Daten. Unter anderem wurden von den Angreifern Reisepassdaten von Kundinnen und Kunden aus Deutschland offengelegt. Das BSI beobachtet zunehmend auch die unfreiwillige Veröffentlichung sensibler Daten aufgrund fehlender adäquater Schutzmaßnahmen mit der Folge, dass sensible (oft personenbezogene) Daten ohne Beteiligung und in vielen Fällen ohne Kenntnis der Betroffenen an die Öffentlichkeit gelangen.

Angriffe auf Kundendatenbanken bei Online-Diensten, wie z. B. im Onlineshopping, liegen meist außerhalb des Einflussbereichs der betroffenen Verbraucherinnen und Verbraucher. Derartige Sicherheitsvorfälle mit darauffolgender Veröffentlichung sensibler persönlicher Daten unterminieren daher in besonderer Weise das Vertrauen in die Nutzung digitaler Dienste sowie in die Digitalisierung insgesamt.

DATENSICHERHEIT VON VERBRAUCHERINNEN UND VERBRAUCHERN STÄRKEN

Der Digitale Verbraucherschutz ist ein gesetzlicher Auftrag des BSI. In diesem Rahmen tritt das BSI gegenüber Herstellern und Anbietern für die Verbraucherbelange und die Sicherstellung der Informationssicherheit von Verbraucherdaten ein. Ein wichtiger Baustein für die Erfüllung dieses Auftrages ist die systematische Beobachtung und Bewertung von IT-Sicherheitsvorfällen mit Verbraucherbetroffenheit. Hierfür hat das BSI eine Detailuntersuchung zu der Sicherheit von Verbraucherdaten in Datenbanken von Onlineshopping-Plattformen in Auftrag gegeben. Ziel der Untersuchung war der Gewinn von Informationen, einerseits in Bezug auf die Sicherheit von Kundendaten zu den auf dem Markt gängigen Onlineshopping-Plattformen sowie andererseits zu den spezifischen Bedürfnissen, Erwartungen, Wahrnehmungen und Verhaltensweisen von Verbraucherinnen und Verbrauchern bei konkreten Datenleak-Vorfällen. Im Rahmen

Andreas Sachs
Bereichsleiter Cybersicherheit und Technischer Datenschutz Vizepräsident Bayerisches Landesamt für Datenschutzaufsicht

„Aus Verbrauchersicht kann man nicht viel mehr machen, es ist ja auch Aufgabe der Onlineshops, eine ausreichende Sicherheit zu gewährleisten."

von Schwachstellenanalysen und Sicherheitstests wurden ausgewählte Software-Lösungen im Onlineshopping (Shop-Software) überprüft. Die dabei entdeckten Schwachstellen behandelt das BSI im Rahmen des üblichen Coordinated-Vulnerability-Prozesses. Darüber hinaus fanden Interviews mit Expertinnen und Experten zum Thema Datensicherheit im Onlineshopping statt. Durch die Befragung ließen sich wichtige Erkenntnisse für wirksame Maßnahmen im Digitalen Verbraucherschutz, speziell im Onlineshopping, beschaffen.

DATENSICHERHEIT ALS GEMEINSCHAFTSAUFGABE

Die bisher vorliegenden Ergebnisse der Studie weisen darauf hin, dass es unerlässlich ist, dass die Hersteller zeitnah Sicherheitsupdates für identifizierte IT-Sicherheitslücken der eingesetzten Shop-Software bereitstellen und dass diese ebenso zeitnah von den Betreiberinnen und Betreibern eines Onlineshops eingespielt werden. Neben Herstellern und Anbietern können auch die Verbraucherinnen und Verbraucher einen gewissen Beitrag zur Erhöhung der Datensicherheit leisten. Hierzu äußerten sich im Rahmen der vorgenannten Studie die befragten Expertinnen und Experten zu Handlungsmöglichkeiten von Verbraucherinnen und Verbrauchern, wie z. B. die Auswahl sicherer und unterschiedlicher Passwörter zum Schutz unterschiedlicher Accounts. Die Notwendigkeit einer sicheren Passwortverwaltung durch die Verbraucherinnen und Verbraucher, aber auch die Verantwortung der Betreiberinnen und Betreiber von Onlineshops betonte Andreas Sachs vom Bayerischen Landesamt für Datenschutzaufsicht. Die kompletten Ergebnisse der Studie werden voraussichtlich Anfang des Jahres 2023 veröffentlicht.

Im Dialog mit Herstellern und Anbietern setzt sich das BSI anlassbezogen und kontinuierlich dafür ein, dass digitale Verbraucherprodukte und -dienste ein Mindestmaß an Informationssicherheit bieten. Auch das nationale IT-Sicherheitskennzeichen des BSI verfolgt das Ziel, das IT-Sicherheitsniveau von verbrauchernahen IT-Produkten und -diensten zu steigern. Hierzu wird das BSI perspektivisch weitere Produktkategorien veröffentlichen. Darüber hinaus steht

Dr. Ayten Öksüz
Referentin Datenschutz und Datensicherheit Gruppe Verbraucherrecht Verbraucherzentrale NRW e.V.

„Passwörter sind auch ein wichtiger Punkt: Wenn man ein und dasselbe Passwort für mehrere Accounts wählt, dann können Angreifer zum Beispiel, wenn sie die E-Mail-Adresse und das Passwort von einem Shop-Account haben, als Erstes schauen, ob sie mit dieser Kombination auch in das E-Mail-Konto der betroffenen Person reinkommen. Bei Erfolg hätten sie Zugriff auf sehr viele sensible Daten. Auf E-Mail-Inhalte, aber auch auf die Kontakt-Listen, um damit dann beispielsweise weitere Phishing-Angriffe zu starten."

die Sensibilisierung von Verbraucherinnern und Verbrauchern im Hinblick auf die Verwendung sicherer Passwörter, den Einsatz eines Passwortmanagers und die Nutzung einer Zwei-Faktor-Authentisierung im Fokus. Dabei hat der Digitale Verbraucherschutz seine drei Kernziele stets im Blick: das Risikobewusstsein der Zielgruppe im digitalen Raum zu schärfen, ihre Beurteilungsfähigkeit zu stärken und ihre Lösungskompetenz zu steigern. ■

Weitere Informationen:

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

Eine Schwachstelle melden:
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen.html

Das IT-Sicherheitskennzeichen des BSI:
www.bsi.bund.de/IT-SiK

Ältere Menschen in den sicheren digitalen Alltag begleiten

Zielgruppenspezifische Sensibilisierung im digitalen Verbraucherschutz

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

**„Damit kenne ich mich nicht so gut aus, da frage ich immer meine Tochter.“ Oder: „Mein Enkel hat mir das eingerichtet, das ist super, jetzt können wir uns per Video am Smartphone sehen.“
Solche und ähnliche Sätze hören die Mitarbeiter und Mitarbeiterinnen des BSI öfter, wenn sie beispielsweise beim Tag der offenen Tür der Bundesregierung im Sommer in Berlin die Angebote des BSI für Verbraucherinnen und Verbraucher vorstellen. Zur Aufgabe des BSI gehört es auch, ältere Menschen bei der sicheren Gestaltung ihres digitalen Alltags zu unterstützen.**

Menschen über 60 nutzen gerne und oft die neuen Möglichkeiten der Kommunikation über mobile Geräte oder Anwendungen im Internet. Viele aus dieser Generation fühlen sich aber im Umgang mit Geräten und Anwendungen nicht immer sicher.

Einmal pro Jahr befragen BSI und die Polizeiliche Kriminalprävention der Länder und des Bundes im Digitalbarometer Bürgerinnen und Bürger in einer repräsentativen Online-Befragung nach ihren Kenntnissen und Erfahrungen zum Thema Cyber-Sicherheit und -Kriminalität. Aus dem aktuellen Digitalbarometer 2022 geht hervor, an wen sich ältere Menschen mit ihren Fragen hierzu wenden: 44 Prozent geben an, Informationen von Familie, Freunden und Bekannten zu erhalten. Etwa genauso viele (48 %) recherchieren im Internet zu ihren Fragen. Gleichzeitig zeichnet sich ein höheres Sicherheitsbewusstsein dieser Altersgruppe ab, die im Vergleich zu jüngeren Menschen mehr Schutzmaßnahmen umsetzt. Beispielsweise aktivieren sie häufiger automatische Updates für ihr Smartphone.

LEBENSWELT IN DEN BLICK NEHMEN

Solche Erkenntnisse werfen unter anderem die Frage auf, wie das Informations- und Beratungsangebot des BSI, das sich explizit an Privatanwenderinnen und -anwender richtet, gestaltet sein sollte, um noch mehr Menschen mit dem digitalen Verbraucherschutz zu erreichen. Es gehört zu den Zielen des BSI, die Sensibilität der Verbraucherinnen und Verbraucher für Informationssicherheit zu erhöhen.
Wenn eine einzelne Zielgruppe wie Menschen über 60 angesprochen werden soll, bietet sich dafür die Zusammenarbeit mit Organisationen oder bestehenden Projekten an, die bereits mit der Zielgruppe vernetzt sind und ihre Lebenswelten und Bedürfnisse kennen. So lässt sich in einem kooperativen Ansatz das Risikobewusstsein erhöhen.

Weitere Informationen:

**Digitalbarometer 2022:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2022.html**

MITTAGSPAUSE MIT DEM BSI

Vor diesem Hintergrund hat das BSI 2022 die Zusammenarbeit mit dem Digital-Kompass ausgebaut, einer Initiative, die von der „BAGSO – Bundesarbeitsgemeinschaft der Seniorenorganisationen“ und „Deutschland sicher im Netz“ in Partnerschaft mit der Verbraucher-Initiative mit Förderung des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz getragen wird. Der Digital-Kompass ist ein Treffpunkt für Fragen zum Internet und stellt unter anderem auch kostenfreie Angebote für Seniorinnen und Senioren bereit – sowohl vor Ort an rund 100 Standorten in Deutschland als auch online.

Teil des Digital-Kompasses sind sogenannte Internetlotsen, die ältere Menschen beim Ausprobieren und Durchklicken begleiten. Genau diese Internetlotsen sind die Zielgruppe der Online-Veranstaltungsreihe „Mittagspause mit dem BSI“, die im Frühjahr und im Herbst 2022 jeweils mit drei Folgen stattfand. Neben aktuellen Vorfällen zu einem bestimmten Themengebiet stellten Mitarbeiterinnen und Mitarbeiter des BSI Empfehlungen zu diesem Thema vor und gaben Hinweise, was unter dem Aspekt der IT-Sicherheit speziell zu beachten ist. Die Themen reichten dabei von sicheren Einstellungen des heimischen Routers über Backups für die Datensicherung und Maßnahmen zum Accountschutz bis hin zu Tipps für sicheres Onlineshopping zu Weihnachten. Auf Basis dieses Wissens können die Internetlotsen künftig als Multiplikatoren die Empfehlungen des BSI weitergeben.

WEITERE KOOPERATIONEN

Neben der bereits seit 2019 in unterschiedlichen Formen bestehenden Zusammenarbeit mit dem Digital-Kompass steht das BSI im ständigen Austausch mit der BAGSO. Die Organisation hat beispielsweise für die Überarbeitung der „Wegweiser für den digitalen Alltag“ des BSI ältere Testleser vermittelt, die wichtige Rückmeldungen zur Verständlichkeit der Texte gaben. Zudem beteiligte sich das BSI im vergangenen Jahr am Deutschen Seniorentag der BAGSO, der coronabedingt als digitales Format stattfinden musste.

Diese und andere Maßnahmen tragen dazu bei, das BSI als Ratgeber für mehr Sicherheit im digitalen Alltag älterer Menschen zu verankern und die Rolle der Cyber-Sicherheitsbehörde des Bundes genau hier zu stärken. Und dies nicht nur in Form von Wissen, das ältere Menschen sich aneignen, sondern ganz praktisch, wenn sie etwa während eines Workshops direkt die Einstellungen an ihrem Router ändern – und damit nicht auf den nächsten Besuch der Tochter oder des Enkels warten müssen. ■

Wegweiser für den digitalen Alltag:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Broschueren/broschueren_node.html

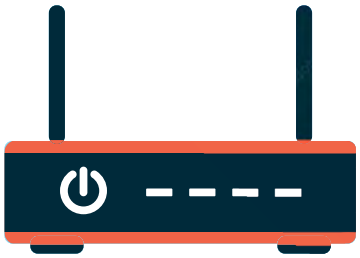
Digitalkompass:
www.digital-kompass.de

BSI-Basis-Tipp

Neun Tipps für ein sicheres Heimnetzwerk

Solider Schutz für den Router – das Herzstück der digitalen Vernetzung zu Hause

Der Router ist das Herzstück der digitalen Vernetzung zu Hause. Er bildet den Knotenpunkt für die Kommunikation aller netzwerkfähigen Geräte – Computer, mobile Geräte, Smart-TVs und intelligente Haustechnik – sowohl mit dem Internet als auch untereinander. Als zentrale Schnittstelle zwischen dem Internet und dem Heimnetzwerk ist es enorm wichtig, den Router gegen unberechtigte Zugriffe und Angriffsversuche von außen zu schützen.



Im ungesicherten Zustand sind Router ein Einfallstor für Cyber-Angriffe. Wenn es Angreifenden gelingt, von außen in den Router einzudringen, können sie das Gerät selbst, aber auch alle angeschlossenen Geräte kompromittieren und den Nutzenden persönlichen oder finanziellen Schaden zufügen:

Datendiebstahl: Angreifende können private Daten, Passwörter oder E-Mails ausspähen. Dabei können sie auch Zugangsdaten fürs Onlineshopping oder Kreditkartendaten stehlen.

Telefonleitung missbrauchen: Angreifende können aus dem Netzwerk heraus kostenpflichtige Rufnummern wählen oder teure Auslandsgespräche auf Kosten des Anschlussinhabenden führen.

Webaktivitäten ausspionieren: Weil der Router den gesamten Internetverkehr im Netzwerk abwickelt und dokumentiert, können Angreifende nicht nur Daten, sondern auch Infos über besuchte Webseiten und genutzte Dienste ausspionieren – und das von allen Geräten im Netzwerk.

Internetzugang missbrauchen: Hackerinnen und Hacker können fremde Netzwerke für das Abrufen oder Teilen illegaler Inhalte oder für Angriffe auf andere Internetnutzer missbrauchen. Dafür wird der Router in ein Botnetz eingebunden und zum Beispiel für Distributed-Denial-of-Service(DDoS)-Angriffe oder zum Versenden von Spam genutzt.

Schadsoftware installieren: Router-Hacking ist oft der erste Schritt für weitergehende Angriffe. Nach dem Hacken des Routers können Angreifende Schadsoftware installieren und damit weitere Cyber-Angriffe vorbereiten.

Geräte im Netzwerk angreifen: Ein gehackter Router kann der Ausgangspunkt weiterer Angriffe auf Geräte im Netzwerk sein. Damit ist jedes mit dem Router verbundene Geräte gefährdet.

Firmware austauschen: Angreifende können die auf dem Router installierte Firmware austauschen oder mit Malware infizieren. Danach funktioniert der Router nicht mehr so, wie er soll, kann von außen gesteuert werden und ist offen für künftige Angriffe oder Spionage-Aktivitäten.

SO SCHÜTZEN SIE IHREN ROUTER

Wer sein Heimnetzwerk und alle damit verbundenen internetfähigen Geräte schützen möchte, muss vor allem seinen Router sicher einrichten und gut absichern. Mit den folgenden neun Basis-Tipps legen Sie den Grundstein für den sicheren Betrieb Ihres (W)LANs.

1. **Ändern Sie das Standardpasswort für die Weboberfläche des Routers:** Die Anwendung zur Verwaltung des Routers, oft eine sogenannte Webapp im Browser, ist durch ein Passwort geschützt. Inzwischen ist bei bestimmten Routermodellen werksseitig ein individuelles Passwort voreingestellt. Sie erkennen das zum Beispiel daran, dass dieses Passwort im Benutzerhandbuch als „individuell" gekennzeichnet ist. Allerdings gibt es immer noch Router, die mit Standardpasswörtern wie „admin" oder „1234" ausgeliefert werden. Solche Zugangscodes sollten Sie sofort ändern, denn auch Angreifende kennen (und nutzen!) diese Standardpasswörter. Das BSI empfiehlt Passwörter mit mindestens acht Zeichen und aus verschiedenen Zeichenarten wie Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.

2. **Ersetzen Sie den Standard-Netzwerknamen:** Manche Router tragen im Namen des WLAN ausführliche Informationen zu Hersteller oder Modell des Geräts. Diese Angaben können potenziellen Angreifenden nützlich sein und sollten geändert werden.

3. **Langes und komplexes WLAN-Passwort:** Das WLAN-Passwort ist nicht identisch mit dem Router-Passwort. Es dient speziell dem drahtlosen Zugang in das lokale Funknetz. In der Regel haben die Router werksseitig bereits ein sicheres WLAN-Passwort eingestellt, das aus 20 Zeichen besteht. Sollte dies bei Ihrem Router nicht der Fall sein, vergeben Sie ein Passwort, das aus mehr als 20 zusammenhanglosen Zeichen aus den vier oben genannten Zeichenarten besteht.

4. **Halten Sie die Firmware auf dem aktuellen Stand:** Softwareupdates sind wichtig, weil sie bekannte Sicherheitslücken schließen. Aktivieren Sie, wenn möglich, die automatische Installation von Softwareupdates, denn damit erhalten Sie ein hohes Maß an Komfort und Sicherheit. Falls es diese Option nicht gibt, schauen Sie regelmäßig selbst nach Updates.

5. **Deaktivieren Sie die Firewall nicht:** Viele Router verfügen über eine standardmäßig aktive Firewall, die Verbindungen von außen nach innen kontrolliert oder deaktiviert. Diese Firewall sollten Sie auf keinen Fall deaktivieren.

6. **Nutzen Sie eine sichere WLAN-Verschlüsselung:** Die Standards WPA2 und WPA3 haben sich bisher als sicher erwiesen. Falls Ihr Router diese beiden Standards (noch) nicht unterstützt, sollten Sie auf ein neues Modell umsteigen.

7. **Deaktivieren Sie nicht benötigte Dienste und den Fernzugriff:** Moderne Router bieten außer dem Zugang zum Internet viele zusätzliche Funktionen, zum Beispiel die Nutzung als Mediaplayer. Diese zusätzlichen Funktionen können allerdings auch ein Einfallstor für Angreifende sein. Deaktivieren Sie diese Funktionen daher, wenn Sie sie nicht benötigen, um die Angriffsfläche zu minimieren.

8. **Richten Sie ein Gast-Netzwerk ein:** Für unsichere Geräte oder für die Geräte Ihrer Gäste sollten Sie, wenn möglich, ein Gast-Netzwerk einrichten. Damit trennen Sie diese Zugänge von sensiblen Diensten wie Onlinebanking oder Home-Office-Anwendungen.

9. **Beachten Sie die IT-Sicherheitskennzeichen:** Router-Anbieter können für ihre Produkte das IT-Sicherheitskennzeichen des BSI erhalten. Voraussetzung dafür: Sie sichern zu, dass ihre Produkte bestimmte Sicherheitseigenschaften besitzen. Falls Sie die Anschaffung eines neuen Routers planen, nutzen Sie dieses Kennzeichen (Infos dazu unten) als Kaufkriterium.

Weitere Informationen:

Transparente Sicherheit durch das IT-Sicherheitskennzeichen:
www.bsi.bund.de/it-sik/verbraucher

WLAN – was man wissen sollte:
www.bsi.bund.de/dok/131126

Sicherheitstipps im privaten und öffentlichen WLAN
www.bsi.bund.de/dok/131138

Sichere Passwörter erstellen:
https://www.bsi.bund.de/dok/131366

Faktenblatt „Sichere Passwörter“:
https://www.bsi.bund.de/dok/409620

DAS IT-SICHERHEITSKENNZEICHEN FÜR ROUTER

Mit dem IT-Sicherheitsgesetz 2.0 hat das BSI vom Gesetzgeber den Auftrag erhalten, ein freiwilliges IT-Sicherheitskennzeichen (IT-SiK) einzuführen, das auch für Router vergeben wird. Das IT-Sicherheitskennzeichen schafft Transparenz für Verbraucherinnen und Verbraucher, indem es die grundlegenden Sicherheitseigenschaften von IT-Produkten auf einen Blick erkennbar macht. Mit dem IT-SiK erhalten Nutzende die Möglichkeit, sich über von Herstellern zugesicherte Sicherheitsfunktionalitäten zu informieren.

Bestellen Sie Ihr BSI-Magazin!

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Referat Öffentlichkeitsarbeit

Postfach 20 03 63
53133 Bonn
Telefon: +49 (0) 228 99 9582 0
Telefax: 0228 99 9582-5455
E-Mail: bsi-magazin@bsi.bund.de

Zweimal im Jahr gibt das BSI-Magazin „Mit Sicherheit“ Einblick in nationale und internationale Cyber-Sicherheitsthemen, die digitale Gesellschaft sowie IT-Sicherheit in der Praxis.

Lassen Sie sich jetzt direkt nach Erscheinen im Juni und im Dezember die aktuellste Ausgabe bequem per Post zusenden, indem Sie sich mit unten stehendem Formular für den Abo-Verteiler anmelden.

Ich möchte die folgende BSI-Publikation im Abo erhalten:

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

Name, Vorname

Organisation

Straße, Hausnr.

PLZ, Ort

E-Mail

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

Datum/Unterschrift:

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

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

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

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

Impressum

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI) 53175 Bonn
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik Referat WG24 – Öffentlichkeitsarbeit Godesberger Allee 185–189 53175 Bonn Telefon: +49 (0) 228 999582-0 E-Mail: bsi-magazin@bsi.bund.de Internet: www.bsi.bund.de
Stand:	Dezember 2022
Redaktion:	Katrin Alberts, Sonia Golás, Mark Schulz, Bundesamt für Sicherheit in der Informationstechnik; FAKTOR 3 AG, Kattunbleiche 35, 22041 Hamburg, www.faktor3.de
Konzept und Gestaltung:	Bundesamt für Sicherheit in der Informationstechnik
Druck:	Appel und Klinger Druck & Medien GmbH Bahnhofstraße 3 96277 Schneckenlohe www.ak-druck-medien.de
Artikelnummer:	BSI-Mag22/716-1
Bildnachweise:	Titel: AdobeStock © sasun Bughdaryan; S. 03: BSI; S. 04 – 05 (von links nach rechts): BSI, AdobeStock © sasun Bughdaryan, BSI, AdobeStock © metamorworks, AdobeStock © jozefmicic, AdobeStock © insta_photos; S. 06 – 07: BSI, BSI, BSI, AdobeStock © BAIVECTOR; S. 8 – 9: AdobeStock © Open Studio; S. 10 – 11 AdobeStock © Meawstory 15Studio; S. 12 – 13: Schloß Elmau, BSI; S. 14: BSI; S. 15 (oben): Bundesregierung/Güngör, S. 15 (unten): BSI; S. 16 – 17: BSI; Seite 18 – 19: AdobeStock © sasun Bughdaryan; S. 20: AdobeStock © sasun Bughdaryan; S. 22 – 23: AdobeStock © whyt; S. 24: AdobeStock © sasun Bughdaryan; S. 27: AdobeStock © samuii, AdobeStock © sasun Bughdaryan; S. 18 – 27 (Hintergrundgrafiken): AdobeStock © lil und AdobeStock © Peter Kögler; S. 28 – 29: BSI; S. 30 – 31: Koivo c/o kombinatrotweiss.de; S. 32 – 33: BSI; S. 34: BSI; S. 36 – 37: BSI; S. 38: BSI; S. 39: AdobeStock © Parradee; S. 41 (links): Matthias Rietschel, S. 41 (rechts): Annett Weigelt; S. 42: AdobeStock © 4zevar und AdobeStock © Daniel Berkmann; S. 43: BSI; S. 45: AdobeStock © metamorworks; S. 46 – 47 (Illustration): AdobeStock © jozefmicic, S. 47 (Foto): Thomas Caspers; S. 48 – 49: AdobeStock © rawku5; S. 50: AdobeStock © New Africa; S. 51 (links): Privat, S. 51 (rechts): © Verbraucherzentrale NRW; S. 52: BSI; S. 53: AdobeStock © insta_photos; S. 54: AdobeStock © pixelalex; S. 55 – 56: AdobeStock © Matthias Enter

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

Es wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

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

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

Follow us:

www.bsi.bund.de