Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Bericht zum Digitalen Verbraucherschutz 2022

2022 im Überblick

Februar

18. IT-Sicherheitskongress 2022

Diskussionsrunde rund um aktuelle Heraus-forderungen des Digitalen Verbraucherschutzes mit Exper-tinnen und Experten aus Wissen-schaft, der Wirtschaft, Zivilgesell-schaft und des BSI.

März

Tech4Germany

Auswahl des eingereichten Projekts "Sicherheit im digitalen Alltag" (Online-Plattform) beim Fellowship-Programm des Bundes Tech4Germany.

Juni

Bericht zum Digitalen Verbraucherschutz 2021

Veröffentlichung des 2. Berichts zum Digitalen Verbraucherschutz mit dem Schwerpunktthema „Digitaler Verbraucherschutz im Automobilbereich“.

August

Beirat Digitaler Verbraucherschutz

Veröffentlichung der ersten Handlungs-empfehlungen des Beirates: "Kommunikation über Sicherheit bei Passwörtern".

Messe: Gamescom 2022

Messebeteiligung mit zielgruppengerechten Medien-Kooperationen sowie Formaten rund um IT-Sicherheitsthemen, z. B. Accountschutz und Deepfakes.

September

Dialog für Cybersicherheit

Durchführung der Denkwerkstatt 2022 in Leipzig: Dialogplattform rund um Themen gesamtgesellschaftlicher Cyber-Sicherheit.

November

Veranstaltung: BSI im Dialog

Vortrag zur Verknüpfung der Anforderungen des Digitalen Verbraucherschutzes mit dem „Cyber Resilience Act“ (Gesetzesinitiative auf EU-Ebene).

Oktober

Tech4Germany

Abschlussevent in Berlin: Vorstellung des erarbeiteten Prototyps eines Online-IT-Sicherheitsatlas als Orientierungshilfe, die Akteure im Digitalen Verbraucherschutz und deren Unterstützungsangebote aufzeigen soll.

Fachmesse/Kongress: it-sa

Messebeteiligung mit Vorträgen und Networking rund um Verbraucherschutzthemen im Kontext der Informationssicherheit in der digitalen Gesellschaft.

Dezember

Zentrales Service-Center des BSI

Insourcing:
Start des Dienstbetriebs.

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn

E-Mail
bsi@bsi.bund.de

Telefon
+49 (0) 22899 9582-0

Telefax
+49 (0) 22899 9582-5400

Stand
Februar 2023

Druck
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Gestaltung
Faktor 3 AG

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bildnachweis
Titel: AdobeStock ©NDABCREATIVITY; S. 2-3, 7, 12, 13, 14, 16, 29: BSI; S. 8, 33: AdobeStock ©Halfpoint; S. 9 (oben): AdobeStock ©peshkova; S. 9 (unten): AdobeStock ©patrick; S. 10: AdobeStock ©Bojan; S. 17: AdobeStock ©Evrymmnt; S. 18: AdobeStock ©bnenin; S. 19: AdobeStock ©kite_rin; S. 20: AdobeStock ©chaylek; S. 21: AdobeStock ©rh2010; S. 23, 34: AdobeStock ©pikselstock; S. 25: AdobeStock ©tippapatt; S. 26: AdobeStock ©akhenatonimages; S. 27: AdobeStock ©Rido; S. 28: AdobeStock ©Seventyfour; S. 30 (oben): BSI; S. 30 (unten) AdobeStock ©denis_vermenko; S. 31 (2 Bilder oben): BSI; S. 31 (unten): AdobeStock ©StratfordProductions; S. 32: AdobeStock ©REDPIXEL.

Grafiken
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Artikelnummer
BSI-DVS23/001

Inhaltsverzeichnis

Vorwort

Verbraucherinnen und Verbraucher sind einer Vielzahl von IT-Sicherheitsrisiken in der digital vernetzten Welt ausgesetzt. Einige dieser Gefahren lauern außerhalb des eigenen Tun und Handelns: So zum Beispiel beim Diebstahl personengebundener Informationen bzw. Daten, die in Organisationen oder Unternehmen gespeichert sind. Andere Mechanismen zielen direkt auf die „Schwachstelle Mensch" im Alltag ab, was besonders für Phishing gilt. Ob über gefälschte E-Mails, Webseiten oder Kurz- bzw. Messengernachrichten – diese Methode kann schon als Evergreen krimineller Methoden bezeichnet werden, die über die Jahre hinweg jedoch nicht weniger effektiv geworden ist.

Die technologischen Möglichkeiten und Varianten von Phishing haben sich stetig weiterentwickelt. Verknüpft mit psychologischen Komponenten wie der Hilfsbereitschaft, spielen sie mit dem Vertrauen oder der Angst potenzieller Opfer. Oft werden Themen ausgenutzt, die wie im Berichtsjahr 2022 mit den Auswirkungen des russischen Angriffskriegs auf die Ukraine, der Inflation und drohender Energieknappheit von großer gesellschaftlichen Bedeutung sind und somit einer breiten öffentlichen Debatte unterliegen. Phishing war, ist und bleibt zukünftig ein hoch relevantes Cyber-Sicherheitsthema, dem wir im Folgenden einen inhaltlichen Schwerpunkt widmen. Damit möchten wir auch alle Akteure im Digitalen Verbraucherschutz ermutigen, noch stärker in die Sensibilisierungs- und Aufklärungsarbeit der Verbraucherinnen und Verbraucher zu investieren. Als Cyber-Sicherheitsbehörde des Bundes leisten wir hierfür unseren Beitrag.

Dies gilt für all unsere Anstrengungen, die neben den Verbrauchergruppen selbst zudem die Anbieter und Hersteller von vernetzten Produkten und digitalen Services, wie auch öffentliche und zivilgesellschaftliche Akteure beinhaltet.

Unser Ziel: Als unabhängige Stelle die Verbraucherinnen und Verbraucher in der Digitalisierung zu schützen. Dafür...

- schafft das BSI die technischen Grundlagen und Rahmenbedingungen für Anbieter und Hersteller, um sichere und vertrauenswürdige Produkte und Dienste zu gestalten.
- informiert, berät und warnt das BSI die Verbraucherinnen und Verbraucher, damit sie digitale Produkte und Dienste sicher nutzen können.
- unterstützt das BSI die Verbraucherinnen und Verbraucher bei der Steigerung ihrer Resilienz, damit sie IT-Sicherheitsvorfälle bewältigen können.

Unser Ziel ist zugleich Anspruch, mit der anerkannten Expertise des gesamten BSI und seiner Partner zur Erhöhung des IT-Sicherheitsniveaus für die Verbraucherinnen und Verbraucher nachhaltig beizutragen.

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

1 Digitaler Verbraucherschutz als Gemeinschaftsaufgabe

Digitalen Verbraucherschutz als Gemeinschaftsaufgabe voranzutreiben und diesen in der Gesellschaft, der Wirtschaft und im staatlich-öffentlichen Bereich gleichermaßen zu verankern ist kein Sprint, sondern ein Marathonlauf. So gibt der vorliegende Bericht zum Digitalen Verbraucherschutz für den Berichtszeitraum 2022 unter anderem einen aktuellen Einblick in die kontinuierliche Arbeit, der das BSI zusammen mit Partnern und Stakeholdern nachgeht, um das Schutzniveau für die Verbraucherinnen und Verbraucher in Deutschland stetig zu verbessern. Dazu zählen Aktivitäten rund um das IT-Sicherheitskennzeichen, die Etablierung des Cyber-Sicherheitsnetzwerkes mit seiner digitalen Rettungskette, die organisatorische Neuausrichtung unseres Zentralen Service Centers und vieles mehr. Dabei gilt es, Wissen und Know-how über die Verbesserung der Informationssicherheit zielgruppengerecht auf breiter Basis zu kommunizieren und zugleich aktiv Themen und Probleme der Verbraucherinnen und Verbraucher aufzunehmen, um diese fachgerecht anzugehen und bestenfalls zu lösen. Die Schwerpunkte an Sicherheitsvorfällen auf dem digitalen Verbrauchermarkt für das Jahr 2022 zeigen die hohe Relevanz sowie den Handlungsbedarf auf.

Der diesjährige thematische Fokus: Im vergangenen Berichtsjahr haben wir auf das Thema *Phishing* sowie die Abwandlungsformen *Smishing* und *Vishing* aufmerksam gemacht. Die dynamisch steigenden Zahlen der (bekannten) Vorfälle zeigen jedoch, dass sich die Bedrohungslage weiter zugespitzt hat. Neben einem Gesamtüberblick über den gewählten Schwerpunkt widmen wir uns in diesem Kontext insbesondere dem Bankensektor, in dem Cyber-Kriminellen besonders häufig das Vertrauen von Verbraucherinnen und Verbrauchern mit Hilfe von Phishing-Methoden ausnutzen. Aktuelle Daten aus dem Phishing-Radar der Verbraucherzentrale Nordrhein-Westfalen, die gemeinsam mit dem BSI analysiert wurden, sowie ein Gastbeitrag des Bundesverbands deutscher Banken e.V. zur Umsetzung von Phishing-Prävention und Verbraucherschutz in der Praxis zeigen die besonderen Herausforderungen sowie mögliche Präventionsansätze in diesem Gefahrenfeld auf.

Branchenspezfische Lage im Bereich Automotive weiter fortgeschrieben

Im Themenfeld Automotive, das im Berichtsjahr 2021 der thematische Schwerpunkt des Berichts war, konnten für 2022 neue Entwicklungen verzeichnet werden. Die Publikation „Branchenlagebild Automotive“ beleuchtet die Risiken der Cyber-Sicherheit in diesem Industriezweig und gibt unter anderem Einblicke in die Themenfelder Security by Design, Cyber Security in der Produktentwicklung sowie die Verletzbarkeit von vernetzen Fahrzeugen und Ladesystemen.

2 Verbraucherinnen und Verbraucher im Blickpunkt

2.1 Ein Jahr IT-Sicherheitskennzeichen: Was wurde erreicht?

Informierte Kaufentscheidung mit dem IT-Sicherheitskennzeichen

Digitale Verbraucherprodukte sind ein beliebtes Ziel von Cyber-Kriminellen. Diese nutzen gezielt bestehende IT-Schwachstellen aus, um an sensible, persönliche Daten der Nutzerinnen und Nutzer zu gelangen oder Cyber-Angriffe auf Infrastrukturen Dritter, beispielsweise über Botnetzwerke, durchzuführen. Verbraucherinnen und Verbraucher sollten daher den Sicherheitseigenschaften von IT-Geräten und -Diensten bei der Kaufentscheidung eine zentrale Bedeutung beimessen.

Mit der Einführung des IT-Sicherheitskennzeichens im Dezember 2021 hat das BSI ein Instrument geschaffen, das Käuferinnen und Käufern ermöglicht, wesentliche IT-Sicherheitseigenschaften von digitalen Produkten schnell zu erfassen und auf dieser Basis eine fundierte Kaufentscheidung zu treffen. Das BSI kam mit der Implementierung des freiwilligen Kennzeichens einem Auftrag aus dem IT-Sicherheitsgesetz 2.0 vom Mai 2021 erfolgreich nach. Hersteller können mit dem IT-Sicherheitskennzeichen ihre Produkte besonders auszeichnen und gleichzeitig dem wachsenden Informationsbedürfnis von Verbraucherinnen und Verbrauchern nachkommen (vgl. BMI 2020).

Durch den zügigen Aufbau entsprechender Verwaltungsstrukturen und als Ergebnis eines effizient gestalteten Antragsverfahrens konnten bereits im Februar 2022 die ersten IT-Sicherheitskennzeichen erteilt und im Rahmen des 18. Deutschen IT-Sicherheitskongresses übergeben werden. Seither arbeitet das BSI fortwährend daran, das IT-Sicherheitskennzeichen weiterzuentwickeln, am Verbrauchermarkt zu etablieren und seinen Einsatz als zentrales Element des digitalen Verbraucherschutzes zu verstetigen. Bis zum Jahresende 2022 konnten bereits 37 IT-Sicherheitskennzeichen an verschiedene Hersteller und Dienstanbieter vergeben werden.

Wie funktioniert das IT-Sicherheitskennzeichen?

1. Antragsverfahren

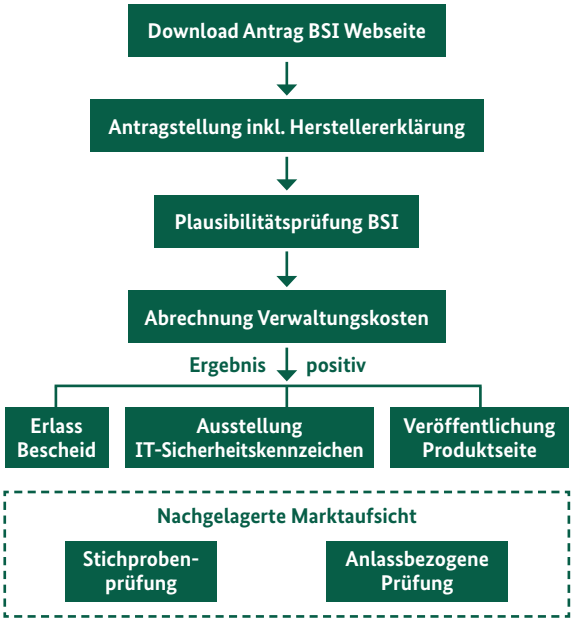
Möchten Hersteller ihre Produkte mit dem IT-Sicherheitskennzeichen auszeichnen, müssen sie zunächst die Konformität ihres Produkts mit den vom BSI festgelegten Sicherheitsanforderungen selbst prüfen oder durch Dritte überprüfen lassen. Erst nach positiver Konformitätsprüfung kann eine Beantragung des IT-Sicherheitskennzeichens erfolgen. Im Rahmen des Antragsverfahrens prüft das BSI die Angaben des Herstellers zur Konformitätsprüfung und dessen eingereichte Unterlagen auf Plausibilität. Dabei wird insbesondere geprüft, ob die vom Hersteller gemachten Angaben nachvollziehbar und widerspruchsfrei sind. Zudem können bereits bekannte Probleme mit dem Produkt (zum Beispiel Sicherheitslücken) oder vorheriges Fehlverhalten der Hersteller (zum Beispiel BSI-Warnungen vor Produkten) in die Entscheidung einbezogen werden. Hierbei wird neben Informationen des BSI-Lagezentrums und des CERT-Bund insbesondere auch auf Erkenntnisse aus der BSI-internen Marktbeobachtung zurückgegriffen. Im Rahmen der Marktbeobachtung untersucht das BSI einzelne Segmente des digitalen Verbrauchermarktes und wird dadurch in die Lage versetzt, aktuelle Marktentwicklungen zu identifizieren und Prognosen in Hinblick auf zukünftige Trends, Entwicklungen und Auswirkungen auf den digitalen Verbrauchermarkt zu treffen. Die Ergebnisse der Marktbeobachtung finden nicht nur im Rahmen der Plausibilitätsprüfung Berücksichtigung, sondern können auch Anstoß für die Entwicklung neuer Produktkategorien des IT-Sicherheitskennzeichens sein.

2. Marktaufsicht

Mit der Freigabe zur Verwendung des IT-Sicherheitskennzeichens unterliegen gekennzeichnete Produkte und Dienste der Aufsicht durch das BSI. Die Marktaufsicht kann prüfen, ob die Einhaltung der vom Hersteller zugesicherten Konformität über die gesamte Laufzeit des IT-Sicherheitskennzeichens gewährleistet ist.

Im Rahmen der Aufsicht können Antragsunterlagen, technische Unterlagen und Herstellerdokumente herangezogen oder technische Überprüfungen veranlasst werden. Dabei kann sowohl die Konformität zur Herstellererklärung als auch die Einhaltung der mit dem IT-Sicherheitskennzeichen

Abbildung 1:
IT-Sicherheitskennzeichen: Antragsverfahren und Marktaufsicht



einhergehenden Pflichten der Hersteller geprüft werden. Zu den letzteren zählt beispielsweise die ordnungsgemäße Benutzung des Etiketts oder die Einhaltung von Informationspflichten bei auftretenden Schwachstellen.

Die Aufsicht kann anlassbezogen sowie anlasslos erfolgen. Anlass zur Prüfung können unter anderem bekanntgewordene Schwachstellen zu dem betreffenden Produkt beziehungsweise im Produkt verwendeten Technologien sowie entsprechende Hinweise oder Informationen von Dritten sein. Unabhängig davon sind stichprobenartige Prüfungen ohne konkreten Anlass möglich, um die Selbsterklärung der Hersteller zu überprüfen.

Werden bei einem Produkt Abweichungen von der Herstellererklärung festgestellt, kann das BSI geeignete Maßnahmen zum Schutz des Vertrauens der Verbraucherinnen und Verbraucher in das IT-Sicherheitskennzeichen ergreifen. Beispielsweise von der Bereitstellung entsprechender Informationen an die Verbraucherinnen und Verbraucher über die dynamische Sicherheitsinformation bis hin zum Widerruf des IT-Sicherheitskennzeichens.

3. Mehrwert für Verbraucherinnen und Verbraucher

Gekennzeichnete Produkte heben sich am Markt besonders hervor und bieten gegenüber ihren Marktbegleitern konkrete Mehrwerte für Verbraucherinnen und Verbraucher. Diese können auf einen Blick erkennen, dass der Hersteller die Selbstverpflichtung eingegangen ist, die vom BSI festgelegten oder anerkannte IT-Sicherheitsanforderungen über die gesamte Laufzeit des Kennzeichens einzuhalten. Das Etikett des IT-Sicherheitskennzeichens enthält einen Link sowie einen QR-Code. Darüber können Verbraucherinnen und Verbraucher eine individuelle Informationsseite zum Produkt aufrufen. Neben dem genauen Inhalt der Herstellererklärung können dort auch verbraucherfreundlich aufbereitete Informationen über die zugesicherten IT-Sicherheitseigenschaften des Produkts abgerufen werden. Verbraucherinnen und Verbraucher finden dort zudem aktuelle Sicherheitsinformationen zum Produkt, wie dem BSI bekanntgewordene Schwachstellen und damit zusammenhängende Sicherheitsupdates. Darüber hinaus erhalten die Verbraucherinnen und Verbraucher weiterführende Beschreibungen und Verweise auf die zugrundeliegenden Sicherheitsanforderungen des BSI.

Ausbau von Produktkategorien

Die Erteilung von IT-Sicherheitskennzeichen ist nur innerhalb von Produktkategorien möglich, die das BSI veröffentlicht hat. Mit den Produktkategorien „Breitbandrouter“ und „E-Mail-Dienste“ wurde das Kennzeichnungssystem in zwei Produktgruppen eingeführt, die für die tägliche IT-Nutzung von Verbraucherinnen und Verbrauchern von zentraler Bedeutung sind.

Nachdem ab Mai 2022 smarte Geräte wie Kameras, Lautsprecher, Reinigungs- und Gartenroboter, Spielzeuge und Fernsehprodukte für die Beantragung des IT-Sicherheitskennzeichen geöffnet wurden, erfolgte eine Überführung dieser Produkte unter der Bezeichnung „Smarte Verbraucherprodukte“ ab September 2022 in eine neue und umfassendere Produktkategorie im Bereich IoT- und Smart-Home. Diese neue Produktkategorie stützt sich im Wesentlichen auf den etablierten europäischen Sicherheitsstandard ETSI EN 303 645. Der Standard wurde im Rahmen der europäischen Standardisierungsarbeit durch Expertinnen und Experten des BSI mitentwickelt sowie in einem Pilotprojekt auf praktische Anwendbarkeit geprüft. Er adressiert IoT-Geräte, die ein Risiko für die Informationssicherheit und Privatsphäre von Nutzerinnen und Nutzern darstellen können. Um möglichen Bedrohungen zu begegnen, beinhaltet der Standard wichtige Sicherheitsanforderungen, wie

Abbildung 2:
Elemente des IT-Sicherheitskennzeichens

zum Beispiel sichere Authentisierungsmechanismen, ein angemessenes Updatemanagement und die Absicherung der Kommunikation.

Das BSI arbeitet auch weiterhin intensiv an der Entwicklung neuer Produktkategorien. Ziel ist es, eine schnellstmögliche und weitreichende Implementierung des IT-Sicherheitskennzeichens im Verbrauchermarkt zu erreichen und Verbraucherinnen und Verbrauchern eine informierte Kauf- und Nutzungsentscheidung in möglichst vielen Bereichen des digitalen Alltags zu ermöglichen. Zudem soll den Unternehmen die Möglichkeit gegeben werden, die IT-Sicherheit ihrer Produkte zu vermarkten.

Internationalisierung des IT-Sicherheitskennzeichens

Obwohl es sich bei dem IT-Sicherheitskennzeichen um ein nationales und freiwilliges Produktkennzeichen handelt, ist es erklärtes Ziel des BSI, mit dem deutschen IT-Sicherheitskennzeichen eine Blaupause und ein Vorbild für andere IT-Kennzeichnungsverfahren im europäischen und internationalen Kontext zu liefern. Bei der Fortentwicklung des IT-Sicherheitskennzeichens wird deshalb besonderer Wert auf einen bestmöglichen Gleichlauf mit bestehenden und zukünftigen europäischen und internationalen Cyber-Sicherheitskennzeichen und Sicherheitsstandards gelegt.

Vor diesem Hintergrund hat das BSI im Oktober 2022 beispielsweise eine bilaterale Vereinbarung mit der Cyber Security Agency Singapore (CSA) zur gegenseitigen Anerkennung des dortigen Cybersecurity Labelling Scheme (CLS) und des deutschen IT-Sicherheitskennzeichens unterzeichnet. Damit wird es Herstellern mit dem deutschen IT-Sicherheitskennzeichen des BSI ermöglicht, in Singapur ein Cybersecurity Label der dortigen Stufe 2 zu erhalten. Hersteller, deren Produkte ein gültiges Kennzeichen aus Singapur tragen, können für diese Geräte ein vereinfachtes Antragsverfahren zur Erteilung des deutschen IT-Sicherheitskennzeichens durchlaufen. Mit der gegenseitigen Anerkennung nimmt das BSI seine Rolle als Wegbereiter und Gestalter der sicheren Digitalisierung nicht nur in Deutschland, sondern auch auf internationaler Ebene wahr.

2.2 Verbraucherschutz im Ohr – Service im Blick: Das Zentrale Service-Center des BSI

Als am 1.12.2022 um kurz nach 8.00 Uhr die ersten Anrufe im Zentralen Service-Center eingingen, waren das Referats-Team sowie zahlreiche Unterstützende aus dem technischen Bereich erleichtert und glücklich. Die zuvor über mehrere Jahre von einem externen Anbieter durchgeführte Dienstleistung wurde von nun an wieder im Haus des BSI angeboten. Das neue Zentrale Service-Center dient als erste Anlaufstelle für Anfragen aller Zielgruppen rund um das Thema Informationssicherheit. Schon mit der Eröffnung des neuen BSI-Standortes im sächsischen Freital im Jahr 2019 kristallisierte sich heraus, dass das Zentrale Service-Center hier seinen zukünftigen Platz finden sollte.

Der Aufbau und die Inbetriebnahme in Freital waren mit einigen Herausforderungen verbunden. So war es zunächst erforderlich, den entsprechenden Personal- und Wissensaufbau zu tätigen. Zudem wurden die technischen Rahmenbedingungen geschaffen und die notwendigen Prozesse konzipiert und erprobt, beispielsweise im Hinblick auf die Qualitätssicherung. Dazu gehörte auch, die bestehende Wissensbasis auszubauen und weiterzuentwickeln, um Anfragen möglichst effektiv und sachkundig beantworten zu können. Die Mitarbeiterinnen und Mitarbeiter durchliefen vielfältige Schulungen und wurden in die Thematiken und Besonderheiten des Service-Center-Betriebes einer deutschen Bundes-

behörde eingearbeitet. Beispielsweise ist es dem BSI, als einer Behörde des Bundes, aufgrund des Gleichstellungsgrundsatzes und aus Wettbewerbsgründen nicht gestattet, konkrete Produkt- oder Dienstleistungsempfehlungen auszusprechen. Dies würde einem Eingriff in den freien Markt gleichkommen. Zudem kann das BSI weder Rechtsberatung anbieten noch strafverfolgend tätig werden. Für Anfragen dieser Art verweist das Zentrale Service-Center an externe Ansprechstellen, sofern diese bekannt sind.

Die Chancen und Verbesserungspotenziale, die sich aus der Verlagerung in ein internes Zentrales Service-Center ergeben, sind sehr vielfältig. Unter anderem können die Antwortqualität bei zu erwartendem steigenden Anfragevolumen erhöht und die Antwortzeiten verkürzt werden. Es entstehen daraus zahlreiche interne Synergieeffekte für unsere Zielgruppen, was sich positiv auf die Reputation und Außenwirkung des gesamten Hauses auswirkt.

Welche konkreten Aufgaben hat das Zentrale Service-Center?

Neben der direkten Beantwortung von Anfragen zur Informationssicherheit aus allen Zielgruppen im First-Level-Support zählen auch die Erfassung und Dokumentation der Anfragen zu seinen Aufgaben. Darüber hinaus koordiniert das Zentrale Service-Center die Aussteuerung von Anfragen, die der First-Level-Support nicht selbst beantworten kann, an die hausinternen Fachreferate und übernimmt die Qualitätssicherung und Dokumentation der Antworten. Weiterhin liegen die Pflege, der Ausbau und die Weiterentwicklung des zentralen Wissensmanagements zur effizienten, korrekten und zufriedenstellenden Beantwortung der Anfragen mit Unterstützung der zuständigen Fachreferate in seiner Verantwortlichkeit. Um das Aufgabenspektrum abzurunden, wird sowohl in regelmäßigen Abständen als auch anlassbezogen die Kundenzufriedenheit erhoben und ausgewertet, um daraus Handlungsbedarfe abzuleiten und deren Umsetzung sicherzustellen.

3 Fragen
an Diana Sachert, stellvertretende Referatsleiterin

Frau Sachert, was zeichnet das neue Zentrale Service-Center aus?

Das Thema Sicherheit in der Informationstechnik ist von Dynamik, Schnelllebigkeit, immer neuen Trends, Herausforderungen und einer sich ständig verschärfenden Bedrohungslage gekennzeichnet, was sich auch in der Menge und der Art der Anfragen widerspiegelt, die das BSI über verschiedene Kanäle wie Telefon, E-Mail, Fax und Online-Kontaktformular erreichen. Zudem führen auch die zunehmende Größe und der Zuwachs an Aufgaben und Zuständigkeiten des BSI dazu, dass Anzahl, Themenvielfalt und Komplexität der Anfragen steigen. Der Inhouse-Betrieb ermöglicht es uns, das Service-Center insgesamt auf ein breiteres Fundament zu stellen und das Service-Angebot zu stärken und auszubauen. Durch den gewachsenen Personalstamm, die enge Vernetzung mit den anderen Fachabteilungen und kurze Kontaktwege können eingehende Anfragen innerhalb kurzer Zeit effektiv und kompetent beantwortet werden. Als zentraler First-Level-Support innerhalb des BSI können wir auf ein breites Basiswissen der IT-Sicherheit und aller Themen, die in den Zuständigkeitsbereich des BSI fallen, zurückgreifen und im Bedarfsfall die zuständigen Fachabteilungen hinzuziehen. Erkenntnisse aus Kundenzufriedenheitsbefragungen können wir direkt prüfen und, falls notwendig und zweckmäßig, unser Dienstleistungsangebot und die Prozesse entsprechend anpassen.

Welche Vision verfolgen sie damit im Bereich der Cyber-Sicherheit?

Als Zentrales Service-Center möchten wir mit unserem Service-Angebot den Anfragenden schnelle und kompetente Unterstützung bei allen Themen rund um die IT-Sicherheit bieten. Hierfür möchten wir alle Zielgruppen aus Staat, Wirtschaft und Gesellschaft – und im Rahmen des Digitalen Verbraucherschutzes gerade auch die Verbraucherinnen und Verbraucher – informieren, beraten und warnen, damit sie digitale Produkte und Dienste sicher nutzen können. Im Falle eines IT-Sicherheitsvorfalls möchten wir bei der Bewältigung mit Hilfe zur Selbsthilfe unterstützen oder an geeignete Stellen und Ansprechpartnerinnen und -partner vermitteln. Das Zentrale Service-Center trägt damit dazu bei, die gesellschaftliche Widerstandsfähigkeit gegen Cyber-Gefahren zu steigern.

Abschließend ein Blick in Zukunft: Wo sehen Sie das Team in einem Jahr?

Wünschenswert ist, dass wir uns in einem Jahr als kompetente und serviceorientierte Ansprechstelle für alle Themen rund um die IT-Sicherheit etabliert haben. Wir informieren, beraten und warnen die Anfragenden aus Staat, Wirtschaft und Gesellschaft zu allen Bereichen der Cyber-Sicherheit. Dazu gehört auch, dass Service-Angebote regelmäßig im Hinblick auf die Bedarfe der Zielgruppen überprüft und weiterentwickelt werden. Bestenfalls wird das Zentrale Service-Center des BSI als sachkundige, erste Anlaufstelle der Cyber-Sicherheitsbehörde wahrgenommen und im Sinne unserer Leitziele Prävention, Detektion und Reaktion aktiv genutzt.

Kontakt:
Telefon: 0800 - 274 1000
E-Mail: service-center@bsi.bund.de

Welche Fragen erreichen das Zentrale Service-Center?

Die Top-Themen des Jahres 2022 in Sachen Informationssicherheit waren Spam- und Phishing-Mails, Anfragen zu Schutzmaßnahmen, Informationen über Angriffe und Infektionen von IT-Systemen als auch Fragen rund um die Öffentlichkeitsarbeit des BSI.

2.3 Cyber-Sicherheitsnetzwerk: Bundesweiter Wirkbetrieb gestartet

Am 1. Oktober 2022 startete der Wirkbetrieb des Cyber-Sicherheitsnetzwerks (CSN). Das CSN und die Digitale Rettungskette adressieren ausdrücklich Verbraucherinnen und Verbraucher sowie kleine und mittlere Unternehmen (KMU), die dadurch Unterstützung bei der Bewältigung von IT-Sicherheitsvorfällen erhalten. Es wird eine dezentrale Struktur aufgebaut, die diese Unterstützung effizient und kostengünstig anbieten kann. Durch die qualifizierten Helferinnen und Helfer wird fachkundige Hilfe auf Augenhöhe gewährleistet

Ausgangslage und Rahmenbedingungen

Die Gefahr für Privatpersonen und Unternehmen, Opfer eines Cyber-Angriffs zu werden, wächst stetig. In dem vom BSI-Lagebericht 2022 betrachteten Zeitraum – Juni 2021 bis Mai 2022 – wurden rund 116,6 Millionen neue Varianten von Schadprogrammen entdeckt, durchschnittlich 319.000 pro Tag. Außerdem wurde eine Zunahme von Spam- und Phishing-Mails sowie eine weiterhin große Anzahl aktiver Botnetze beobachtet. Angriffe mit Ransomware stellten dabei eine der größten Cyber-Bedrohungen für Staat, Wirtschaft und Gesellschaft dar.

Zielsetzungen des BSI und Grundidee des CSN

Das Bundesamt für Sicherheit in der Informationstechnik möchte daher als die zentrale Cyber-Sicherheitsbehörde des Bundes für Staat, Wirtschaft und Gesellschaft sein reaktives Angebot für Verbraucherinnen und Verbraucher stärken, aber auch für kleine und mittlere Unternehmen. Zielsetzung ist das vorhandene Wissen und die verfügbaren Fähigkeiten mit denjenigen zusammenzubringen, die dieses bei einem IT-Sicherheitsvorfall akut benötigen. Das Cyber-Sicherheitsnetzwerk ist dabei ein Baustein zur breiten Stärkung der Resilienz gegen Cyber-Bedrohungen insbesondere von Wirtschaft und Gesellschaft. Betroffene sollen schnell eine qualifizierte Unterstützung auf Augenhöhe erhalten.

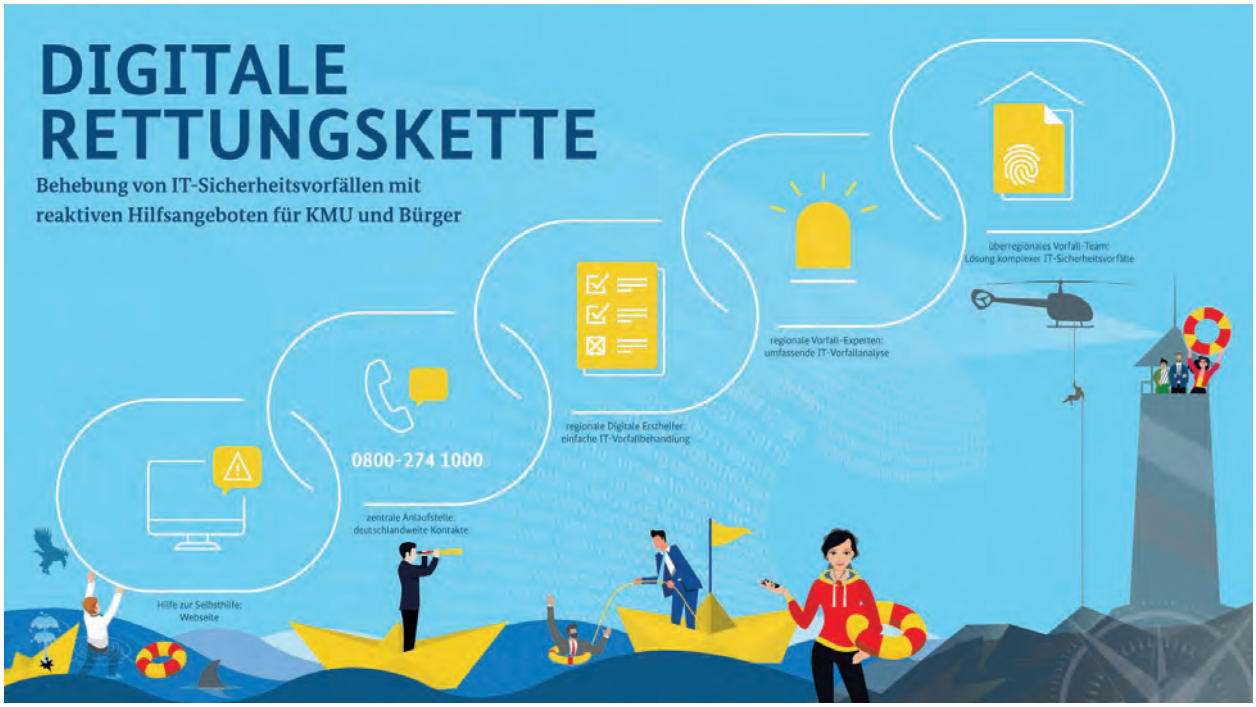
Das CSN ist ein freiwilliger Zusammenschluss von qualifizierten Expertinnen und Experten, die sich bereit erklären, ihr individuelles Fachwissen zur Behebung von IT-Sicherheitsvorfällen zur Verfügung zu stellen, und so mithelfen, die IT-Sicherheitslage in Deutschland zu verbessern. Sie unterstützen Betroffene dabei, IT-Sicherheitsvorfälle zu erkennen und zu analysieren, das Schadensausmaß zu begrenzen sowie weitere Schäden abzuwenden. Dabei können die Unterstützungsleistungen, die in der Digitalen Rettungskette des CSN beschrieben werden, je nach Vorfall und Zielgruppe unterschiedlich ausfallen. Die Digitale Rettungskette beginnt mit der Hilfe zur Selbsthilfe und führt über das CSN Service Center sowie die Digitalen Ersthelfer, Vorfall-Praktiker und Vorfall-Experten hin zu den IT-Sicherheitsdienstleistern. Sie bilden den Kern des Cyber-Sicherheitsnetzwerks.

Die Digitale Rettungskette

Die Digitale Rettungskette lehnt sich nicht zufällig an die bekannte Rettungskette bei Unfällen an. Sie zeichnet den Weg vor, den Betroffene und/oder Helferinnen und Helfer bei einem IT-Sicherheitsvorfall von den ersten Sofortmaßnahmen (Erste Hilfe) bis zum Einsatz von Profis (Vorfall-Experten, IT-Sicherheitsdienstleister) beschreitet. Mit jedem Glied der Kette wird der Vorfall zu einer höheren Qualifikationsstufe eskaliert, wenn er nicht gelöst werden kann. Durch die schrittweise Eskalation wird sichergestellt, dass den Betroffenen genau der Grad an Hilfestellung zur Verfügung gestellt wird, der der Art und dem Umfang des Vorfalls angemessen ist. Dies führt zu einem effizienten Einsatz der fachlichen und personellen Ressourcen des CSN – bei gleichzeitiger Kostenminimierung für Betroffene. Erster Schritt ist die Hilfe zur Selbsthilfe. Dieser Bereich wird durch die Informationsmaterialien des BSI abgedeckt. Verbraucherinnen und Verbraucher können sich an einer Schritt-für-Schritt-Anleitung orientieren und bekommen gleichzeitig eine zentrale Ansprechperson, die sie bei der Suche nach Hilfe und der Problemlösung unterstützt. Für den ersten persönlichen Kontakt ist das Zentrale Service Center des BSI eingerichtet. Dieses ist montags bis freitags zwischen 8 und 18 Uhr über die kostenfreie Hotline (0800 274-1000) erreichbar und hilft Betroffenen dabei, das passende Glied der Rettungskette auszuwählen.

Digitale Ersthelfer (DEH) sind für die First-Level-Unterstützung in der Digitalen Rettungskette im CSN zuständig. Sie unterstützen vorwiegend Verbraucherinnen und Verbraucher sowie Kleinstunternehmen mit schneller, telefoni-

Abbildung 3:
Die Digitale Rettungskette im Überblick



scher Ersthilfe. Zu den von ihnen angegebenen Servicezeiten stehen sie Betroffenen für Anfragen zur Verfügung.

Die Ersthelfer sollen auf Basis ihrer Einschätzung auch die Kontaktaufnahme mit den Vorfall-Experten empfehlen, wenn sie es für notwendig erachten. Den Rahmen für die Mitarbeit als Ersthelfer gibt der „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer“ vor. Dieser Leitfaden unterstützt die Ersthelfer auch bei der Analyse von IT-Sicherheitsvorfällen und gibt passende Handlungsempfehlungen. Sollten diese nicht für die Lösung des Vorfalls ausreichen, empfehlen die Ersthelfer die Kontaktaufnahme mit den Vorfall-Experten. Zur Dokumentation des Kontakts erstellen die Ersthelfer einen Vorfallsbericht, welchen sie den Betroffenen im Nachgang zusenden.

Die weiteren Glieder der Digitalen Rettungskette sind vor allem auf kleine und mittlere Unternehmen spezialisiert. Über den Ersthelfer stehen die aufgrund der Erfahrungen in der Pilotphase neu eingeführte Vorfall-Praktiker. Diese bieten eine First-Level-Unterstützung für KMU hinsichtlich der Digitalen Rettungskette. Die höchste Personenqualifikation ist die der Vorfall-Experten, die vom BSI zertifiziert werden. Hat ein Unternehmen mehrere Vorfall-Praktiker und Vorfall-Experten, so kann es sich außerdem als IT-Sicherheitsdienstleister zertifizieren lassen. Diese leisten bei größeren Vorfällen auch Vor-Ort-Unterstützung.

Breites Bundesweites Netzwerk

Ein wichtiger Baustein für die Netzwerkarbeit sind die Regionalen Foren. Ziel der Regionalen Foren ist neben dem Informationsaustausch vor allem die Bildung eines vertrauensvollen Netzwerks mit Gleichgesinnten, in welchem alle Teilnehmerinnen und Teilnehmer sich ohne wirtschaftliche, rechtliche und andere Zwänge auf Augenhöhe austauschen können. Das Regionale Forum soll insbesondere eine Anlaufstelle für Digitale Ersthelfer sein, bei der sie ihre Erfahrungen bei der Arbeit in der Digitalen Rettungskette des Cyber-Sicherheitsnetzwerks teilen können und von erfahrenen Forenleiterinnen und -leitern Tipps und Empfehlungen erhalten. Vor allem sollen hier IT-Sicherheitsprobleme und Lösungsmöglichkeiten besprochen werden. Auch für die Evaluierung von Fällen und die Entwicklung von Best Practices bieten Regionale Foren den passenden Rahmen.

Zusätzlich sollen die Regionalen Foren genutzt werden, um in sicherer Umgebung die Vorfallsbearbeitung möglichst realitätsnah zu trainieren. Hierfür wurde der CSN-Trainingskoffer entwickelt. Dieser beinhaltet verschiedene spielerische Ansätze zum Kennenlernen der Digitalen Rettungskette sowie zum Üben von Szenarien. Alle Inhalte des Trainingskoffers sind so gestaltet, dass sie selbst ausgedruckt werden können – die Materialien dürfen und sollen auch von Unternehmen oder anderen Interessierten kostenfrei für eigene Schulungsmaßnahmen verwendet werden.

Ausblick

Wie jedes neue Netzwerk kann auch das CSN mehr leisten, wenn es wächst. Daher liegt der Fokus derzeit auf der Skalierung der Prozesse, dem Ausbau des Helfernetzwerks sowie der Schulungsmöglichkeiten. Um Verbraucherinnen und Verbrauchern sowie KMU immer die bestmögliche Hilfe anbieten zu können, ohne gleichzeitig die Helferinnen und Helfer zu überlasten, ist eine große Anzahl von engagierten Menschen notwendig. Jede IT-affine Person kann Teil dieses Netzwerks werden, anderen bei der Bewältigung von IT-Sicherheitsvorfällen helfen und gleichzeitig von den Qualifizierungs- und Austauschangeboten des CSN profitieren. An einer Teilnahme Interessierte erhalten weiterführende Informationen über die Webseite des BSI beziehungsweise direkt über www.cyber-sicherheitsnetzwerk.de. Das CSN-Team freut sich über jede Neuregistrierung.

3 Jahresübersicht 2022: Schwerpunkte von Sicherheitsvorfällen auf dem digitalen Verbrauchermarkt

Für Verbraucherinnen und Verbraucher war im IT-Sicherheitsbereich das Jahr 2022, wie auch das vorherige, von den Themen Phishing, Ransomware und Datenleaks geprägt. Aber auch Sicherheitslücken bei digitalen Diensteanbietern, Schwachstellen in digitalen Verbraucherprodukten und Täuschungsversuche bei Onlinediensten haben die Lage der Informationssicherheit beeinflusst. Neben Angriffen auf Unternehmen rückten zunehmend Institutionen des öffentlichen Sektors in den Fokus von Cyber-Kriminellen. So haben im Jahr 2022 unter anderem zahlreiche Cyber-Angriffe auf Kommunalverwaltungen in mehreren Bundesländern verdeutlicht, wie schnell Verbraucherinnen und Verbraucher indirekt Opfer von Cyber-Kriminalität werden können.

Cyber-Angriffe im öffentlichen Sektor

Exemplarisch sei hier ein Angriff von Cyber-Kriminellen vom April 2022 auf eine baden-württembergische Stadtverwaltung genannt, bei welchem unter anderem persönliche Daten von Einwohnerinnen und Einwohnern erbeutet und anschließend im Darknet veröffentlicht worden sind. Nach Medienberichten und eigener Aussage der Täterinnen und Täter soll es sich dabei um 170 Gigabyte an Daten gehandelt haben. Darin enthalten waren sensible Informationen von Ausweisdokumenten, Verträgen und Asylanträgen. Der Angriff mittels Ransomware verursachte zudem einen zeitweiligen Ausfall des Verwaltungsbetriebs. Insbesondere die Erreichbarkeit von wichtigen Einrichtungen wie Schulen, Kindergärten, Bürger- und Standesamt wurde vorübergehend eingeschränkt. Verantwortlich zeichnete sich die für ihre Ransomware-Angriffe einschlägig bekannte Gruppe „LockBit 2.0“ (vgl. golem, 2022).

Ransomware-Gruppen wenden regelmäßig eine zweistufige Erpressungstechnik an. Auf der ersten Stufe werden Dateien auf den angegriffenen Systemen verschlüsselt und anschließend wird Lösegeld für deren Entschlüsselung gefordert. Auf der zweiten Stufe betreiben die Ransomware-Gruppen Leak-Seiten im Darknet, auf denen die gestohlenen Daten veröffentlicht werden (vgl. BSI 2022, S. 15 f.). In letzter Konsequenz ist nicht auszuschließen, dass die Erpresserinnen und Erpresser doppelt profitieren: Sowohl vom Lösegeld als auch vom Verkauf der Daten an interessierte Dritte.

Neben weiteren Angriffen auf Stadtverwaltungen wurde in Rheinland-Pfalz eine gesamte Kreisverwaltung durch einen Cyber-Angriff lahmgelegt – auch hier sind teils personenbezogene Daten abgeflossen, die später im Darknet veröffentlicht worden sind (vgl. Heise, 2022).

Auch der Bildungssektor war im Berichtsjahr Zielscheibe zahlreicher Cyber-Angriffe. Ob Angriffe auf die Verfügbarkeit der Systeme mittels „Distributed Denial of Service“-Attacken (DDoS), Ransomware oder Kompromittierung von Social Media Accounts – die Betroffenheit war vielfältig. Besonders häufig kam Ransomware zum Einsatz. Im April 2022 konnte beispielsweise die für ihre zahlreichen Ransomware-Angriffe auf Hochschulen bekannte Gruppe „Hive“ nach eigenen Angaben über 400 Gigabyte an Daten von einer Hochschule in Berlin erbeuten (vgl. HTW Berlin, 2022). Neben den Bildungseinrichtungen selbst sind die Studierenden in vielen Fällen gleich doppelt leidtragend: Zu dem eingeschränkten Studienbetrieb, den nicht verfügbaren Lernplattformen und den ausgefallenen Prüfungen kam für die Studierenden die Sorge zum Verbleib eingereichter Prüfungsleistungen und zur Preisgabe von personenbezogenen Daten hinzu.

Derartige Cyber-Angriffe auf öffentliche Institutionen im Kommunal- und Bildungsbereich führen zu erheblichen Beeinträchtigungen bis hin zum Ausfall kritischer Dienstleistungen wie zum Beispiel den Zahlungen von Sozialleistungen oder Elterngeld (vgl. BSI 2022, S. 21).

Ransomware in der Dienstleistungsbranche

Neben Ransomware-Angriffen auf Einrichtungen des öffentlichen Sektors waren im Jahr 2022 auch eine Vielzahl von Unternehmen von dieser Angriffsform betroffen. Infolge des damit zusammenhängenden Diebstahls und der anschließenden Veröffentlichung von teils sensiblen, personenbezogenen Daten ist die Bedrohungslage für Verbraucherinnen und Verbraucher weiterhin angespannt. So kam es im Frühjahr 2022 zu einem IT-Sicherheitsvorfall bei einem europäischen Anbieter im Bereich des Forderungsmanagements. Die Verschlüsselung von Servern hatte Auswirkungen auf den Geschäftsbetrieb der Unternehmensgruppe in mehreren Ländern, darunter Deutschland. Dem Modus Operandi folgend hatten die Angreifenden Daten des Unternehmens, insbesondere auch personenbezogene Daten von Privatpersonen, abgegriffen und anschließend im Darknet veröffentlicht. Dieser Vorfall ist dahingehend gravierend, als dass es sich bei den gestohlenen und veröffentlichten Daten um äußerst vertrauliche Informationen, wie zum Beispiel offene Zahlungsverpflichtungen von Verbraucherinnen und Verbrauchern, handelte (vgl. Lowell, 2022).

Ebenfalls von Ransomware betroffen war ein deutscher Konzern in der Autovermietungsbranche. Die laufende Auswertung des Vorfalls ergab, dass die dafür verantwortliche Gruppe von Hackerinnen und Hackern, „Black Basta“, einen Teil der Kundenstammdaten kopiert hatte. Unter den Daten waren unter anderem Vor- und Nachnamen, Kundennummern sowie Kontaktdaten wie zum Beispiel Anschrift und E-Mailadresse (vgl. Spiegel, 2022). Obwohl die Hackergruppe noch relativ neu in der Szene ist, wurden zwischen April und September 2022 bereits über 75 Unternehmen und Institutionen von ihr angegriffen (vgl. B2B Cyber Security, 2022).

Sicherheitslage im Onlineshopping

Fehlende adäquate Schutzmaßnahmen waren im Jahr 2022 für eine Vielzahl von IT-Sicherheitsvorfällen verantwortlich (vgl. BSI 2022, S. 19). So auch im Onlineshopping, das bei Verbraucherinnen und Verbrauchern besonders beliebt ist. Gemäß einer bevölkerungsrepräsentativen Umfrage im Rahmen einer BSI-Studie gaben 91 Prozent der Befragten an, zumindest gelegentlich online einzukaufen (vgl. BSI 2022a).

Anfang des Jahres gelang Cyber-Kriminellen mittels eines Brute-Force-Angriffs auf den Onlineshop eines Buchhändlers der Zugriff auf eine mittlere fünfstellige Anzahl von Kundenaccounts. Über mehrere Stunden wurden systematisch Benutzername-Passwort-Kombinationen durchprobiert (vgl. Heise 2022a). Ein weiterer Fall verdeutlicht, dass das Risiko eines Datendiebstahls für Verbraucherinnen und Verbraucher im Onlineshopping besonders hoch ist. Ebenfalls im ersten Quartal 2022 hatten Cyber-Kriminelle über einen Zeitraum von mehreren Wochen den Onlineshop eines deutschen Matratzenherstellers angegriffen. Infolge dieses Angriffs hatten die Cyber-Kriminellen während des Bestellvorgangs Zugriff auf persönliche Kundendaten in zwölf Ländern, darunter Deutschland. Betroffen von dem Vorfall war der Bestellvorgang, wodurch die Angreifenden Zugriff auf Daten von Kredit- und Debitkarten erlangten (vgl. The Register 2022).

IT-Sicherheit auf dem digitalen Verbrauchermarkt - Fokus: Onlineshopping-Plattformen.

Im Jahr 2022 hat das BSI eine Detailuntersuchung zur Sicherheit von Verbraucherdaten in Datenbanken von Onlineshopping-Plattformen in Auftrag gegeben. Ziele der Untersuchung waren der Gewinn von Informationen in Bezug auf die Sicherheit von Kundendaten ausgewählter Softwarelösungen im Onlineshopping sowie zu den Bedürfnissen, Erwartungen, Wahrnehmungen und Verhaltensweisen von Verbraucherinnen und Verbrauchern bei konkreten Datenleak-Vorfällen. Die Studienergebnisse sind unter folgendem Link veröffentlicht.

Ein besonders gravierender Vorfall, der sich bereits im Jahr 2021 ereignete, allerdings Anfang 2022 erneut durch die Medien aufgegriffen wurde, verdeutlicht die Ohnmacht der von einem Datenleak betroffenen Verbraucherinnen und Verbraucher. Infolge einer fehlkonfigurierten Schnittstelle zwischen großen Online-Marktplätzen und externen Händlerinnen und Händlern standen über mehrere Jahre zirka eine Million Datensätze von ungefähr 700.000 Kundinnen und Kunden ungeschützt im Internet, darunter E-Mail- und Postadressen, Bestellinformationen, Telefonnummern und teilweise sogar Bankverbindungen. Die von dem Vorfall betroffenen Verbraucherinnen und Verbraucher wurden weder von den Online-Marktplätzen noch den jeweiligen Online-Händlerinnen und Händlern informiert (vgl. Tagesschau 2022).

Die geschilderten Fälle verdeutlichen, dass aufgrund unzureichender IT-Sicherheitsmaßnahmen ein hohes Risiko für Verbraucherinnen und Verbraucher besteht, Opfer eines Datenleak-Vorfalls zu werden. In der bereits erwähnten Studie zur IT-Sicherheit von Onlineshopping-Plattformen gaben 68 Prozent der Befragten an, dass sie generell Bedenken beim Onlineshopping haben. Nach konkreten Bedenken gefragt, nannten 61 Prozent der Befragten das Weiterreichen der persönlichen Daten an Dritte und die Hälfte nannte das unrechtmäßige Einsehen oder Veröffentlichen der persönlichen Daten. Über ein Drittel (37 %) äußerte Bedenken, dass das Passwort zum Kundenbereich im Onlineshopping nicht sicher abgelegt wird.

Täuschung bei Onlinediensten

Cyber-Kriminelle entwickeln permanent neue Angriffsmethoden, um Verbraucherinnen und Verbraucher im Internet zu täuschen. Im Jahr 2022 waren insbesondere Fake-Webseiten, Fake-Accounts und Fake-Shops aktuell. Fake-Webseiten täuschen Verbraucherinnen und Verbraucher durch das gleiche Erscheinungsbild wie das vertrauter Originalseiten. Jedoch werden die Nutzenden auf den gefälschten Webseiten dazu aufgefordert, persönliche Daten wie Bankdaten anzugeben, oder Schadsoftware wird unwissentlich installiert. Auch Fake-Accounts werden häufig als Täuschungsinstrument im Internet benutzt. Dabei geben Cyber-Kriminelle vor, eine andere reale oder fiktive Person zu sein, um das Abgreifen von sensiblen Daten zu ermöglichen oder falsche Informationen zu verbreiten. Ein beispielhaftes Szenario ist das Vortäuschen eines gewonnenen Gewinnspiels. Angreifende behaupten dabei in einer privaten Nachricht an die Opfer, dass diese ein Gewinnspiel gewonnen haben und erfragen sensible Daten oder verweisen auf einen Phishing-Link.

Fake-Shops locken Verbraucherinnen und Verbraucher mit Sonderangeboten. In diesem Jahr tauchte beispielsweise ein Fake-Shop eines bekannten Luxusmode-Unternehmens aus Italien auf. Designerartikel werden auf einer realitätsnahen Nachbildung der Webseiten zum Bruchteil der Originalpreise angeboten (vgl. vzhh, 2022). Die Bezahlung in gefälschten Shops erfolgt meistens durch Vorkasse, jedoch wird die bestellte Ware zumeist gar nicht oder in mangelhafter Qualität geliefert.

Woran erkenne ich sichere Onlineshops?

Um den finanziellen Schaden bei Verbraucherinnen und Verbrauchern zu vermeiden, gibt es hier weitere hilfreiche Hinweise zum sicheren Onlineshopping.

Fake-Shops zu identifizieren kann für Verbraucherinnen und Verbraucher schwierig sein. Eine fehlende Anbieterkennzeichnung kann unter anderem auf einen Fake-Shop hindeuten, denn jede Online-Präsenz, die nicht ausschließlich privaten Zwecken dient, benötigt ein Impressum. Die Impressumspflicht ist durch § 5 TMG (Telemediengesetz) geregelt. Steht in einem Onlineshop nur eine Zahlungsmöglichkeit zur Verfügung oder sind die allgemeinen Geschäftsbedingungen sowie Informationen zum Datenschutz nicht einsehbar, dann können dies weitere Indizien für einen Fake-Shop sein (vgl. BSI, 2022).

Steigende Energiepreise: Betrug unter falscher Flagge

Im Bericht zum Digitalen Verbraucherschutz 2020 wurde anhand der COVID-19-Pandemie dargestellt, wie schnell und flexibel Cyber-Kriminelle auf gesellschaftliche Krisensituationen reagieren und versuchen, diese gewinnbringend zu nutzen (vgl. BSI, 2021). Im Berichtsjahr 2022 konnte diese Beobachtung anhand der angespannten Situation auf den Energiemärkten fortgeschrieben werden. Angesichts stark steigender Preise beschloss die Bundesregierung mehrere Entlastungspakete, um unter anderem die Folgen steigender Energiepreise für Verbraucherinnen und Verbraucher abzumildern. Mithilfe griffiger Betreffzeilen wie „Jetzt Energiepauschale sichern!“, „Wir überweisen die Energiepauschale“ oder auch „Bereit für Ihren Energiebonus?“ instrumentalisierten Cyber-Kriminelle die angekündigten Staatshilfen für Betrugsversuche, insbesondere mithilfe von Phishing-Mails.

Das Phishing-Radar der Verbraucherzentrale Nordrhein-Westfalen dokumentierte in der zweiten Jahreshälfte 2022 ein erhöhtes Aufkommen gefälschter E-Mails, welche den Empfängerinnen und Empfängern beispielsweise eine Auszahlung der Energiepauschale in Aussicht stellten, sofern diese der Aufforderung nachkommen, personenbezogene Daten, Kontoverbindungen oder Kreditkartennummern auf einer verlinkten Internetseite bereitzustellen. Häufig geschah dies begleitet von der Aussage, die Daten müssten abgeglichen werden, um die Auszahlung der Pauschale sicherzustellen. Für einen vertrauenswürdigen Eindruck und Seriosität agierten die Cyber-Kriminellen nicht selten unter dem Deckmantel bekannter Kreditinstitute oder auch Bundesministerien. Als Beispiele seien hier gefälschte E-Mails und Internetseiten mit Logos von Banken oder auch vermeintliche SMS des Bundesministeriums der Finanzen genannt. In letzterem Fall spricht man von „Smishing“ (zusammengesetzt aus den Begriffen SMS und Phishing). Die Verbraucherzentrale Nordrhein-Westfalen, die Bundesnetzagentur und das BSI veröffentlichten entsprechende Warnungen (vgl. Verbraucherzentrale NRW, 2022).

Das Thema Phishing ist Fokusthema dieses Berichts und wird im nächsten Kapitel detailliert aufgegriffen, wobei besonders die Herausforderungen von Phishing im Bankensektor detailliert erläutert werden. Auch weiterführende Informationen zum Phishing-Radar der Verbraucherzentrale Nordrhein-Westfalen mit seinem Melde- und Warnverfahren sind an dieser Stelle zu finden.

Neben Betrugsversuchen via Mail, SMS und Fake-Anrufen breiteten sich Fake-Shops vermehrt im Bereich des Brennstoffhandels aus. In mehreren Bundesländern warnte die Polizei vor Online-Betrügereien mit Brennholz und Pellets. Mit besonders niedrigen Preisen und seriös anmutenden Seitenlayouts wurden Opfer in Versuchung gebracht, eine vermeintlich günstige Alternative für den Heizbedarf erwerben zu können. Hierfür wurden neben eigenen Fake-Shops auch bekannte Online-Marktplätze und Tauschbörsen genutzt (vgl. ZDF, 2022). Der Bundesverband Brennholz musste zudem feststellen, dass sich die Täter nicht selten der Identitäten von real existierenden, seriösen Händlern bedienten. Eine Liste gemeldeter Fake-Shops ist auf dem Webauftritt der Bundesverbandes Brennholz veröffentlicht (vgl. Bundesverband Brennholz, 2022).

Bei den aufgezeigten Fällen ist das Muster der Cyber-Kriminellen ähnlich: Sie bedienen sich Social-Engineering-Methoden, welche auf das Ausnutzen der Schwachstelle „Mensch“ abzielen. Täterinnen und Täter nutzen bekannte psychologische Effekte aus, nach denen Menschen in unsicheren Situationen, mit Ängsten oder in Notlagen eher dazu tendieren, emotional statt rational zu handeln. Im Jahr 2022 waren Kriegsängste und finanzielle Existenzängste hierbei maßgebend. Um Verbraucherinnen und Verbraucher schnell und direkt für solche und ähnliche Angriffsmethoden zu sensibilisieren, veröffentlicht das BSI regelmäßig entsprechende Hinweise auf seinen Internetseiten und Social-Media-Kanälen.

Digitale Energiewende: Mit Sicherheit begleiten

Im Berichtsjahr führten Cyber-Angriffe auf Energie- und Immobiliendienstleister zu weiteren Einschränkungen für Verbraucherinnen und Verbraucher, auch unabhängig von der Heizmittelbeschaffung selbst. Unter anderem wurden zwingend notwendige Arbeitsprozesse wie Heiz- und Betriebskostenabrechnungen in Mitleidenschaft gezogen. In einem konkreten Fall vom Juli 2022 wurde ein weltweit operierender Energie- und Immobiliendienstleister mit Sitz in Deutschland Opfer eines Ransomware-Angriffs. Die Folge: Nach Unternehmensangaben wurden neben zeitweise eingeschränkten technischen Dienstleistungen und verzögerten Abrechnungen, zahlreiche Verbrauchsdaten – wie Heiz-, Warm- und Kaltwasserverbrauch – sowie zum Teil personenbezogene Daten durch die Cyber-Kriminellen erbeutet

und veröffentlicht. Das Unternehmen zog unverzüglich externe Unterstützung heran und informierte die zuständigen Datenschutz- und Ermittlungsbehörden.

Im Rahmen der digitalen Energiewende und mit wachsender Innovationskraft bei intelligenten Messsystemen werden neben bereits gesetzlich vorgeschriebenen fernablesbaren Wasserzählern und Heizkostenverteilern aller Voraussicht nach immer mehr Gebäude auf IoT-Fähigkeit ausgelegt. Verbraucherinnen und Verbraucher werden dadurch verstärkt in die Lage versetzt, ihren aktuellen Verbrauch beispielsweise per Webanwendung, per E-Mail oder mithilfe einer Smartphone-App kontinuierlich im Blick zu behalten. Dies schafft Transparenz und zeigt Einsparpotenziale auf, welche gerade in der angespannten Situation auf den Energiemärkten von hoher Bedeutung sind.

Die Aufgabe des Digitalen Verbraucherschutzes im BSI ist es, die Entwicklungen in dem Bereich genau zu beobachten und mögliche Gefährdungen der Informationssicherheit frühzeitig im Sinne eines ganzheitlichen Verbraucherschutzes zu begegnen. Denn auch hier ist klar: Fortschritte in der Digitalisierung gelingen nur im Gleichschritt mit Informationssicherheit.

Smarte Geräte im Haushalt: Gefahrenpotenzial weiterhin vorhanden

Mit dem Einzug vernetzter Geräte in die eigenen vier Wände entscheiden sich Verbraucherinnen und Verbraucher – im Gegensatz zur meist nur mittelbar wahrgenommenen Gebäudeinfrastruktur – ganz bewusst für die Digitalisierung des Alltags. Die vernetzten Objekte versprechen dabei Komfort, Intelligenz und Energieeinsparpotenziale. Laut einer repräsentativen Umfrage im Auftrag des Digitalverbandes Bitkom nutzten 43 Prozent der Verbraucherinnen und Verbraucher im Jahr 2022 Smart Home-Technologien. Vor dem Hintergrund der gestiegenen Energiepreise verwundert es nicht, dass vor allem der Einsatz von smarten Energiespar-Tools angestiegen ist. 25 Prozent der Befragten gaben an, inzwischen smarte Heizkörperthermostate zu nutzen. Doch trotz der großen Verbreitung smarter Haushaltsgeräte gab fast die Hälfte (47 %) der Gruppe der Nicht-Nutzenden an, sich vor Cyberangriffen zu fürchten. Auch Sorgen vor dem Missbrauch von persönlichen Daten hält mehr als ein Drittel (37 %) der Befragten von der Anschaffung smarter Haushaltsgeräte ab (vgl. Bitkom 2022).

Dass die Sorgen der Verbraucherinnen und Verbraucher nicht unbegründet sind, zeigen die im Jahr 2022 entdeckten Schwachstellen und Sicherheitsvorfälle. Die Palette ist vielfältig: Smarte Speaker, die sich selbst Befehle zum Onlineshopping erteilen konnten, oder ein mit einer Kamera ausgestatteter Katzenfutterautomat, der einen nächtlichen Polizeieinsatz auslöste, da die Besitzerin im Internet auf veröffentlichte Video- und Tonaufnahmen ihrer Wohnung gestoßen ist (vgl. Spiegel, 2022). Ein besonders bemerkenswerter Fall: Bei einer Untersuchung von videogestützten Babyphones gelang es Sicherheitsforschenden, Live-Bilder abzufangen und Schadcode direkt im Betriebssystem der Geräte auszuführen (vgl. Bitdefender, 2022). Nicht selten sind Sicherheitsvorfälle im IoT- und Smart Home-Bereich auf eine unzureichend gesicherte Gerätekonfiguration ab Werk zurückzuführen und wären vermeidbar gewesen.

Das BSI und auch die Verbraucherzentralen werben daher mit Nachdruck gegenüber Herstellern und Anbietern für die Beachtung der Prinzipien „Security by Design“ und

Den Wohnraum sicher vernetzen.

Ob Energiesparmaßnahme oder persönlicher Komfortgewinn: Das BSI empfiehlt Verbraucherinnen und Verbrauchern in jedem Fall beim Einsatz vernetzter Geräte auf Datensparsamkeit zu achten und niemals das vom Hersteller vergebene Standard-Passwort zu nutzen. Weiterführende Informationen zur sicheren Einrichtung vernetzter Geräte im Eigenheim finden Sie als Ratgeber auf dem Webauftritt des BSI.

„Security by Default". Nur wenn die Informationssicherheit von vernetzten Geräten und Anwendungen schon ab der Konzeptions- und Entwicklungsphase und über den gesamten Lebenszyklus hinweg mitgedacht wird, kann ein ausreichender Basisschutz erreicht werden. Zudem sollten die Bedürfnisse und Fähigkeiten der Nutzenden bereits mit in die Produktentwicklung einbezogen und beim Design von Nutzeroberflächen mitgedacht werden, um auch die Bedienbarkeit von sicherheitsrelevanten Eigenschaften gewährleisten zu können. In der Forschung hat sich hierfür der Begriff der „Usable Security" etabliert. Das wachsende Risikobewusstsein in der Gesellschaft könnte in der strategischen Produktentwicklung von Herstellern und Anbietern als Marktvorteil verwertet werden.

Eine repräsentative Umfrage des Marktforschungsinstituts Kantar im Auftrag des Verbraucherzentrale Bundesverband (vzbv) legt offen, dass Verbraucherinnen und Verbraucher viele Risiken bei vernetzten Geräten sehen und ein Großteil sich einen umfassenderen Schutz und gesetzliche Verpflichtungen wünscht. Beispielsweise sehen 75 Prozent der Befragten ein Risiko, wenn Produktvoreinstellungen auf das niedrigste Schutzniveau vorkonfiguriert sind. 75 Prozent der Befragten sehen es kritisch, wenn keine Sicherheitsupdates mehr für ihre Produkte angeboten werden. Um das Vertrauen zu erhöhen, wünschen sich 70 Prozent der Befragten gesetzlich festgeschriebene, einheitliche und von anerkannten Stellen kontrollierte Mindestanforderungen für ihre IT-Sicherheit (vgl. vzbv, 2022). Der bisherige europäische Rechtsrahmen für das Inverkehrbringen und den Betrieb von Verbraucherprodukten konzentriert sich vorwiegend auf die allgemeine Produktsicherheit – beispielsweise Risikominimierung bei Gefahr für Leib und Leben.

Das BSI begrüßt entsprechende Vorstöße der EU-Gesetzgebung, welche sich im Berichtsjahr vermehrt mit dem Thema der Informationssicherheit und dem Schutz von Verbraucherinnen und Verbrauchern im digitalen Alltag auseinandergesetzt haben. Hierfür werden einheitlich geltende und transparente Regelungen für den europäischen Binnenmarkt angestrebt, was eine erfreuliche Entwicklung im Sinne eines ganzheitlichen Verbraucherschutzes darstellt. Bei der Ausgestaltung entsprechender Gesetzesinitiativen wie unter anderem den in Verhandlung befindlichen Gesetz über Cyberresilienz, beteiligt sich das BSI regelmäßig mit seiner Erfahrung und Fachkenntnis.

EU-Gesetzgebung: Mehr Cyber-Resilienz in Europa

Mit dem im Herbst 2022 durch die Europäische Kommission auf den Weg gebrachten Vorschlag für ein Gesetz über Cyber-Resilienz (2022/0272 (COD)), sollen gemeinsame Sicherheitsvorschriften für Hard- und Softwareprodukte im Europäischen Binnenmarkt vorgeschlagen werden. Es wird die erste EU-weite Rechtsvorschrift ihrer Art sein und richtet sich vor allem an Hersteller und Entwicklerinnen sowie Entwickler von Produkten mit digitalen Elementen. Der bisherige europäische Flickenteppich an unterschiedlichen nationalen Schutzniveaus von digitalen Produkten soll durch die vollharmonisierende Vorschrift aufgelöst und zu einheitlichen europäischen IT-Sicherheitsanforderungen zusammengeführt werden. Der in Kurzform „CRA" genannte Entwurf erfasst alle drahtgebundenen und drahtlos mit dem Internet verbundenen Produkte und Software. Diese müssen künftig bestimmten Sicherheitsanforderungen genügen, um überhaupt in der EU in Verkehr gebracht werden zu können. Neben diesen Markteintrittsvoraussetzungen sollen Hersteller zum ersten Mal auch die Informationssicherheit ihrer Produkte während der Lebensdauer verpflichtend betrachten. Eine regelmäßige Updateversorgung und ein geeignetes Schwachstellenmanagement sollen über einen angemessenen Zeitraum obligatorisch vorgesehen werden. Außerdem sollen Anwenderinnen und Anwender mit ausreichend Informationen beim Kauf und während der Verwendung ihrer Produkte versorgt werden.

Das geplante Gesetz über Cyber-Resilienz befindet sich derzeit im europäischen Gesetzgebungsverfahren und ist im Zusammenspiel mit einer Reihe weiterer geplanter oder schon in Anwendung befindlicher EU-Verordnungen und Richtlinien zu betrachten. Zu nennen sind hier insbesondere der Rechtsakt für Cybersicherheit (CSA) ((EU) 2019/881) oder die überarbeitete Richtlinie zur Sicherheit von Netz- und Informationssystemen (NIS 2.0) ((EU) 2022/2555).

Resümee

Sogenannte Offline-Produkte, die im Nutzungsalltag von Verbraucherinnen und Verbrauchern längst etabliert sind, verfügen zunehmend über digitale und vernetzte Elemente. Sie sind dann auf einer Stufe mit den klassischen Soft- und Hardware-Produkten und werden damit überhaupt erst relevant für die Informationssicherheit im digitalen Raum. Die hier exemplarisch aufgeführten Vorfälle zeigen erneut, dass Informationssicherheitsrisiken frühzeitig adressiert und abmildernde Maßnahmen von Anfang an mitgedacht werden sollten.

Die Begleitung des kontinuierlich wachsenden Anteils an vernetzten Geräten in privaten Haushalten wird eine wachsende Herausforderung im Digitalen Verbraucherschutz sein. Ferner sollen Verbraucherinnen und Verbraucher für mögliche Gefahren und Angriffsvektoren beim Einsatz smarter Alltagshelfer – insbesondere, wenn diese über Mikrofon- und Videofunktionen verfügen – sensibilisiert und zu einem sicheren Betrieb derer befähigt werden. Mit Informationskampagnen, Broschüren und Messeauftritten wird das BSI auch im Jahr 2023 breite Präsenz zeigen und seinem Aufklärungsauftrag nachkommen.

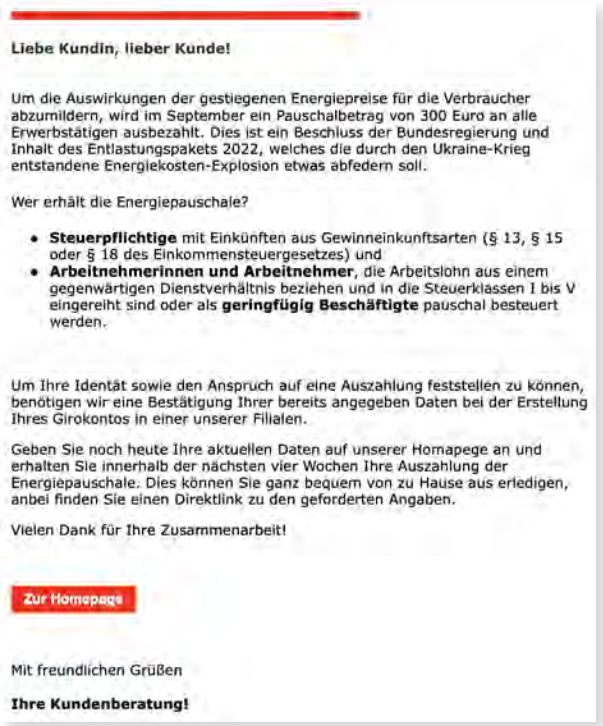
Zur spürbaren Stärkung der Resilienz im digitalen Raum müssen Verbraucherinnen und Verbraucher eigene Schutzmaßnahmen aktiv ergreifen. Dies ist ein wichtiger Baustein. Die Verbesserung der gesamtgesellschaftlichen Informationssicherheit ist zudem eine gemeinsame Aufgabe aller Akteurinnen und Akteure in Staat, Wirtschaft und Gesellschaft.

4 Fokusthema: Gefahrenquelle Phishing

Zu viel Stress, wenig Zeit und keine Lust auf Ärger: Beim sogenannten Phishing nutzen Cyber-Kriminelle unseren vollgepackten Alltag aus. Ein Klick in einer Mail ist schnell erfolgt, aber kann weitreichende Folgen haben, wenn es sich dabei um Betrugsversuche handelt. Diese sind nach wie vor sehr verbreitet und stellen Verbraucherinnen und Verbraucher vor Herausforderungen.

Phishing, eine Komposition aus „password" und „fishing", steht für den gezielten Diebstahl von Zugangsdaten zu Online-Nutzerkonten und ist bedauerlicherweise ein verbreitetes Phänomen. Im BSI-Lagebericht 2022 wird das Ausmaß von Phishing deutlich: Rund 90 Prozent aller betrügerischen E-Mails sind darauf ausgelegt, Daten und Passwörter von Anwenderinnen und Anwendern abzugreifen. Knapp 30 Prozent aller versendeten Spam-Mails fallen in die Kategorie Phishing. Aufgrund der großen Verbreitung kennen viele Verbraucherinnen und Verbraucher das Problem gut. Im Digitalbarometer 2022 gaben mehr als sechs von zehn Befragten an, bereits betrügerische Mails erhalten zu haben, ohne jedoch auf deren Forderungen eingegangen zu sein. Dabei ist genau das nicht selbstverständlich, denn oft nutzen Bertrügerinnen und Betrüger menschliche Verhaltensmuster gezielt aus, um ihre Ziele zu erreichen.

Das Prinzip Phishing ist keinesfalls neu. Schon seit Jahren warnen Sicherheitsbehörden und das BSI vor Betrugsversuchen. Allerdings entwickeln Cyber-Kriminelle ihre Methoden immer weiter. Das bewährte Vorgehen bleibt dabei grundsätzlich gleich: Potenzielle Opfer werden kontaktiert und unter Nennung von angeblich dringlichen Gründen gebeten, ihre Daten einzugeben oder sich bei ihrem Konto anzumelden. Dazu enthält die E-Mail meist einen Link, der auf eine fingierte Webseite führt. Diese haben die Cyber-Kriminellen vorbereitet, um die eingegebenen Daten abzufangen. Manche dieser Phishing-Attacken kann man anhand von Mängeln in Orthografie, Grammatik und Sprachstil schnell erkennen – aber nicht alle. Es gibt eine Vielzahl von sehr realistisch gestalteten Phishing-Mails, in denen beispielsweise das Corporate Design von Firmen exakt nachgeahmt wird. Immer wieder beziehen sich die Täterinnen und Täter auch auf aktuelle Anlässe, was den Kontext einer Nachricht plausibler erscheinen lässt. Das geschah beispielsweise bei der Auszahlung der Energiepreispauschale im Herbst 2022, aus der Cyber-Kriminelle auf vielfältige Weise versuchten, Profit zu schlagen. Ein Phishing-Versuch aus dieser Zeit, der sich an Kundinnen und Kunden der Sparkasse richtete, war sprachlich gut formuliert und zitierte sogar eine Gesetzesgrundlage.



Liebe Kundin, lieber Kunde!

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

Wer erhält die Energiepauschale?

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

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

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

Vielen Dank für Ihre Zusammenarbeit!

Zur Homepage

Mit freundlichen Grüßen

Ihre Kundenberatung!

Da das Thema zudem medial sehr präsent war, wirkten die Behauptungen der Cyber-Kriminellen beim unbedarften Lesen plausibel. Die Täterinnen und Täter bauten auf diese Weise Vertrauen auf und nutzten die schwierige Lage der Bevölkerung aus.

Dass sich das obige Beispiel an Onlinebanking-Kundinnen und -Kunden richtete, ist keineswegs ein Zufall. Die Finanzdaten der Verbraucherinnen und Verbraucher sowie der mögliche Zugriff zum Onlinebanking sind für Cyber-Kriminelle lohnende Ziele. Aber auch Adressdaten oder die Zugänge zu E-Mail-Konten oder Online-Händlern sind interessant für Angreifende. Mögliche Folgen können sein, dass die Cyber-Kriminellen Bestellungen im Namen der Opfer tätigen oder Verträge abschließen. Zusätzlich infizieren manche Phishing-Webseiten die Endgeräte ihrer Besucherinnen und Besucher mit Schadsoftware, sodass Betroffene mit einem weiteren Problem konfrontiert sind.

Erste Hilfe für Betroffene

Sollte es für die Prävention bereits zu spät sein, bietet das BSI ebenfalls Unterstützung an. Ein Beispiel dafür ist die in Zusammenarbeit mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) erarbeitete „Checkliste für den Ernstfall“ zum Thema Phishing.

Hier bekommen Verbraucherinnen und Verbraucher klare Hilfestellungen und Handlungsempfehlungen dazu, welche Schritte sie ergreifen müssen, wenn sie Opfer einer Phishing-Attacke geworden sind. Dazu gehört unter anderem auch, dass Betroffene Anzeige erstatten sollten. Schließlich sind Phishing-Angriffe Straftaten und sollten erfasst und verfolgt werden.

Aber Phishing ist keinesfalls ein reines E-Mail-Phänomen: Das Abfangen von Passwörtern wird auch auf anderen Wegen betrieben. Vom Vorgehen her ähnlich ist das Smishing – also das Phishing per SMS. Beispielsweise werden Betroffene informiert, für sie läge eine Sprachnachricht vor. Der beigefügte Link führt dann aber nicht zu einer Sprachnachricht, sondern zum Download einer Schadsoftware. Hier und beim E-Mail-Verkehr gilt, dass Provider versuchen, betrügerische Nachrichten über Spam-Filter zurückzuhalten, was aber nicht in allen Fällen gelingt.

Zudem gibt es Betrugsversuche am Telefon, auch Vishing (von Voice-Phishing) genannt. Die Geschichte der betrügerischen Anrufenden wechselt dabei. Schon viele Jahre bekannt ist der Anruf von vermeintlichen Mitarbeitenden von Tech-Konzernen, die ein Sicherheitsrisiko auf dem heimischen PC identifiziert haben wollen. Teilweise wird behauptet, die Rentenversicherung riefe an – oder aber die Polizei oder andere Strafverfolgungsbehörden. Gerade im letzteren Fall wird ein enormer Druck auf die Opfer aufgebaut, teilweise wird sogar mit Anzeige wegen Behinderung von Ermittlungen gedroht, wenn die gewünschten Informationen nicht preisgegeben werden. Zusätzlich wurde bei Vishing oft das sogenannte Call-ID-Spoofing, das Anzeigen einer frei gewählten Nummer im Display der angerufenen Person, genutzt. Seit dem 01. Dezember 2022 sind die Telekommunikationsanbieter verpflichtet, solche Anrufe direkt abzubrechen. Das ist ein wichtiger Schritt für den Schutz von Verbraucherinnen und Verbrauchern .

Trotz technischer Filterung liegt die Herausforderung, der Bedrohungslage durch Phishing zu begegnen, aktuell vor allem bei Verbraucherinnen und Verbrauchern. Denn sie müssen als direkt Betroffene mögliche Gefährdungen erkennen. Hier gilt es insbesondere, Verbraucherinnen und Verbraucher auf das Thema aufmerksam zu machen, über die Betrugsmethoden zu informieren und über mögliche Folgen aufzuklären. Deswegen macht das BSI in seinen Informationsangeboten für Verbraucherinnen und Verbraucher immer wieder auf Phishing aufmerksam und erklärt, welche Faktoren auf Betrugsversuche hinweisen können. Dabei gibt es Schnittpunkte mit unterschiedlichen Anwendungsfeldern, wie zum Beispiel sicheres Onlineshopping oder Onlinebanking. Auch im Rahmen der bundesweiten Kampagne „#einfachaBSIchern“ wird Phishing als mögliches Risiko im Kontext von Home-Office thematisiert. Dabei liegt der Fokus der Kampagne darauf, möglichst positiv, motivierend und aktivierend zu einem sicheren und wachsamen Verhalten aufzurufen.

Besondere Phishing-Maschen macht das BSI zum Beispiel in den sozialen Medien öffentlich. Schließlich fallen diejenigen, die schon von einer Betrugsmasche gehört haben, nicht so leicht auf sie herein. So bleiben Verbraucherinnen und Verbraucher wachsam - und gehen Betrügerinnen und Betrügern nicht so schnell ins Phishing-Netz.

4.1 GASTBEITRAG DER VERBRAUCHERZENTRALE NORDRHEIN-WESTFALEN: Alles Wissenswerte rund um das Phishing-Radar der Verbraucherzentrale NRW.

verbraucherzentrale Nordrhein-Westfalen

Wie funktioniert das Phishing-Radar?

Die Verbraucherzentrale Nordrhein-Westfalen (NRW) führt seit Dezember 2010 ein Phishing-Radar. Verbraucherinnen und Verbraucher leiten betrügerische E-Mails, die sie selbst erhalten haben, vor der Löschung an die Verbraucherzentrale NRW weiter. Täglich gehen derzeit über 540 E-Mails ein, die so gesammelt und ausgewertet werden. Seit dem Start sind bis heute eine knappe Million E-Mails eingegangen. Im Herbst 2017 wurde das Phishing-Radar in einer Kooperation der Verbraucherzentrale Nordrhein-Westfalen mit dem BSI neu konzipiert und technisch weiterentwickelt.

Was genau ist Phishing aus der Sicht der Verbraucherzentrale NRW?

- Phishing im engeren Sinn ist eine E-Mail, in der der Name eines echten Anbieters missbraucht wird.
- Phishing ohne bekannten Anbieternamen (PobA) ist eine E-Mail, mit der jemand zwar an Daten kommen will, dafür aber nicht die Namen Dritter benutzt oder missbraucht.
- Sonstiger Cybercrime hat Ziele wie zum Beispiel die Installation eines Schadprogramms über eine Datei oder auch einen Erpressungsversuch.
- Sonstige E-Mails fasst als eine Art Auffangposten alles Sonstige zusammen: zum Beispiel nerviger aber harmloser Spam

Beispiel für das Jahr 2022 (Stand 06.01.2023):

Im Phishing-Radar wurden insgesamt **198.227 E-Mails** weitergeleitet. Davon waren **26.285 Phishing-E-Mails** im engeren Sinn, **144.366 Phishing** ohne bekannten Anbieternamen, **25.765 sonstiger Cybercrime** und **1.811 sonstige E-Mails.**

Welche Daten gehen in die Zählung des Phishing-Radars ein?

Das Phishing-Radar ist keinesfalls repräsentativ. Dies liegt daran, dass die Zahl der eingehenden E-Mails viel zu gering ist. Die eingegangenen E-Mails haben sich in der Vergangenheit jedoch als ausreichend erwiesen, um neue Phishing-Wellen oder abgeänderte Vorgehensweisen identifizieren zu können (zum Beispiel der Wechsel von betrügerischen HTTP-Seiten auf HTTPS-Seiten).

Täglich werden eine oder zwei Methoden ausgewählt, vor denen öffentlich gewarnt wird. In der Regel wird eine Variante ausgewählt, die entweder besonders häufig am Tag registriert wird oder aber eine besondere Relevanz aufweist (zum Beispiel die ersten Phishing-E-Mails mit Bezug zum russischen Angriffskrieg in der Ukraine im Frühjahr 2022).

Wie werden die Daten verwertet?

Nach der Analyse der eingehenden E-Mails warnt die Verbraucherzentrale auf der Seite (https://www.verbraucherzentrale.nrw/phishing) an jedem Arbeitstag vor aktuellen Betrugsmaschen. Zusätzlich erfahren Verbraucherinnen und Verbraucher auf der Homepage, woran sie eine Phishing-E-Mail erkennen können und erhalten Informationen darüber, wie sie im Schadensfall reagieren sollten.
Das Phishing-Radar wird um einen Twitter-Account (https://twitter.com/vznrw_phishing), das Phishing-Archiv (https://www.verbraucherzentrale.de/phishingarchiv) sowie eine Phishing-Facebook-Gruppe ergänzt.

Beispiel: Phishing im Bankenbereich

Abbildung 4:
Beispiel: Phishing im Bankenbereich

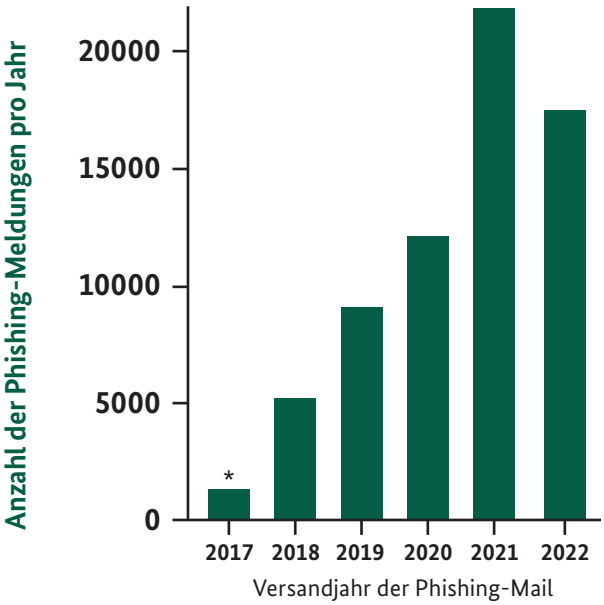


Abbildung 4:
Die Balken zeigen die Gesamtanzahl der im Phishing-Radar der Verbraucherzentrale NRW empfangenen Mails. Hier werden nur Mails betrachtet, die Phishing mit der Zielmarke einer Bank oder eines Finanzdienstleisters (zum Beispiel Sparkasse, Volksbank) durchführen. Die Zahlen für das Jahr 2017 sind auf ein volles Jahr hochgerechnet und daher mit einem * gekennzeichnet. Stand der Daten 06.01.2023

Abbildung 5: Rollende 7-Tage-Inzidenz

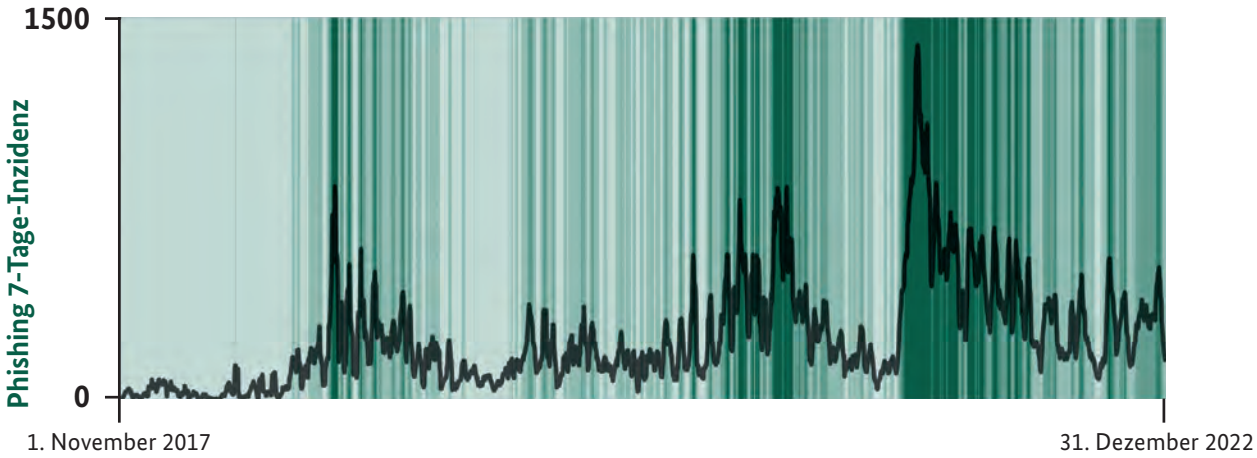


Abbildung 5:
Zeitverlauf der rollenden 7-Tage-Inzidenz der durch das Phishing-Radar der Verbraucherzentrale NRW empfangenen Phishing-Mails mit Zielmarke eines Bankdienstleisters. Die 7-Tage-Inzidenz wird auch als rollende 7-Tage-Summe bezeichnet. Die schwarze Linie zeigt den Wert der 7-Tage-Inzidenz, und die Farbschattierung stellt diese durch eine Schattierung von hell für wenig nach dunkel für sehr viele Phishing-Mails ebenfalls dar. Stand der Daten: 06.01.2023

Was ist zu erkennen?

Abbildung 4 zeigt die jährliche Anzahl der vom Phishing-Radar der Verbraucherzentrale NRW empfangenen E-Mails. In der Darstellung werden nur Phishing-Mails betrachtet, die auf eine Zielmarke im Bankensektor abzielen. Für das Jahr 2017 wurden die Daten auf das volle Jahr hochgerechnet. Im Jahresvergleich zeigt sich eine Zunahme der detektierten Phishing-Mails von anfangs einigen tausend um nun rund 20-mal so viele Mails.

Abbildung 5 unterstreicht diese gemessene Zunahme mit der Darstellung der 7-Tage-Phishing-Inzidenz (der rollenden 7-Tage-Summe an Phishing-Mails) für den Bankensektor. Der Anstieg an Phishing-Mails erfolgt in Wellen, sogenannten Kampagnen. Diese treten immer wieder zeitlich versetzt auf. Die Anzahl an versandten Mails in Kampagnen steigt über die Jahre kontinuierlich an, was die farblichen Streifen in **Abbildung 5** hervorheben. Die Farben fassen Tage mit hohen Phishing-Mail-Aufkommen visuell zusammen. Sie veranschaulichen, dass neben der Phishing-Mail-Anzahl auch die Dauer zunimmt.

Was bedeutet diese Entwicklung?

Das Phishing-Radar ist ein Indikator zur Erkennung von Phishing-Kampagnen. Dieser zeigt: Die Bedrohungslage durch Phishing-Mails im Bankensektor ist allgemein hoch. Phishing-Kampagnen nehmen mit der Anzahl an versandten Mails zu und dauern länger an. Die Wahrscheinlichkeit für Verbraucherinnen und Verbraucher eine Phishing-Mail in diesem Bereich zu erhalten, ist sehr hoch. Cyber-Kriminelle nutzen im Phishing immer wieder neue Methoden. Dabei beschränken sie sich mit ihren Angriffe nicht auf einzelne Banken, sondern haben es gleichermaßen auf alte wie neue Akteure am Markt abgesehen. Sie vollziehen auch fortwährend den Wandel der Branche mit - von den bekannten regionalen und überregionalen Banken zu Neobanken und Kryptowallet.

4.2 GASTBEITRAG DES BUNDESVERBANDES DEUTSCHER BANKEN E.V.: Professionelle Phishing-Angriffe sind eine wachsende Herausforderung.

bankenverband

Anzahl und Komplexität von Phishing-Angriffen haben in den vergangenen Jahren stark zugenommen – in Deutschland, aber auch weltweit. Dies ist nicht verwunderlich, entstehen durch die digitale Transformation sämtlicher Lebensbereiche sowie die stärkere Vernetzung der Unternehmen doch immer wieder neue Einfallstore für Cyber-Kriminelle. Im Bankensektor stellen Cyber-Angriffe bereits seit Beginn des Onlinebankings im November 1980 ein relevantes Thema dar. Für die Institute hat es daher oberste Priorität, das Bewusstsein von Kundschaft und Mitarbeitenden für die Gefahren von Phishing und anderen kriminellen Szenarien zu schärfen.

Zunehmende Komplexität der Angriffe

Phishing, das Abfischen von Daten, hat sich über die Jahre signifikant weiterentwickelt. Haben aufmerksame Verbraucherinnen und Verbraucher in der Vergangenheit vergleichsweise schnell identifizieren können, wenn Daten abgefischt werden sollten – beispielsweise aufgrund fehlerhafter Schreibweisen oder schlecht nachgebauter Webseiten – ist dies heute deutlich schwieriger. Die kriminellen Angriffe haben inzwischen einen hohen Professionalisierungsgrad erreicht. Ähnlich wie Wirtschaftsunternehmen arbeiten die Cyber-Kriminellen grenzüberschreitend und arbeitsteilig organisiert zusammen. Das Spektrum der Cyber-Attacken reicht von breit gestreuten Phishing-E-Mails bis hin zu gezielten Angriffen auf einzelne, speziell ausgewählte Personen, die teilweise über Monate ausspioniert wurden.

André Nash,
kommissarischer Leiter der Themengruppe Banktechnologie und Sicherheit im Bundesverband deutscher Banken e.V.

Im Fokus der Cyber-Kriminellen: der Mensch

Die Qualität der Angriffe hat mittlerweile also ein neues Ausmaß erreicht, das beobachten wir auch im Finanzsektor: So versuchen Cyber-Kriminelle bei einem Großteil ihrer Angriffsszenarien, menschliches Verhalten zu manipulieren, um technische Sicherheitsmaßnahmen zu überwinden, sogenanntes Social Engineering. Ganz gleich ob Phishing, Smishing oder angebliche Anrufe von Bankmitarbeitenden: Ziel der Angreifenden ist es, Privatpersonen dazu zu verleiten, persönliche Informationen und Zugangsdaten preiszugeben oder Transaktionen zu veranlassen. Oftmals liegt es an der Unachtsamkeit von uns Internetnutzenden selbst, wenn daraus ein Schaden entsteht. Ob als Privatpersonen, Verbraucherinnen oder Verbraucher oder als Beschäftigte – wir klicken vorschnell auf Links, öffnen unbekannte Anhänge, lassen uns schlimmstenfalls zur Eingabe persönlicher, sensibler Daten verleiten.

Exemplarisch für eine raffinierte Vorgehensweise ist folgendes Szenario: Über ein vermeintlich gutes Kaufangebot in einer Phishing-Mail wird das Opfer auf einen Fake-Shop geleitet. Im angeblichen Zahlungsvorgang gibt es seinen Namen, seine Adresse, die Telefonnummer und persönliche Konto- beziehungsweise Kreditkartendaten ein. Tatsächlich sind dies Informationen, die oftmals für einen regulären Verkaufsvorgang abgefragt werden. Da die Cyber-Kriminellen mit der Eingabe der Daten ihr (erstes) Ziel erreicht haben, erhält das Opfer im weiteren Verlauf die Fehlermeldung, dass der Verkauf abgebrochen wurde.

Einige Tage später rufen ein angeblicher Bankmitarbeiter oder eine -mitarbeiterin das Opfer an. Dabei muss es nicht zwingend die „eigene Bank" sein, die vermeintlich den Kontakt sucht. Oft werden auch andere seriöse Organisationen oder Unternehmen, wie beispielsweise Interpol, vorgetäuscht. Da die kriminellen Anrufenden die persönlichen Daten kennen, erhöht dies die Glaubwürdigkeit des Anrufs.

Realistische Szenarien werden nunmehr vorgespiegelt: Beispielsweise müsse eine Fehlüberweisung korrigiert werden, oder das Konto in betrügerischer Weise genutzt, so dass eine Buchungskorrektur erforderlich sei. Die Anrufenden treten häufig sehr höflich und hilfsbereit auf. In anderen Fällen wird das Opfer – zum Teil unter Androhung von Strafmaßnahmen, wenn die Unterstützung ausbleibt – unter Druck gesetzt. Ziel des Ganzen ist es, das Opfer dazu zu bringen, Transaktionsnummern (TANs) einzugeben oder Überweisungen beziehungsweise andere Transaktionen in seinem Onlinebanking auszuführen.

Unangetastet: die technischen Systeme der Banken

Das vielleicht größte Einfallstor für Cyber-Attacken ist also der Mensch selbst. Denn eine zwischenmenschliche Manipulation führt zu einem technischen Vorgang, der für sich selbst genommen nicht manipuliert ist.

Sicherheitsmaßnahmen der Banken, wie beispielsweise die Zweifaktor-Authentifizierung, laufen dadurch ins Leere. Diese sollen sicherstellen, dass nur die Bankkunden beziehungsweise Kontoberechtigte entsprechende Transaktionen durchführen können. Genau das aber ist hier ja der Fall.

Das sicherste technische System kann also keinen ausreichenden Schutz bieten, wenn die Nutzerinnen und Nutzer dieses Systems durch Cyber-Kriminelle ausgetrickst werden. Denn die technischen Systeme der Banken selbst werden nicht angegriffen und Banken haben nur beschränkte Möglichkeiten, solche Transaktionen zu verhindern beziehungsweise überhaupt zu erkennen.

Herausforderungen der Zukunft

Die technische Entwicklung von Software und auch die Fortschritte im Bereich Künstlicher Intelligenz (KI) werden künftig neue und perfektionierte Attacken ermöglichen. So werden bereits Fälle von Telefonbetrug registriert, bei denen die Täterinnen und Täter mit Hilfe entsprechender Software ihre Stimmen manipulieren und so versuchen, Privatpersonen oder Mitarbeitende von Unternehmen zu täuschen und Gelder zu ergaunern.

Die Weiterentwicklung der Sicherheitssysteme zum Schutz der Kundendaten und des Kundenvertrauens genießen daher höchste Priorität. Der zunehmenden Professionalisierung krimineller Angriffe begegnen Banken mit hohen Investitionen in die IT-Sicherheit. Doch das ist nicht alles: Damit der menschliche Faktor als Einfallstor für Cyber-Kriminelle deutlich verringert und möglichst ausgeschaltet wird, betreiben Banken einen hohen Aufwand für Schulungen, Awareness-Kampagnen und Aufklärungsarbeit, um Verbraucherinnen und Verbraucher sowie Mitarbeitende von Unternehmen kontinuierlich zu informieren und zu sensibilisieren.

Die Kundinnen und Kunden scheinen dies zu registrieren. In Fragen der Sicherheit bringen sie den Banken großes Vertrauen entgegen. So wird das Onlinebanking unserer Umfrage vom August 2022 zufolge von 78 Prozent der Deutschen als sicher oder sehr sicher bewertet.

Von Bedeutung ist auch der freiwillige, regelmäßige Austausch von Informationen zwischen Banken, Sicherheits- und Strafverfolgungsbehörden. Die Strafverfolgung bleibt aufgrund des professionellen Vorgehens der Cyber-Kriminellen und angesichts von grenzüberschreitenden Aktivitäten aber grundsätzlich schwierig.

Eine Daueraufgabe: Aufklärung und Sensibilisierung

Der Schutz persönlicher Daten im Netz ist auch ein wichtiger Bestandteil der Verbraucheraufklärung des Bankenverbandes. Mit Blog-Beiträgen, Videoformaten und Social-Media-Kampagnen weisen wir auf aktuelle Betrugsmaschen, wie Phishing-Szenarien, hin und setzen dabei auch auf bankenübergreifende Zusammenarbeit. Beispielsweise engagieren wir uns beim jährlichen European Cyber Security Month (ECSM), dem europäischen Aktionsmonat zur Cyber-Sicherheit.

5 Literatur-verzeichnis/ Quellen

B2B Cyber Security (2022):
Erkenntnisse zur Ransomware-Gruppe Black Basta.
Einzusehen unter:
https://b2b-cyber-security.de/erkenntnisse-zur-ransomware-gruppe-black-basta/, zuletzt eingesehen am 12.12.2022

Bitdefender (2022):
Sicherheitslücken im Nooie Babyphone erlauben Angreifern Zugriff auf Live-Bild und Cloud-Aufnahmen.
Einzusehen unter:
https://www.bitdefender.de/blog/hotforsecurity/sicherheitslucken-im-nooie-babyphone-erlauben-angreifern-zugriff-auf-live-bild-und-cloud-aufnahmen, zuletzt eingesehen am: 01.12.2022

Bitkom e. V. (2022):
43 Prozent der Deutschen nutzen Smart-Home-Technologien.
Einzusehen unter:
https://www.bitkom.org/Presse/Presseinformation/Smart-Home-2022, zuletzt eingesehen am: 12.12.2022

Bundesamt für Sicherheit in der Informationstechnik (2022):
Die Lage der IT-Sicherheit in Deutschland 2022.
Einzusehen unter:
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html, zuletzt eingesehen am: 12.12.2022

Bundesamt für Sicherheit in der Informationstechnik (2022):
Face/Off – Täuschung von Verbraucherinnen und Verbrauchern bei Internetdiensten.
Einzusehen unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/digitaler_Verbraucherschutz/Publikationen/Faceoff_taeuschung_von-VerbraucherInnen.pdf?__blob=publicationFile&v=2, zuletzt eingesehen am 12.12.2022

Bundesamt für Sicherheit in der Informationstechnik (2022a):
IT-Sicherheit auf dem digitalen Verbrauchermarkt – Fokus: Onlineshopping-Plattformen.

Bundesamt für Sicherheit in der Informationstechnik (2022):
Woran erkenne ich sichere Onlineshops?
Einzusehen unter:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/Online-Shopping/Worauf-beim-Online-Einkauf-zu-achten-ist/worauf-beim-online-einkauf-zu-achten-ist_node.html, zuletzt eingesehen am 13.12.2022

Bundesministerium des Innern und für Heimat (2020):
BMI und BSI: Informationskampagne zur IT-Sicherheit.
Einzusehen unter:
https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/02/safer-internet-day.html, zuletzt eingesehen am 21.12.2022.

Bundesverband Brennholzhandel und Brennholzproduktion e.V. (2022):
Warnung vor Betrug beim Online-Kauf von Brennholz.
Einzusehen unter:
https://www.bundesverband-brennholz.de/warnung-vor-betrug-beim-kauf-von-brennholz/, zuletzt eingesehen am: 08.12.2022

DsiN (2022):
Steigende Energiepreise: Verbraucherzentrale warnt vor Fake Shops im Netz.
Einzusehen unter:
https://www.sicher-im-netz.de/steigende-energiepreise-verbraucherzentrale-warnt-vor-fake-shops-im-netz, zuletzt eingesehen am: 05.12.2022

Golem (2022):
Ransomware - Stadt informiert Bürger über Daten im Darknet.
Einzusehen unter:
https://www.golem.de/news/ransomware-stadt-informiert-buerger-ueber-daten-im-darknet-2205-165414.html, zuletzt eingesehen am: 25.11.2022

Heise (2022):
Nach Cyberangriff auf Verwaltung Daten ukrainischer Geflüchteter im Darknet.
Einzusehen unter:
https://www.heise.de/news/Nach-Cyberangriff-auf-Verwaltung-Daten-ukrainischer-Gefluechteter-im-Darknet-7337774.html, zuletzt eingesehen am: 22.11.202

Heise (2022a):
Brute-Force-Angriff: "Mittlere fünfstellige" Zahl von thalia.de-Konten gehackt.
Einzusehen unter:
https://www.heise.de/news/Brute-Force-Angriff-Mittlere-fuenfstellige-Zahl-von-thalia-de-Konten-gehackt-6336552.html, zuletzt eingesehen am 12.12.2022

HTW Berlin (2022):
IT-Sicherheitsvorfall.
Einzusehen unter:
https://www.f3.htw-berlin.de/it-sicherheitsvorfall/#c78899, zuletzt eingesehen am: 12.11.2022

Lowell Financial Services GmbH (2022):
Cyber-Attacke auf die Lowell-Gruppe in Deutschland, Österreich und der Schweiz.
Einzusehen unter:
https://www.lowellgroup.de/cyber-attack, zuletzt eingesehen am 12.12.2022

Spiegel (2022):
Ausgespäht per Katzenfutterautomat – Frau erstattet Strafanzeige.
Einzusehen unter:
https://www.spiegel.de/netzwelt/apps/gelsenkirchen-ausgespaeht-per-katzenfutterautomat-frau-erstattet-strafanzeige-a-73f9b137-332c-40a9-a301-dc5e277226d8, zuletzt eingesehen am 22.11.2022

Spiegel (2022):
Hackerbande erbeutete bei Sixt auch Kundendaten.
Einzusehen unter:
https://www.spiegel.de/netzwelt/web/sixt-hacker-gruppe-erbeutete-auch-kundendaten-a-ba9d93de-ec01-4406-aaac-30c5044a1481), zuletzt eingesehen am 13.12.2022

Tagesschau (2022):
Nutzerdaten jahrelang online.
Einzusehen unter:
https://www.tagesschau.de/wirtschaft/verbraucher/datenleck-verbraucherdaten-101.html, zuletzt eingesehen am 12.12.2022

The Register (2022):
Emma Sleep Company admits checkout cyber attack.
Einzusehen unter:
https://www.theregister.com/2022/04/04/emma_the_sleep_company_admits/, zuletzt eingesehen am 12.12.2022

Verbraucherzentrale Bundesverband (2022):
Cybersicherheit bei vernetzten Geräten stärken.
Einzusehen unter:
https://www.vzbv.de/pressemitteilungen/cybersicherheit-bei-vernetzten-geraeten-staerken, zuletzt eingesehen am: 01.12.2022

Verbraucherzentrale Hamburg (2022):
Fake Shop Liste: Wenn günstig richtig teuer wird!
Einzusehen unter:
https://www.vzhh.de/themen/einkauf-reise-freizeit/online-shopping/fake-shop-liste-wenn-guenstig-richtig-teuer-wird, zuletzt eingesehen am 13.12.2022

Verbraucherzentrale Nordrhein-Westfalen (2022):
Achtung, Phishing: Betrug mit Energiepauschale und Gaspreis-Rabatten.
Einzusehen unter:
https://www.verbraucherzentrale.nrw/aktuelle-meldungen/digitale-welt/achtung-phishing-betrug-mit-energiepauschale-und-gaspreisrabatten-76907, zuletzt eingesehen am 07.12.2022

www.bsi.bund.de